The Multiplicitive Group of Complex Numbers

$\mathbb{C} = \{ a + bi \mid a, b \in \mathbb{R} \}$ $\qquad \mathbb{C}^* = \mathbb{C} \setminus \{0\}$

$i^2 = -1$

$z = a + bi, \quad w = c + di$

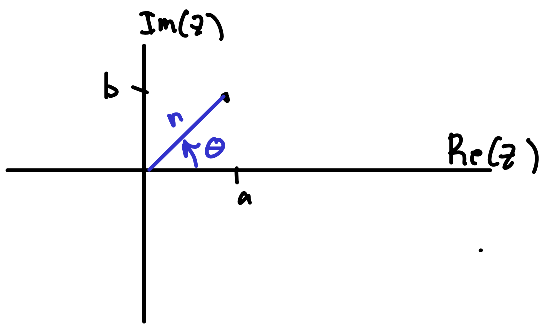
$z + w = (a+c) + (d+b)i$

$z \cdot w = (ac - db) + (ad + bc)i$

$z \neq 0$

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

$|z| = \sqrt{a^2 + b^2}$: modulus or abs. value



$z = a + bi$ (a: Re(z), b: Im(z))

cartesian coords, Polar coords

$z = a + ib$ $\qquad z = r(\cos\theta + i\sin\theta)$

$z = r \cdot e^{i\theta} = r(\cos\theta + i\sin\theta)$ — Euler's formula.

we restrict $0 \leq \theta < 2\pi$

May show that

$z = re^{i\theta}, \quad w = se^{i\phi}$

$z \cdot w = rse^{i(\theta + \phi)}$

Theorem (De Moivre)

$z = re^{i\theta}$ then $z^n = (re^{i\theta})^n = r^n e^{in\theta}$ for $n = 1, 2, \ldots$

Proof: Induction + Euler formula + trig identities.

$\mathbb{C}^*$ has cool subgroups of finite order ($\mathbb{R}^*, \mathbb{Q}^*$ do Not have subgroups of finite order)

$\mathbb{T} = \{ z \in \mathbb{C} \mid |z| = 1 \}$ ← The circle group

$|z| = a^2 + b^2 = 1$

To show $\mathbb{T}$ is a subgroup:

$|z| = 1 \iff z = e^{i\theta}$

- id $\iff \theta = 0$
- closed $e^{i\theta} e^{i\phi} = e^{i(\theta + \phi)}$
- inverse $e^{-i\theta}$

— Circle group has infinite order

$H = \{1, -1, i, -i\}$ is a cyclic subgroup of the circle group

$\updownarrow$

$z^4 = 1$ gives elements of H

The complex solutions of $z^n = 1$ are called the nth roots of unity.

Theorem: If $z^n = 1$ then the n^{th} roots of unity are

$$z = e^{\frac{2k\pi}{n} i}, \quad k = 0, 1, \dots, n-1$$

Furthermore the n^{th} roots of unity form a cyclic subgroup of $\mathbb{T}$ having order n.

Proof overview

- $z^n = \left(e^{\frac{2k\pi}{n} i} \right)^n = e^{2k\pi i} = \cos(2\pi k) + i \sin(2\pi k)$
  $= 1 \quad \forall k$

- $\frac{2k\pi}{n}$ are distinct in $[0, 2\pi)$ $\therefore$ n roots
- By the fundemental Theorem of Algebra (cor. 17.9) $\exists$ at most n roots.
- These are all of the roots. and $|z| = 1$ $\therefore$ we have all n roots of unity
- 1 is a root of unity, check inverses ... $\blacksquare$

A generator of the n^{th} roots of unity a <u>Primitive n^{th} root.</u>

$$\Updownarrow$$

$$z = e^{\frac{2k\pi}{n} i}$$

<u>Ex 1</u> Consider the 8^{th} roots of unity, $z^8 = 1$

$$k=1$$

$$w = e^{\frac{2\pi}{8} i} = e^{\frac{\pi}{4} i} = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} i$$

8^{th} roots of unity $= \langle w \rangle = \langle w^3 \rangle = \langle w^5 \rangle = \langle w^7 \rangle$

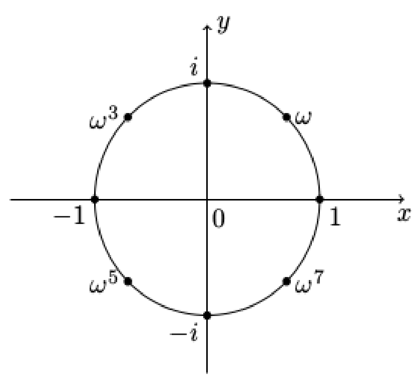


Figure 4.27: 8th roots of unity

Permutation Groups

- The permutations of a set X form a group S_X
- If X is finite we may take $X = \{1, 2, \dots, n\}$ and write S_n
- S_n is called the symmetric group on n letters.

Theorem 5.1 | The symmetric group on n letters, S_n, is a group with $n!$ elements where the binary op. is composition of maps.

Proof:

- identity is

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix} \longleftrightarrow 1 \mapsto 1, 2 \mapsto 2, \dots, n \mapsto n$$

- If $f : S_n \to S_n$ is a permutation $\Rightarrow$ f is bijective

  $\therefore$ f^{-1} exists and is bijective $\therefore$ $f^{-1} : S_n \to S_n$

- composition of maps is associative
- $|S_n| = n!$ is a Question in the book.

$\blacksquare$

A subgroup of S_n is called a permutation group

Note: we will use the convention of multiplying permutations right to left

$$\sigma\tau \Rightarrow \text{do } \tau \text{ first then do } \sigma$$

since

$$\sigma\tau(x) = \sigma \circ \tau(x) = \sigma(\tau(x))$$

- $\sigma\tau \neq \tau\sigma$ mostly.