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.

a) Suppose d divides m & n

Bézout: $\exists\, s, t \in \mathbb{Z}$ $\gcd(m,n) = sm + tn$

Since d divides both sm & tn,

d divides $\gcd(m,n)$ ☺

b) Suppose n & m divide s

Div. alg.: $\exists!\, q, r$ s.t. $s = q\,\operatorname{lcm}(m,n) + r$

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

$r = s - q\,\operatorname{lcm}(m,n)$

Since m, n divide both s and $-q\,\operatorname{lcm}(m,n)$,

m, n divide r

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

2. Sketch the subgroup lattice for $\mathbf{Z}_{28}$. For each subgroup, list all the elements and indicate all possible generators of the subgroup.

Divisors of 28: $1, 2, 4, 7, 14, 28$

$\langle 1 \rangle = \mathbb{Z}_{28} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27\}$

Possible generators (co-prime to 28)

$\langle 2 \rangle = \{0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26\} \cong \mathbb{Z}_{14}$

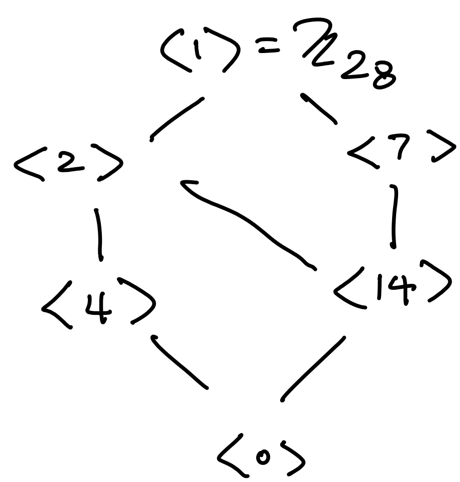
$\langle 4 \rangle = \{0, 4, 8, 12, 16, 20, 24\} \cong \mathbb{Z}_7$

$\langle 7 \rangle = \{0, 7, 14, 21\} \cong \mathbb{Z}_4$

$\langle 14 \rangle = \{0, 14\} \cong \mathbb{Z}_2$

$\langle 28 \rangle = \langle 0 \rangle = \{0\}$

Possible generators (smallest gcd with 28)



3. Find a proper non-trivial normal subgroup of the symmetric group S_n. Find a subgroup of S_n that is not normal. Prove your assertions.

For $n \geq 3$ A_n is a nontrivial proper normal subgroup of S_n

$A_n = \ker \phi$, where $\phi : S_n \to \mathbb{Z}_2$ is the hom. defined by $\phi(\text{even}) = 0$, $\phi(\text{odd}) = 1$

$\langle (1,2) \rangle = \{ \varepsilon, (1,2) \}$ is not normal in S_3

$(1,3)^{-1}(1,2)(1,3) = (1,3)(1,2)(1,3) = (2,3) \notin \langle (1,2) \rangle$

4. Suppose G is a finite group with m elements and $x \in G$. Prove:

(a) x has finite order.

(b) $x^n = e$ if and only if the order of x divides n.

(c) $x^m = e$.

a) By Pigeonhole Principle $\{x^j : j \in \mathbb{Z}\}$ cannot be all distinct, so for some $j \neq k$ $x^k = x^j$

WLOG assume $j < k$, then $x^j = x^k = x^{k-j+j}$
$= x^{k-j} x^j$

$\therefore$ $\underline{x^{k-j} = e}$ $(k-j>0)$

$\therefore$ x has finite order

In fact the order of x is the minimum of $\{j>0 : x^j = e\} \neq \phi$ (min exist by the well-ordering principle)

Let $k = |x| = \min\{j>0 : x^j = e\}$

b) "$\Leftarrow$" if k divides n, $\exists q$ $n = kq$, so

$x^n = x^{kq} = (x^k)^q = e^q = e$ ☺

"$\Rightarrow$" Div. alg.: $\exists! q, r \in \mathbb{Z}$ s.t. $n = kq + r$
& $0 \leq r < m$

Then $r = n - kq$.

$x^r = x^{n-kq} = x^n \cdot (x^k)^{-q} = e \cdot e^{-q} = e$ ☺

Since $r < k$ (minimal pos. power), $r = 0$ ☺

c) $k = |\langle x \rangle|$, so by Lagrange's theorem $k \mid m$,

so by (b) $x^m = e$. ☺

5. Let R be the ring of continuous functions $\mathbf{R} \to \mathbf{R}$ with pointwise operations. Define $\varepsilon\colon R \to \mathbf{R}^2$ by $\varepsilon(f) = [f(0), f(1)]$. Prove that ε is a ring homomorphism. Is ε onto? Is $\ker\varepsilon$ a maximal ideal? Prime ideal?

$\varepsilon(f+g) = [(f+g)(0), (f+g)(1)] = [f(0)+g(0), f(1)+g(1)]$

$= [f(0), f(1)] + [g(0), g(1)] = \varepsilon(f) + \varepsilon(g)$ and similarly for multiplication, so ε is a ring hom

Note: ε is the hom. given by the universal property of product and $\varepsilon_{0,1}$:

$$\begin{tikzcd} & R \arrow[dl, bend right, "\varepsilon_0"'] \arrow[d, "\varepsilon"] \arrow[dr, bend left, "\varepsilon_1"] & \\ \mathbb{R} & \mathbb{R}^2 \arrow[l, "\pi_1"] \arrow[r, "\pi_2"'] & \mathbb{R} \end{tikzcd}$$

Given $[a,b] \in \mathbb{R}^2$ let $f(x) = a + (b-a)x$.

