1. Suppose m and n are natural numbers. Prove that
   (a) any common divisor of m and n divides $\gcd(m, n)$.
   (b) $\mathrm{lcm}(m, n)$ divides any common multiple of m and n.

a) Let d be a common divisor of m, n

Then $\exists m', n'$ $\quad m = m'd \quad n = n'd$

Bézout: $\exists s, t \quad \gcd(m,n) = sm + tn$

$\therefore \gcd(m,n) = sm'd + tn'd = (sm' + tn')d$

$\therefore d$ divides $\gcd(m,n)$ ☺

b) Let d be a common multiple of m, n

Div. Alg: $\exists!\, q, r \quad d = q \cdot \mathrm{lcm}(m,n) + r$

$0 \le r < \mathrm{lcm}(m,n)$

$r = \underline{d} - q \cdot \underline{\mathrm{lcm}(m,n)}$

both common multiples of m, n

$\therefore r$ is a common multiple of m, n

Since $r < \mathrm{lcm}(m,n)$, $r = 0$. ☺

2. Let $\alpha = (1,2,5,4)(2,6,3)(5,6,3,2,1)$ be a permutation (in cycle notation). Express α as a product of disjoint cycles. What is the order of α? Simplify α^{61}.

$$\alpha = \underbrace{(1\ 4)}_{\text{order } 2}\ \cancel{(2)}\ \underbrace{(3\ 6\ 5)}_{\text{order } 3}$$

Ruffini: $|\alpha| = \operatorname{lcm}(2,3) = 6$

$61 \equiv 1 \bmod 6$

$$\alpha^{61} = \alpha^{60+1} = (\underbrace{\alpha^6}_{\varepsilon})^{10} \cdot \alpha = \alpha$$

3. Suppose G is a group and every element, other than the identity, has order 2. Prove G is commutative.

If $g \in G$, $g^2 = e$ (works for e too: $e^2 = e$)

so $g = g^{-1}$

Let $x, y \in G$

In general $\underbrace{x\underbrace{yy^{-1}}_{e}x^{-1}}_{e} = e$

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

Now $xy = (xy)^{-1} = y^{-1}x^{-1} = yx$

4. Suppose G is a multiplicative group, $x \in G$ and n is a natural number. Prove that $x^n = e$ if and only if the order of x divides n.

"$\Leftarrow$" Suppose $|x|$ divides n, then

$\exists\, n'$ $\quad n = n'|x|$

then $\quad x^n = x^{n'|x|} = (\underbrace{x^{|x|}}_{e})^{n'} = e$ ☺

"$\Rightarrow$" Suppose $x^n = e$

Div. alg: $\exists!\, q, r$ $\quad n = q|x| + r$

$\qquad 0 \le r < |x|$

$e = x^n = x^{q|x|+r} = (\underbrace{x^{|x|}}_{e})^q \cdot x^r$

$\therefore x^r = e$, but $r < |x|$ $\quad \therefore r = 0$ ☺

5. Define $\varphi, \psi : \mathbf{C}^* \to \mathbf{C}^*$ by $\varphi(z) = z^5$ and $\psi(z) = |z|$. Prove that φ and ψ are group homomorphisms. Describe and sketch their kernels. Are they cyclic groups? Explain.

$$\phi(zw) = (zw)^5 = z^5 w^5 = \phi(z)\phi(w)$$

($\mathbb{C}^*$ is commutative)

$\therefore \phi$ is a hom.

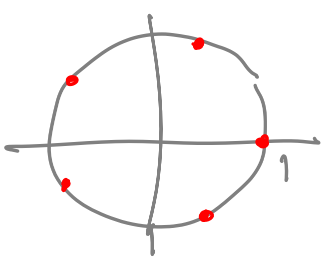
$$\psi(zw) = |zw| = |z||w| = \psi(z)\psi(w)$$

pf: Let $z = re^{i\theta}$, $w = se^{i\beta}$

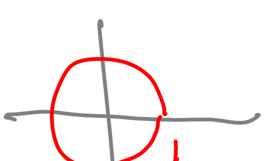
$|zw| = |rse^{i(\theta+\beta)}| = rs = |z||w|$ ◡̈

$\therefore \psi$ is a hom.

$$\ker \phi = \{z \in \mathbb{C}^* : \phi(z) = 1\}$$
$$= \{z \in \mathbb{C}^* : z^5 = 1\}$$
$$= \{5^{\text{th}} \text{ roots of unity}\}$$
$$= \{e^{i\frac{2\pi k}{5}} : k = 0, 1, 2, 3, 4\}$$
$$= \langle e^{i2\pi/5} \rangle \cong \mathbb{Z}_5 \text{ (cyclic)}$$



$$\ker \psi = \{z \in \mathbb{C}^* : \psi(z) = 1\}$$
$$= \{z \in \mathbb{C}^* : |z| = 1\}$$
$$= \{\text{unit circle}\}$$



cyclic groups are $\cong \mathbb{Z}$ or $\mathbb{Z}_m$ for some m

S^1 is uncountable so $\nexists$ a bijection between S^1 and $\mathbb{Z}$ & $\mathbb{Z}_m$, so S^1 is not cyclic ◡̈