The Multiplicitive Group of Complex numbers

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

$i^2 = -1$

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

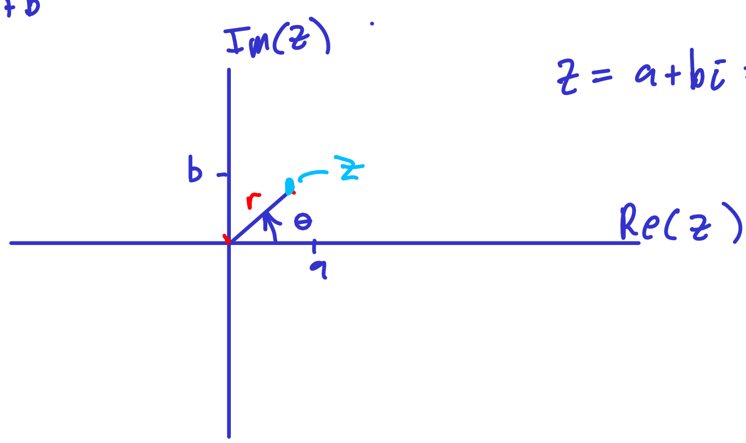
$$z \cdot w = (ac - db) + (ad + bc)i$$

$z \neq 0$

$$z^{-1} = \frac{a}{a^2+b^2} + \frac{(-b)}{a^2+b^2} i = \frac{a - bi}{a^2+b^2} = \frac{1}{a+ib} \cdot \left(\frac{a-ib}{a-ib} \right)$$

$|z| = \sqrt{a^2+b^2}$

$z = a+bi = Re(z) + Im(z) i$



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

May show that complex exponential

$$z = r e^{i\theta} = r(\cos\theta + i \sin\theta)$$

$$w = s e^{i\phi}$$

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

Theorem (De Movre)

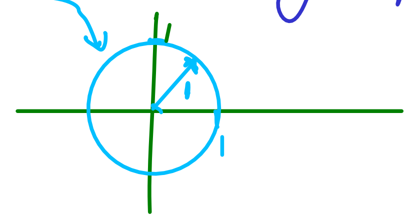
If $z = re^{i\theta}$ then $z^n = (re^{i\theta})^n = r^n e^{in\theta}$ for $n \in \mathbb{Z}$.

Proof follows from trig identities and induction.

$\mathbb{C}^*$ is a group with multiplication

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

$a^2 + b^2 = 1$



Show $\mathbb{T}$ is a subgroup

$|z| = 1$ and think of $z = re^{i\theta}$

but if $|z| = 1 \Rightarrow r = 1$

$|r(\cos\theta + i\sin\theta)| = |r|\,|\cos\theta + i\sin\theta|$
$= |r|$

$\therefore$ if $z \in \mathbb{T}$ $\quad z = e^{i\theta}$

- id ⟺ $\theta = 0$
- closed since $e^{i\theta}e^{i\phi} = e^{i(\phi+\theta)}$
- inverses $e^{-i\theta} \cdot e^{i\theta} = e^{i(\theta-\theta)} = 1$

- It has interesting subgroups of finite order

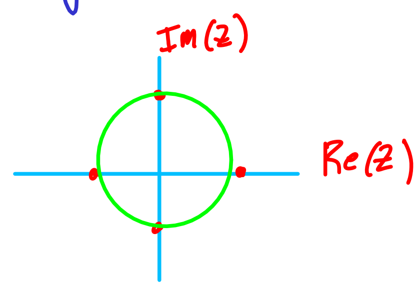
A subgroup of $\mathbb{T}$ (and $\mathbb{C}^*$) is

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

$H = \langle i \rangle = \{ i, -1, -i, 1 \}$

⇕

All roots of $z^4 = 1$



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

Further more the n^{th} roots of unity form a cyclic subgroup of the circle group.

Proof over view

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

- $\frac{2k\pi}{n} \neq \frac{2l\pi}{n} \quad \forall\, l \neq k \quad \therefore$ we have n roots
- By the fundamental theorem of Algebra (cor 17.4 in Book) $\exists$ at most n roots
- $\therefore$ these are all the n^{th} roots of unity and $|z| = 1$
- 1 is an n^{th} root of unity
- $e^{\frac{-k2\pi i}{n}} \cdot e^{\frac{k(2\pi i)}{n}} = 1$

inverse

trig identity

$$e^{\frac{-k2\pi i}{n}} = e^{\frac{(n-k)2\pi i}{n}}$$

Corrollary

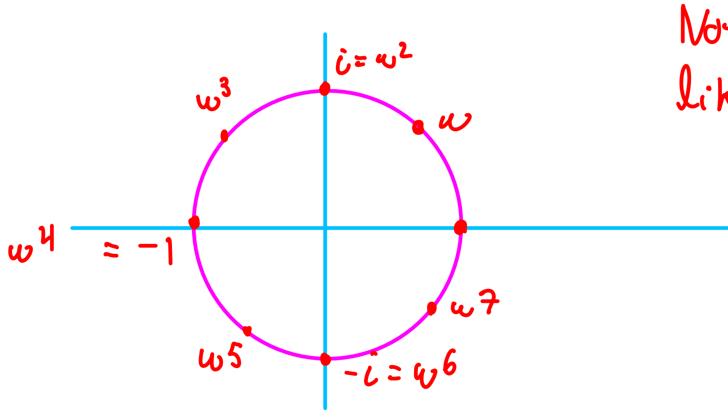
the nth roots of unity $= \langle e^{\frac{2\pi i}{n}} \rangle$

