1. Let $m \in \mathbf{N}$ and $m\mathbf{Z} = \{mn : n \in \mathbf{Z}\}$. Prove $m\mathbf{Z} < \mathbf{Z}$. Conversely, prove that any subgroup of $\mathbf{Z}$ is of this form.

   Hint: given $H < \mathbf{Z}$, let m be the smallest positive element of H.

$0 = 0 \cdot m \in m\mathbb{Z}$ ✓

If $mn, mn' \in m\mathbb{Z}$, $mn - mn' = m(n-n') \in m\mathbb{Z}$

$\therefore m\mathbb{Z} < \mathbb{Z}$

Let $H < \mathbb{Z}$. If $H = \{0\}$, then $H = 0 \cdot \mathbb{Z}$ ✓

Otherwise let $m = \underline{\underline{\min}} \{h \in H : h > 0\}$ $\neq \emptyset$

(well-ordering principle)

Since $H < \mathbb{Z}$, $m \in H$, $\underline{m\mathbb{Z} < H}$

Let $h \in H$, div. alg.: $\exists! q, r$ $h = qm + r$, $0 \leq r < m$

$r = \underset{\in H}{h} - \underset{\in m\mathbb{Z} < H}{qm} \in H$ since m is smallest pos. in H

$r \not> 0$, so $r = 0$

so $h \in m\mathbb{Z}$ $\therefore$ $\underline{H < m\mathbb{Z}}$ $\therefore H = m\mathbb{Z}$

2. Suppose $\alpha = (1,2,3)(2,3,4,5)$ is a permutation (in cycle notation). What is the order of α? What is the parity of α? Express α^{2017} as a product of disjoint cycles.

$$\alpha = \boxed{\underbrace{(1\ 2)}_{\text{ord } 2}\underbrace{(3\ 4\ 5)}_{\text{ord } 3}} \qquad \text{ord}(\alpha) = \text{lcm}(2,3) = \boxed{6}$$

(Ruffini)

$$\text{odd} + \text{even} = \boxed{\text{odd}}$$

$$2017 \equiv 1 \bmod 6 \qquad \therefore \quad \alpha^{2017} = \boxed{\alpha}$$

3. Suppose G is finite group of order n and $a \in G$. Prove that $a^n = e$. What conclusions can you draw about the order of a, if $a \neq e$ and n is prime? What conclusion can you draw about groups of prime order?

Let $k = \text{ord}(a)$

Lagrange $\Rightarrow$ $k \mid n$ $\quad \exists i \quad n = ki$

index of $\langle a \rangle$ in G

$[G : \langle a \rangle]$

$a^n = a^{ki} = (a^k)^i = e^i = e$

If $a \neq e$ $\quad k \neq 1$, so since $k \mid n \leftarrow$ prime, $k = n$

So $G = \langle a \rangle$

$\therefore$ Groups of prime order are cyclic and have no proper nontrivial subgroups

4. Let $H = \{z \in \mathbf{C} \colon z^n = 1\}$. Prove that H is a subgroup of $\mathbf{C}^*$ isomorphic to $\mathbf{Z}_n$.

1. $H < \mathbb{C}^*$

$1^n = 1$, so $1 \in H$ ✓

Suppose $x, y \in H$. Then $x^n = 1$, $y^n = 1$

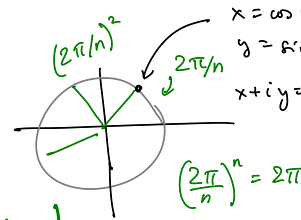
$$(xy^{-1})^n = x^n y^{-n} = x^n (y^n)^{-1} = 1 \cdot 1^{-1} = 1$$

$\therefore \quad xy^{-1} \in H$ ☺

2. $e^{2\pi i k/n}$, $k = 0, 1, \dots n-1$ ← all distinct

Also $z^n = 1$ has at most n distinct roots

(factor $z^n - 1$)



$x = \cos\left(\frac{2\pi}{n}\right)$ Euler's formula

$y = \sin\left(\frac{2\pi}{n}\right)$

$x + iy = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right)$

$= e^{2\pi i/n}$

$$\therefore H = \left\{\left(e^{2\pi i/n}\right)^k : k = 0, \dots n-1\right\} = \left\langle e^{2\pi i/n} \right\rangle$$

← cyclic!

