The Multiplicative Group of Complex Numbers

\[ \mathbb{C} = \left\{ a + bi \mid a, b \in \mathbb{R} \right\} \quad \mathbb{C}^* = \mathbb{C} \setminus \{0\} \]

\[ i^2 = -1 \]

\[ z = a + bi, \quad w = c + di \]

\[ z + w = (a + c) + (d + b)i \]

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

\[ z \neq 0 \]

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

\[ |z| = \sqrt{a^2 + b^2} \quad \text{modulus or abs. value} \]

\[ z = a + ib \]

\[ z = r (\cos \theta + i \sin \theta) \quad \text{Euler's formula.} \]

\[ z = r e^{i\theta}, \quad w = s e^{i\phi} \]

\[ z \cdot w = rs e^{i(\theta + \phi)} \]

\[ z = re^{i\theta} \quad \text{then} \quad z^n = (re^{i\theta})^n = rn e^{i\theta} \quad \text{for } n = 1, 2, \ldots \]
Proof: Induction + Euler formula + trig identities.

\( \mathbb{C}^* \) has cool subgroups of finite order \( \left\{ \mathbb{R}^*, \mathbb{Q}^* \right\} \). To show \( \mathbb{T} \) is a subgroup:

\[
|2| = 1 \quad \Rightarrow \\
2 = e^{i \theta} \\
\cdot \text{id} \Rightarrow \theta = 0 \\
\cdot \text{closed} \quad e^{i \theta} e^{i \phi} = e^{i(\theta + \phi)} \\
\cdot \text{inverse} \quad e^{-i \theta}
\]

Circle group has infinite order.

\( H = \{ 1, -1, i, -i \} \) is a cyclic subgroup of the circle group \( \mathbb{T} \).

\( z^n = 1 \) gives elements of \( H \).

The complex solutions of \( z^n = 1 \) are called the \( n \)-th roots of unity.

**Theorem:** If \( z^n = 1 \) then the \( n \)-th roots of unity are

\[
z = e^{2k \pi i/n}, \quad k = 0, 1, \ldots, n-1
\]

Furthermore, the \( n \)-th roots of unity form a cyclic subgroup of \( \mathbb{T} \) having order \( n \).

Proof overview:

\[
z^n = \left( e^{2k \pi i/n} i \right)^n = e^{2k \pi i} = \cos (2k \pi k) + i \sin (2k \pi k) = 1 \quad \forall k
\]
\( \frac{2k\pi}{n} \) are distinct in \([0, 2\pi)\), \( n \) roots.

By the Fundamental Theorem of Algebra (cor. 17.9), \( \exists \) at most \( n \) roots.

These are all of the roots, and \( |z| = 1 \), 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 primitive \( n \)th root.

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

**Ex.** Consider the 8th roots of unity, \( z^8 = 1 \)

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

8th roots of unity = \( \langle w \rangle = \langle w^3 \rangle = \langle w^5 \rangle = \langle w^7 \rangle \)

![Diagram of 8th roots of unity](image)

**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 $X = \{1, 2, \ldots, n\}$ 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
  
  $$(1 \ 2 \ \ldots \ n) \rightarrow 1 \mapsto 1, 2 \mapsto 2, \ldots, n \mapsto n$$

- If $f : S_n \rightarrow S_n$ is a permutation $\Rightarrow$ $f$'s bijective
  
  $\therefore$ $f^{-1}$ exists and is bijective $\therefore f^{-1} : S_n \rightarrow S_n$

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

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.