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

If $z^n = 1$, $|z^n| = 1$, $|z|^n = 1$. Since $|z| \geq 0$, $|z| = 1$

$(e^{i\theta})^n = 1 \iff e^{in\theta} = 1 \iff n\theta = 2\pi k$ for some $k \in \mathbb{Z}$

$\therefore H = \{ e^{i 2\pi k/n} : k \in \mathbb{Z} \}$

Claim: $H < \mathbb{C}^*$ (i) $1 = e^{2\pi i 0/n} \in H$

(ii) If $e^{2\pi i k/n}, e^{2\pi i j/n} \in H$, then $e^{2\pi i k/n}(e^{2\pi i j/n})^{-1} = e^{2\pi i (k-j)/n} \in H$

Define $\phi : \mathbb{Z}_n \to H$ by $\phi([k]_n) = e^{2\pi i k/n}$

$k \equiv j \bmod n \iff n$ divides $k - j \iff \frac{k-j}{n} \in \mathbb{Z} \iff \underbrace{e^{2\pi i k/n}}_{\varphi(k)} = \underbrace{e^{2\pi i j/n}}_{\varphi(j)}$

$\therefore \phi$ is well defined

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

$\therefore \varphi$ is a hom. By inspection ϕ is onto

$\varphi(k) = 1 \iff n$ divides $k \iff k \equiv 0 \bmod n$ $\therefore \phi$ is 1-1 ☺

Alt. proof 1: $H = \langle e^{2\pi i/n} \rangle$ $\left(e^{2\pi i k/n} = (e^{2\pi i/n})^k\right)$

Also $\# H = n$ $\therefore H \cong \mathbb{Z}_n$ by classification of cyclic gps ü

Alt. proof 2: $H = \ker \psi$, where $\psi(z) = z^n$ $(\psi : \mathbb{C}^* \to \mathbb{C}^*)$

$\psi(xy) = (xy)^n = x^n y^n = \psi(x)\psi(y)$ $\therefore H < \mathbb{C}^*$

Define $\alpha : \mathbb{Z} \to H$ by $\alpha(1) = e^{2\pi i/n}$

free

$\alpha(k) = 1 \iff e^{2\pi i k/n} = 1 \iff n \mid k$ $\therefore$ $\ker \alpha = n\mathbb{Z}$

By 1st iso. thm $\operatorname{im} \alpha = H \cong \dfrac{\mathbb{Z}}{\ker \alpha} = \dfrac{\mathbb{Z}}{n\mathbb{Z}} = \mathbb{Z}_n$ ☺

2. Suppose $\alpha = (1,6,2,5,3)(2,6)(4,7,3,5,1,2)$ is a permutation (in cycle notation). What is the order of α? What is the parity of α? Simplify α^{2017}.

$\alpha = \overset{\text{odd}}{(1,2,4,7)}\overset{\text{odd}}{(5,6)}$ disj

Ruffini $\Rightarrow |\alpha| = \text{lcm}(4,2) = 4$

α is even

$2017 \equiv 1 \bmod 4 \quad \therefore \quad 1 \equiv \bmod 2 \quad \therefore \quad \alpha^{2017} = \alpha^1 = \alpha$ ☺

A_n

3. Prove that the set of all even permutations in the symmetric group S_n is a normal subgroup of S_n. Exhibit a subgroup of S_3 that is not normal. Explain.

Direct proof: $A_n < S_n$: (i) $\varepsilon \in A_n$ (0 flips)

(ii) if $\alpha, \beta \in A_n$ then $\alpha = \delta_1 \cdots \delta_k$, $\beta = \tau_1 \cdots \tau_j$ where δ's & τ's are flips, k, j are even

$\alpha\beta^{-1} = \delta_1 \cdots \delta_k \tau_j \cdots \tau_1$. parity $= k + j =$ even $\therefore \alpha\beta^{-1} \in A_n$ ☺

$A_n \triangleleft S_n$: Suppose $\alpha = \delta_1 \cdots \delta_k \in A_n$, $\gamma \in S_n$

Then $\gamma = \delta_1 \cdots \delta_j$, where δ's are flips.