By the characterization of cyclic groups

$H \cong \mathbb{Z}_n$ ☺

More explicitly, define $\phi : \underset{\langle [1]_n \rangle}{\overset{\shortparallel}{\mathbb{Z}_n}} \to \mathbb{C}^*$ by

$$\phi(1) = e^{2\pi i/n}$$

$$\Rightarrow \quad \phi(k) = \phi(1)^k = e^{2\pi i k/n} \quad \leftarrow \text{all in } \mathbb{C}^*$$

Well-def'd: Suppose $k' \equiv k \mod n$ then $\exists\, q \quad k' = k + qn$

$$\phi(k') = e^{2\pi i k'/n} = e^{2\pi i(k+qn)/n} = e^{2\pi i k/n} \cdot \underbrace{e^{2\pi i q}}_{1}$$

$$= \phi(k) \quad ☺$$

$$\phi(k + \ell) = e^{2\pi i(k+\ell)/n} = e^{2\pi i k/n} \cdot e^{2\pi i \ell/n} = \phi(k) \cdot \phi(\ell)$$

$\therefore \phi$ is a hom

ϕ is 1-1: If $\phi(k) = e^{2\pi i k/n} = 1 \qquad \frac{k}{n} \in \mathbb{Z} \iff n \mid k$

$\iff k \equiv 0 \mod n$

$\therefore \ker \phi$ is trivial $\quad \therefore \phi$ is 1-1

$\operatorname{Im} \phi = H \qquad \therefore H < \mathbb{C}^*$

$\therefore \phi : \mathbb{Z}_n \to H$ is an isomorphism.

5. Prove $\mathrm{Aut}(\mathbf{Z}) \cong \mathbf{Z}_m$ $(m = ?)$

A hom $\phi : \mathbb{Z} \to \mathbb{Z}$ is uniquely determined by a (free) choice of $\phi(1)$ $\quad \phi(k) = k\,\phi(1)$

Since $U(\mathbb{Z}) = \{1, -1\}$, if φ is an iso $\varphi(1) = 1$ or -1 $\quad \phi(k) = k$ or $\phi(k) = -k$

$\mathrm{Aut}(\mathbb{Z}) = \{\varepsilon, \psi\}$, where $\varepsilon(k) = k$, $\psi(k) = -k$

Any group of order 2 is $\cong \mathbb{Z}_2$ ☺

More explicitly define $T : \mathrm{Aut}\,\mathbb{Z} \to \mathbb{Z}_2$ by $T(\varepsilon) = 0$, $T(\psi) = 1$. Clearly 1-1 & onto

Verify T is a hom, e.g.

$$T(\psi\psi) = T(\varepsilon) = 0$$

$$T(\psi) + T(\psi) = 1 + 1 = 0$$

$=$ ☺

etc.

$\therefore T$ is an iso ☺

Take 2: Define $\phi : \mathbb{Z} \to \mathbb{C}^*$

$\phi(k) = e^{2\pi i k/n}$

Don't have to prove well-def'd :)

ker ϕ = ? If $\phi(k) = 1$, then $e^{2\pi i k/n} = 1$

so $n \mid k$ (same as before)

Conversely if $n \mid k$, then $\phi(k) = e^{2\pi i \frac{k}{n}} = 1$ $\in \mathbb{Z}$

$\ker \phi = n\mathbb{Z}$, meanwhile $\operatorname{im} \phi = H$

1^{st} iso. theorem: $\dfrac{\mathbb{Z}}{n\mathbb{Z}} \cong H$

↑ $\mathbb{Z}_n$