Then $\varepsilon(f) = [f(0), f(1)] = [a,b]$, so ε is onto.

let $g(x) = x$ and $h(x) = 1-x$

then $\varepsilon(g) = [0,1]$ and $\varepsilon(h) = [1,0]$

so neither g nor h $\notin \ker\varepsilon$, but

$\varepsilon(gh) = \varepsilon(x - x^2) = [0,0]$ $\in \ker\varepsilon$

$\therefore$ $\ker\varepsilon$ is not a prime ideal, so not maximal either.

For example, $\ker\varepsilon \subsetneq \ker\varepsilon_0 \subsetneq R$.

Slick proof: By 1st isomorphism theorem

$[1,0]\cdot[0,1] = [0,0]$

$\dfrac{R}{\ker\varepsilon} \cong \text{image}(\varepsilon) = \mathbb{R}^2 \leftarrow$ not an integral domain, so not a field either.

6. Suppose $m, n, k \in \mathbf{N}$ with $\operatorname{lcm}(m, n) = k$. Define a group homomorphism $\varphi\colon \mathbf{Z} \to \mathbf{Z}_m \oplus \mathbf{Z}_n$ by $\varphi(i) = [i \bmod m, i \bmod n]$. Prove that $\ker \varphi = k\mathbf{Z}$. What does the first isomorphism theorem tell you about the image of φ? What can you say about $\mathbf{Z}_m \oplus \mathbf{Z}_n$ if $\gcd(m, n) = 1$?

Let $\pi_m : \mathbb{Z} \to \mathbb{Z}_m$

$\pi_n : \mathbb{Z} \to \mathbb{Z}_n$ be the natural projection.

Universal property of product:

$$\begin{tikzcd}[column sep=small] & \mathbb{Z} \arrow[dl, bend right, "\pi_m"'] \arrow[d, "\exists!\,\phi"] \arrow[dr, bend left, "\pi_n"] & \\ \mathbb{Z}_m & \mathbb{Z}_m \oplus \mathbb{Z}_n \arrow[l, "\pi_1"] \arrow[r, "\pi_2"'] & \mathbb{Z}_n \end{tikzcd}$$

$$\begin{aligned} \ker \varphi &= \{ i : \phi(i) = 0_{\mathbb{Z}_m \oplus \mathbb{Z}_n} \} \\ &= \{ i : [i \bmod m, i \bmod n] = [0, 0] \} \\ &= \{ i : i \equiv 0 \bmod m \ \& \ i \equiv 0 \bmod n \} \\ &= \{ i : m \mid i \ \& \ n \mid i \} \quad \text{(all common multiples of } m, n) \\ &= \{ i : \operatorname{lcm}(m, n) \mid i \} \quad \text{(see midterm 1)} \\ &= \{ i : k \mid i \} = k\mathbb{Z} \end{aligned}$$

1st isomorphism thm: $\dfrac{\mathbb{Z}}{\ker \phi} \cong \operatorname{image}(\varphi)$

$\therefore \operatorname{image}(\varphi) \cong \dfrac{\mathbb{Z}}{k\mathbb{Z}} = \boxed{\mathbb{Z}_k}$

If $\gcd(m, n) = 1$, $k = \operatorname{lcm}(m, n) = mn$

$\underbrace{\operatorname{image}(\phi)}_{k = mn} \subseteq \underbrace{\mathbb{Z}_m \oplus \mathbb{Z}_n}_{mn}$

$\therefore \operatorname{image}(\phi) = \mathbb{Z}_m \oplus \mathbb{Z}_n$ (ϕ is onto)

$\boxed{\therefore \mathbb{Z}_m \oplus \mathbb{Z}_n \cong \mathbb{Z}_{mn}}$

7. Show that the set of all polynomials in $\mathbf{Z}[x]$ with even constant term is a maximal ideal of $\mathbf{Z}[x]$. What is the quotient ring?

Let $I = \{ p \in \mathbb{Z}[x] : \text{const. term is even} \} =$

$= \{ p \in \mathbb{Z}[x] : p(0) \equiv 0 \mod 2 \} = \langle 2, x \rangle$ (so an ideal)

Suppose J is an ideal, $I \subsetneq J$. Then $\exists\, p \in J \setminus I$,

i.e. $p(x) = a_0 + a_1 x + \dots$ with $a_0 = 2k+1$ for some k.

Then $1 = \underbrace{p(x)}_{\in J} - \underbrace{2k - x(a_1 + \dots)}_{\in I \subset J} \in J$ $\quad \therefore J = \mathbb{Z}[x]$

So I is maximal ☺

Since I and $1+I$ (all polynomials with odd const. term) partition $\mathbb{Z}[x]$,

the quotient ring is $\mathbb{Z}_2$. ☺

Slick proof with homs.:

Let $\varepsilon : \mathbb{Z}[x] \to \mathbb{Z}$ be the evaluation hom. $\varepsilon(p) = p(0)$

and $\pi : \mathbb{Z} \to \mathbb{Z}_2$ the projection hom. $\pi(n) = n \mod 2$

Let $\phi : \mathbb{Z}[x] \to \mathbb{Z}_2$ be the composition $\phi = \pi \circ \varepsilon$.

Then $I = \ker \phi$

Pf: $p \in \ker \phi \iff \phi(p) = p(0) \mod 2 = 0 \iff p \in I$ ☺

Since π & ε are onto, ϕ is onto.

By the 1^{st} iso. thm.: $\dfrac{\mathbb{Z}[x]}{I} = \dfrac{\mathbb{Z}[x]}{\ker \phi} \cong \text{image}(\phi) = \mathbb{Z}_2$

Since $\mathbb{Z}_2$ is a field, I is a maximal ideal of $\mathbb{Z}[x]$ ☺