(as a subgroup of $\mathbb{T}$)

Ex] consider 8^{th} roots of unity, $z^8 = 1$

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

$G = 8^{th}$ roots of unity $= \langle \omega \rangle$



Note G behaves like $\mathbb{Z}_8$

Permutation groups

Recall a permutation on a set S is

a 1-1 and onto map $\pi : S \to S$

Ex $S = \{a, b, c\}$ $\begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix} \Leftrightarrow$ $a \mapsto b$, $b \mapsto c$, $c \mapsto a$

Denote the permutations of a set X as S_X

- If X is finite, take $X = \{1, 2, \ldots, n\}$ and write S_n
- S_n is called the symmetric group on n letters.

Thm. S_n is a group with $n!$ elements where the operation is composition of maps.

Proof:

- Identity $\begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix} \Leftrightarrow 1 \mapsto 1,\ 2 \mapsto 2, \ldots, n \mapsto n$

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

  $\Rightarrow f$ is bijective

  $\therefore f^{-1}$ exists and is also a map $f^{-1} : S_n \to S_n$

- composition of maps is associative.

- $|S_n| = n!$ Book problem

$\blacksquare$

A subgroup of S_n will called a permutation group.

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

i.e.

$\sigma\tau \Rightarrow$ do τ first, then σ

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

- $\sigma\tau \neq \tau\sigma$ usually.

Ex) G is a subgroup of S_5 consisting of the identity and

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix}\begin{matrix} -x \\ -\sigma(x) \end{matrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix}, \quad \mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$$

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

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}-x = \mu$$

we got

$$\mu\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix} = \sigma$$

$\tau\mu = \sigma$

	e	σ	τ	μ
e	e	σ	τ	μ
σ	σ	e	μ	τ
τ	τ	μ	e	σ
μ	μ	τ	σ	e

Ex) Permutations may not commute i.e. in S_4

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}\begin{matrix} -x \\ -\tau(\sigma(x)) \end{matrix}$$

$$\overset{\sigma(\tau(x))}{\sigma\tau} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}\begin{matrix} x \\ \sigma(\tau(x)) \end{matrix}$$

$\therefore \sigma\tau \neq \tau\sigma.$

Cycle notation

A permutation $\sigma \in S_X$ is a <u>cycle of length k</u> if

$\exists$ $a_1, \ldots, a_k \in X$ s.t.

$$\sigma(a_1) = a_2$$
$$\sigma(a_2) = a_3$$
$$\vdots$$
$$\sigma(a_k) = a_1$$

and $\sigma(x) = x$ for all $x \notin \{a_1, \ldots, a_k\}$

we write $(a_1, a_2, \ldots, a_k)$

Ex)

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 3 & 5 & 1 & 4 & 2 & 7 \end{pmatrix} = (1\,6\,2\,3\,5\,4)$$

is a cycle of length 6

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 6 & 5 \end{pmatrix} = (1\,2\,4\,3)(5\,6)$$

is not a cycle

Ex) Products of cycles

$\sigma = (1\,3\,5\,2)$ $\qquad \tau = (2\,5\,6)$

$\sigma\tau \neq \tau\sigma$ (check)

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

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 5 & 4 & 6 & 1 \end{pmatrix} \begin{array}{l} \to x \\ \sigma(\tau(x)) \end{array}$$

Sumary : $\sigma\tau = (1\,3\,5\,2)(2\,5\,6) = (1\,3\,5\,6)$

Def: Two cycles $\sigma = (a_1, \ldots, a_k)$, $\tau = (b_1, \ldots, b_\ell)$ are disjoint if $a_i \neq b_j \ \forall i, j$.

Ex) $(1\,3\,5)$ and $(2\,7)$ are disjoint

$(1\,3\,5)$ and $(3\,4\,7)$ are not

$$(1\,3\,5)(2\,7) = (1\,3\,5)(2\,7)$$

$$(1\,3\,5)(3\,4\,7) = (1\,3\,4\,7\,5)$$

Proposition)

Let σ, τ be disjoint cycles in S_X. Then $\sigma\tau = \tau\sigma$.

Proof:

Let $\sigma = (a_1, \ldots, a_k)$, $\tau = (b_1, \ldots, b_k)$

Show $\sigma\tau(x) = \tau\sigma(x) \quad \forall x \in X$

If $x \notin \{a_1, \ldots, a_k\}$ and $x \notin \{b_1, \ldots, b_k\}$

$\Rightarrow \sigma(x) = x$, $\tau(x) = x$

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

Suppose $x \in \{a_1, \dots, a_k\}$ (WLOG)

So $x = a_j$ for some j

$$\sigma(a_i) = a_{(i \bmod k)+1}$$

a