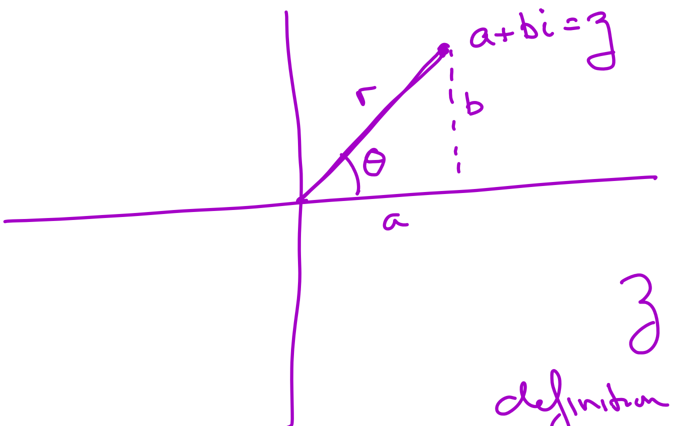
Roots of Unity

Polar and rectangular form of complex numbers

Brief review of polar and rectangular form of complex numbers.

$$\mathbb{C} = \{a+bi \mid a,b \in \mathbb{R},\ i^2=-1\}$$



$$r^2 = a^2+b^2 = \|z\|^2$$

$$b = r\sin\theta$$
$$a = r\cos\theta$$

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

definition: $\mathrm{cis}(\theta) = \cos\theta + i\sin\theta$

$$z = r\,\mathrm{cis}(\theta)$$

$$z_1 = r_1\,\mathrm{cis}(\theta_1)$$
$$z_2 = r_2\,\mathrm{cis}(\theta_2)$$

$$z_1 z_2 = r_1 r_2\,\mathrm{cis}(\theta_1)\,\mathrm{cis}(\theta_2)$$

$$\mathrm{cis}(\theta_1)\,\mathrm{cis}(\theta_2) = \mathrm{cis}(\theta_1+\theta_2)$$

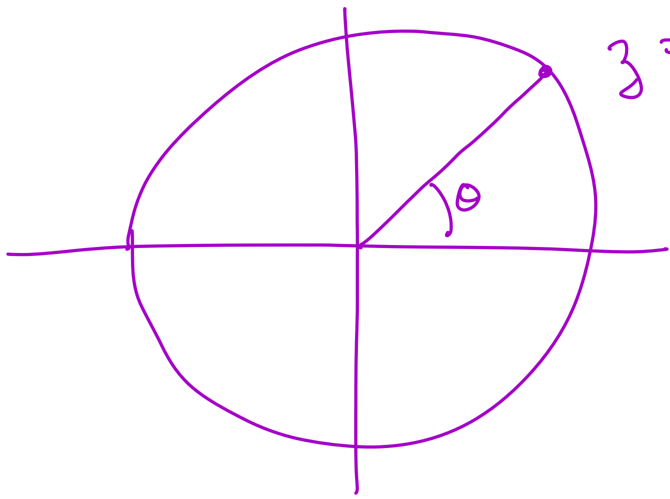
$$\boxed{z_1 z_2 = r_1 r_2\,\mathrm{cis}(\theta_1+\theta_2)}$$

$$(\cos\theta_1 + i\sin\theta_1)(\cos(\theta_2) + i\sin\theta_2)$$
$$= (\quad) + i(\quad)$$

addition laws for sin, cos

The circle group

$\mathbb{T} = \{ z \mid z = \mathrm{cis}(\theta),\ \theta \in \mathbb{R} \}.$



$z = \mathrm{cis}(\theta)$ $\quad [r = 1]$

$\ominus$ $1 = \mathrm{cis}(0)$ $I_{\mathbb{T}}$

$\ominus$ $z = \mathrm{cis}(\theta)$

$z^{-1} = \mathrm{cis}(-\theta)$ since

$\mathrm{cis}(\theta)\,\mathrm{cis}(-\theta) = \mathrm{cis}(0) = 1.$

abelian.

$\mathrm{cis}(\theta)\,\mathrm{cis}(\tau) = \mathrm{cis}(\theta + \tau)$

$= \mathrm{cis}(\tau + \theta)$

$= \mathrm{cis}(\tau)\,\mathrm{cis}(\theta)$

Roots of unity

Fix an integer $n > 0$. For any integer k, let $z(k) = \mathrm{cis}(\frac{2k\pi}{n})$.