$\gamma\alpha\gamma^{-1} = \delta_1 \cdots \delta_j \, \delta_1 \cdots \delta_k \, \delta_j \cdots \delta_1$ parity $= 2j + k$ = even $\therefore \gamma\alpha\gamma^{-1} \in A_n$

Part 2: Let $H = \langle (1,2) \rangle = \{\varepsilon, (1,2)\}$

$(2,3)(1,2)(2,3) = (1,3$ ... already not in H $\therefore H \ntriangleleft S_n$ $\forall n \geq 3$

Alt. proof: Define $\phi : S_n \to \mathbb{Z}_2$ by $\phi(\alpha) = \begin{cases} 0 & \text{if } \alpha \in A_n \\ 1 & \text{otherwise} \end{cases}$

Let $\alpha, \beta \in A_n$ Cases: $\alpha, \beta \in A_n$ (so $\alpha\beta \in A_n$)

$\phi(\alpha\beta) = 0 = 0 + 0 = \phi(\alpha) + \phi(\beta)$

$\alpha \in A_n$, $\beta \notin A_n$. Then $\alpha\beta \notin A_n$

$\phi(\alpha\beta) = 1 = 0 + 1 = \phi(\alpha) + \phi(\beta)$ (similarly if α & β are switched)

$\alpha \notin A_n$, $\beta \notin A_n$, then $\alpha\beta \in A_n$

$\phi(\alpha\beta) = 0 = 1 + 1 = \phi(\alpha) + \phi(\beta)$

$\therefore \phi$ is a hom. $\therefore H = \ker\phi \triangleleft S_n$ ☺

4. How many group homomorphisms are there from $\mathbf{Z}$ to $\mathbf{Z}_{24}$? How many of them are one-to-one? How many of them are onto? For those that are onto, what is the kernel? Explain.

Since $\mathbb{Z}$ is free, a hom $\phi : \mathbb{Z} \to \mathbb{Z}_{24}$ is uniquely determined by $\phi(1)$ & the choice is free.

$\therefore$ There are 24 homs $\mathbb{Z} \to \mathbb{Z}_{24}$

Since $\mathbb{Z}$ is infinite & $\mathbb{Z}_{24}$ is finite none of the homs is 1-1.

φ is onto $\Leftrightarrow$ $\phi(1)$ generates $\mathbb{Z}_{24}$ $\Leftrightarrow$ $\phi(1)$ is coprime to n

$\therefore$ there are $\varphi(24)$ of them

Euler totient

$$\varphi(24) = \varphi(2^3)\varphi(3) = (2^3 - 2^2)(3-1) = 8$$

1, 5, 7, 11, 13, 17, 19, 23 are coprime to 24

Suppose $k \in \ker \varphi$, then $\varphi(k) \equiv 0 \mod 24$

$$\varphi(k) = \varphi(k \cdot 1) = k\varphi(1) \equiv 0 \mod 24$$

$\therefore$ $24 \mid k\varphi(1)$ but if φ is onto $\varphi(1)$ generates $\mathbb{Z}_{24}$ so $\gcd(\varphi(1), n) = 1$

$\therefore$ $24 \mid k$ $\therefore$ $k \equiv 0 \mod 24$

Conversely $\varphi(24k) = 24\varphi(k) \equiv 0$ in $\mathbb{Z}_{24}$

$\therefore$ $\ker \varphi = 24\mathbb{Z}$

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

Since $\langle a \rangle < G$, By Lagrange's theorem

$|a| = |\langle a \rangle|$ divides n, i.e. $\exists i$ $n = |a| \cdot \underbrace{i}_{\text{\# of cosets of } \langle a \rangle}$

$$a^n = a^{|a| i} = \left(a^{|a|}\right)^i = e^i = e$$ ☺

Since $|a|$ divides n, if n is prime, $|a| = 1$ (so $a = e$)

or $|a| = n$, so $G = \langle a \rangle$

$\therefore$ groups of prime order are simple and cyclic

(no nontrivial proper subgroups)