1. Suppose m and n are natural numbers. Prove that

   (a) any common divisor of m and n divides $\gcd(m, n)$.

   (b) $\operatorname{lcm}(m, n)$ divides any common multiple of m and n.

Given $n, m \in \mathbb{N}$

a) any common divisor of n & m divides $\gcd(n,m)$

Pf By Bézout $\exists\, s,t \in \mathbb{Z}$ $\gcd(n,m) = sn + tm$

Suppose d is a common divisor of n & m

Then $\exists\, j, k$ s.t. $n = jd$, $m = kd$

So $\gcd(n,m) = sn + tm = sjd + tkd = (sj+tk)d$

$\therefore$ d divides $\gcd(n,m)$ ☺

b) any common multiple of n & m is divisible by $\operatorname{lcm}(n,m)$ $(=\ell)$

Pf Let $a > 0$ be a common multiple of m and n.

Use div. algorithm: $\exists!\, q, r \in \mathbb{Z}$ s.t.

$a = q\ell + r$ and $0 \le r < \ell$

Let $S = \{k > 0 : k \text{ is a common mult. of } n \text{ \& } m\} \subseteq \mathbb{N}$

Since $a \in S$, so $S \neq \phi$, so S has a min

and by def. $\ell = \min S$

$r = \underset{\substack{\uparrow \\ \text{common}}}{a} - q\underset{\substack{\uparrow \\ \text{multiple of } n \text{ \& } m}}{\ell}$ $\therefore$ r is a common multiple of n & m

If $r > 0$, then $r \in S$

But $r < \ell$ ☹

$\therefore$ $r = 0$

$\therefore$ ℓ divides a ☺

2. Suppose H is a subgroup of $\mathbf{Z}$ that contains two distinct primes. Prove that $H = \mathbf{Z}$.

Suppose p, q are primes, $p, q \in H$ and $p \neq q$

then $\gcd(p,q) = 1 = sp + tq$ for some $s, t \in \mathbb{Z}$

Since $p \in H$, $sp \in H$ (e.g. $p \in H \Rightarrow -p \in H$ so $-3p = -p-p-p \in H$)

Similarly $tq \in H$

So $1 = sp + tq \in H$

so $\forall k \in \mathbb{Z}$ $k = k \cdot 1 \in H$ $\therefore$ $H = \mathbb{Z}$ ☺

3. Sketch the subgroup lattice for $\mathbf{Z}_{18}$. For each subgroup, list all the elements and indicate all possible generators of the subgroup.

Divisors of 18 : 1, 2, 3, 6, 9, 18

$\langle 1 \rangle = \mathbb{Z}_{18} = \{0, \underline{1}, 2, 3, 4, \underline{5}, 6, \underline{7}, 8, 9, 10, \underline{11}, 12, \underline{13}, 14, 15, 16, \underline{17}\}$

$\langle 2 \rangle = \{0, \underline{2}, \underline{4}, 6, \underline{8}, \underline{10}, 12, \underline{14}, \underline{16}\}$

$\langle 3 \rangle = \{0, \underline{3}, 6, 9, 12, \underline{15}\}$

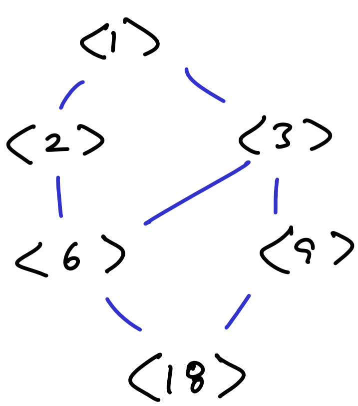
generators underlined

$\langle 6 \rangle = \{0, \underline{6}, \underline{12}\}$

$\langle 9 \rangle = \{0, \underline{9}\}$

$\langle 18 \rangle = \langle 0 \rangle = \{0\}$

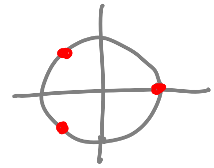
If $k \mid 18$, then m is a generator for $\langle k \rangle \iff \gcd(m, 18) = k$



4. Consider the set of all complex cube roots of unity $H = \{z \in \mathbf{C} \colon z^3 = 1\}$

(a) Show H is a subgroup of the multiplicative group of nonzero complex numbers $\mathbf{C}^*$.