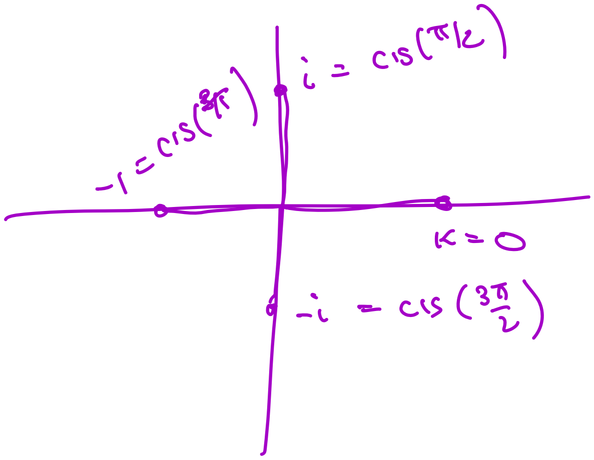
Proposition: The $z(k)$ have the following properties:

- $z(k)z(j) = z(k+j)$.
- $z(k)^m = z(km)$.
- $z(k) = 1$ if and only if $n|k$. More generally $z(i) = z(j)$ if and only if $i \equiv j \pmod{n}$.

$n = 4$

$z(k) = \mathrm{cis}\left(\frac{2k\pi}{4}\right)$

$= \mathrm{cis}\left(k\frac{\pi}{2}\right)$



PROOF:

- $z(k)z(j) = z(k+j)$

$\mathrm{cis}\left(\frac{2k\pi}{n}\right)\mathrm{cis}\left(\frac{2j\pi}{n}\right)$

$= \mathrm{cis}\left(\frac{2(k+j)\pi}{n}\right)$

$= z(k+j)$

- $z(k)^m = z(mk)$

$z(k)^m = z(\underbrace{k + \dots \dots + k}_{m})$

$= z(km)$

$z(k) = 1 \iff n|k$.

$z(k) = \mathrm{cis}\left(\frac{2k\pi}{n}\right) = 1$ only if

$\frac{2k\pi}{n}$ is an integer multiple of 2π

$\iff \frac{k}{n} \in \mathbb{Z} \iff n|k$.

$z(i) = z(j) \iff z(i-j) = 1$

$\iff$ $i-j$ is a multiple of n $\iff i \equiv j \bmod n$.

Proposition: For any integer $n > 0$, the distinct complex solutions to the polynomial equation $z^n = 1$ are the complex numbers $z(i)$ for $i = 0, \ldots, n-1$. These solutions form a cyclic group of order n that we will call μ_n.

Proof: From the preceeding proposition, we know that the $z(i)$ are distinct for $i = 0, \ldots, n-1$ and satisfy $z(i)^n = 1$. Further, $z(i) = z(1)^i$ so $z(1)$ is a generator for μ_n.

$z(i)^n = z(ni)$ $\quad ni \equiv 0 \mod n$ so $z(ni) = 1$.

$z(0), z(1), \ldots, z(n-1)$ are different and there are n of them. $z(i)$ are a subgroup

$z(i) z(-j) = z(i-j) \in \mu_n$

$z(1), z(1)^2 = z(2), z(1)^3 = z(3), \ldots, z(1)^n = z(n) = z(0)$

μ_n is a cyclic group of order n.

Proposition: $z(i)$ is a generator of μ_n if and only if $\gcd(i, n) = 1$. These generators are called *primitive* roots of unity.

analog: $\{z(0), z(1), \ldots, z(n-1)\} = \mu_n$

$z(j)$ is a generator of μ_n means

$z(j)^k = 1 \iff n \mid jk \iff \frac{n}{d} \mid k$ where

$z(j)^k = z(jk)$

$d = \gcd(n, j)$.

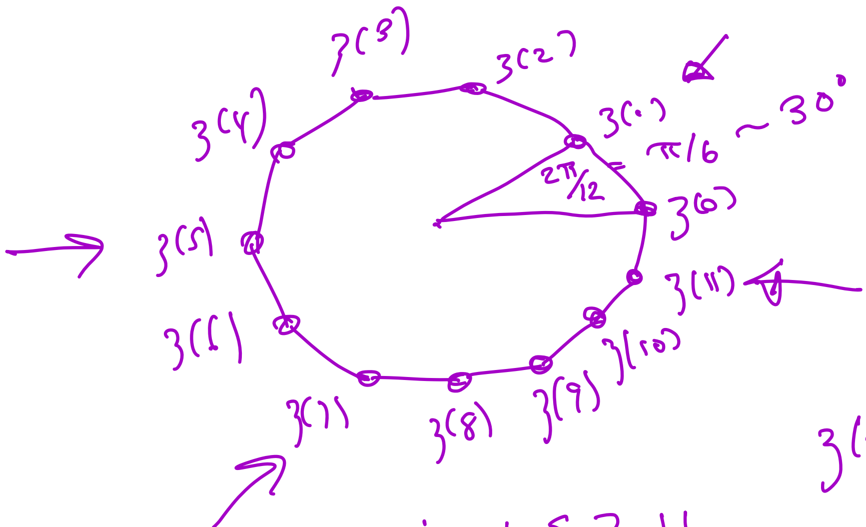
$d > 1$, then $z(j)^{n/d} = 1$ So $z(j)$ not a generator

$\langle z(j) \rangle$ is not everything

$d = 1$ then $z(j)$ is a generator.

Example

Suppose $n = 12$.



$\zeta(j)$ with $(j, 12) = 1$

$j = 1, 5, 7, 11$

$\zeta(j)$ called primitive if it generates μ_n.