(b) How many elements does H have? List them.



a) Direct proof:

(i) $1^3 = 1$, so $1 \in H$

(ii) Closure: If $z, w \in H$, then $z^3 = w^3 = 1$,

so $(zw)^3 = z^3 w^3 = 1 \cdot 1 = 1$ so $zw \in H$

(iii) Inverses: If $z \in H$, $\underline{z \neq 0}$, so $\exists z^{-1}$

$0^3 = 0 \neq 1$ so $0 \notin H$

Also $z z^{-1} = 1$, so

$(z z^{-1})^3 = 1^3 = 1$, so $z^3 \cdot (z^{-1})^3 = 1$

so $1 \cdot (z^{-1})^3 = 1$ so $(z^{-1})^3 = 1$ so $z^{-1} \in H$

Fancy proof: Define $\varphi : \mathbb{C}^* \to \mathbb{C}^*$ by $\varphi(z) = z^3$

φ is a hom: If $z, w \in \mathbb{C}^*$ $\varphi(zw) = (zw)^3 = z^3 w^3 = \varphi(z)\varphi(w)$

Then $H = \ker \varphi$ so H is a subgroup.

b) If $z \in H$, then $z^3 = 1$ so $|z^3| = |1|$, so $|z|^3 = 1$

Since $|z| > 0$ (in $\mathbb{R}^+$), $|z| = 1$ $\therefore$ $z = e^{i\theta}$

Since $z \in H$ $(e^{i\theta})^3 = 1$, i.e. $e^{i3\theta} = 1$

so $\exists k$ $3\theta = 2\pi k$, so $z = e^{i\theta} = e^{2\pi k i/3}$

$\therefore H = \{ e^{2\pi k i/3} : k \in \mathbb{Z} \}$

$e^{2\pi k i/3} = e^{2\pi j i/3} \iff \dfrac{e^{2\pi k i/3}}{e^{2\pi j i/3}} = 1 \iff e^{2\pi (k-j)/3} = 1 \iff$

$\iff \cancel{2\pi}(k-j)/3 = \cancel{2\pi} n$ for some $n \in \mathbb{Z} \iff 3 \mid k-j \iff k \equiv j \bmod 3$

$\therefore |H| = |\mathbb{Z}_3| = 3$ $H = \{ e^{2\pi k i/3} : k = 0, 1, 2 \} = \{1, e^{2\pi i/3}, e^{4\pi i/3}\}$

5. With H as in the preceding problem, define a function $\varphi\colon \mathbf{Z} \to H$ by $\varphi(k) = e^{2k\pi i/3}$.

(a) Prove that φ is a group homomorphism.

(b) Is φ 1-1? Onto? Explain.

a) If $k, j \in \mathbb{Z}$ $\varphi(k+j) = e^{2\pi(k+j)i/3}$

$= e^{2\pi k i/3} \cdot e^{2\pi j i/3} = \varphi(k) \cdot \varphi(j)$ ☺

b) φ is onto: $1 = \varphi(0)$, $e^{2\pi i/3} = \varphi(1)$, $e^{4\pi i/3} = \varphi(2)$

Since $\mathbb{Z}$ is infinite and H is finite,
By the pigeonhole principle φ is not 1-1.

e.g. $\ker\varphi = \{k : \varphi(k) = 1\} = \varphi^*(\{1\}) = \{0, \pm 3, \pm 6, \pm 9, \ldots\} = 3\mathbb{Z}$

$\varphi^*(\{e^{2\pi i/3}\}) = \{\ldots, -2, 1, 4, 7, \ldots\} = 3\mathbb{Z}+1$

$\varphi^*(\{e^{4\pi i/3}\}) = 3\mathbb{Z}+2$