1. Let $m \in \mathbf{N}$ and $m\mathbf{Z} = \{mk \colon k \in \mathbf{Z}\}$. Prove $m\mathbf{Z}$ is an ideal of $\mathbf{Z}$. Conversely, prove that any ideal of $\mathbf{Z}$ is of this form.

(i) $0 = m \cdot 0 \in m\mathbb{Z}$

(ii) Given $x, y \in m\mathbb{Z}$

$\exists k, k'$ $x = mk$, $y = mk'$

$x - y = mk - mk' = m(k-k') \in m\mathbb{Z}$

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

(iii) If $x \in m\mathbb{Z}$, $y \in \mathbb{Z}$, then

$\exists k$ $x = mk$, so $xy = mky \in m\mathbb{Z}$

$\therefore m\mathbb{Z}$ is an ideal of $\mathbb{Z}$.

Conversely suppose $H < \mathbb{Z}$, then by the classification theorem for cyclic groups

H is cyclic, i.e. $H = m\mathbb{Z}$ for some m.

(If $m < 0$, replace m by $-m$)

Direct proof: If $H = \{0\}$, then $H = 0\mathbb{Z}$ ☺. If not,

then $S = \{k \in H : k > 0\} \neq \emptyset$. (If nec. replace k with $-k$)

well ordering principle: $\exists m = \min S$. Let $k \in H$

Div. alg: $\exists!\, q, r$ $k = mq + r$, $0 \le r < m$

$r = \underbrace{k}_{\in H} - \underbrace{mq}_{\in H} \in H$. Since $r < m$, $r \notin S$ $\therefore r = 0$ $\therefore k = mq$

$\therefore H = m\mathbb{Z}$ ☺

2. Suppose $\alpha = (1,6,2,5,3)(4,7,3,5,1,2)(2,6)$ is a permutation (in cycle notation). What is the order of α? What is the parity of α? Express α^{404} as a product of disjoint cycles.

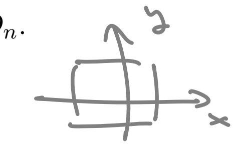
$\alpha = (1\,5\,6\,4\,7)$ $\quad |\alpha| = 5$, α is even

Since $404 = 400 + 4$

$$\alpha^{404} = \alpha^{400}\alpha^{4} = (\underbrace{\alpha^{5}}_{\varepsilon})^{80}\alpha^{4} = \alpha^{4} = \alpha^{-1}$$

$$= (1\,7\,4\,6\,5)$$

3. Prove that the set of all rotations in the dihedral group D_n is a normal subgroup of D_n. Exhibit a subgroup of D_4 that is not normal. Explain.



$\{\text{All rotations}\} = \ker \det \qquad (\det : D_n \to \{1,-1\})$

$\therefore \quad \{\text{all rotations}\} \triangleleft D_n$

Let $F_1 \in D_4$ be the flip $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
(w.r.t x-axis)

$$\langle F_1 \rangle = \left\{ \underbrace{\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}}_{R_0}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \right\}$$

Let $F_2 \in D_4$ be the flip $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
(w.r.t main diagonal)

$$F_2^{-1} F_1 F_2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \underbrace{\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}}_{\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}} = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \notin \langle F_1 \rangle$$

$\therefore \quad \langle F_1 \rangle \not\triangleleft D_4$

4. How many group homomorphisms are there from $\mathbf{Z}$ to $\mathbf{Z}_{40}$? How many of them are one-to-one? How many of them are onto?

Since $\mathbb{Z}$ is a free group on one generator $(\mathbb{Z} = \langle 1 \rangle)$

There is a 1-1 corresp. between homs φ

and elements $\varphi(1) \in \mathbb{Z}_{40}$

The choice of $\varphi(1)$ is free, so there are

40 homs : $\mathbb{Z} \to \mathbb{Z}_{40}$

Given a hom $\varphi : \mathbb{Z} \to \mathbb{Z}_{40}$

$\varphi(1), \varphi(2), \dots \in \mathbb{Z}_{40}$ cannot all distinct

by the pigeonhole principle

$\therefore \exists k \neq j \quad \varphi(k) = \varphi(j) \quad \therefore \varphi$ is not 1-1

$\therefore$ No homs $\mathbb{Z} \to \mathbb{Z}_{40}$ are 1-1.

Given $\varphi : \mathbb{Z} \to \mathbb{Z}_{40}$, $\operatorname{im} \varphi = \langle \varphi(1) \rangle$

(Given $y \in \operatorname{im} \varphi$, $\exists k \quad y = \varphi(k) = k\varphi(1)$)

$\therefore \operatorname{im} \varphi = \mathbb{Z}_{40} \iff \varphi(1)$ generates $\mathbb{Z}_{40}$

$\iff \gcd(\varphi(1), 40) = 1$

$\therefore$ The Number of onto homs $\mathbb{Z} \to \mathbb{Z}_{40}$ is

Euler's totient $= \varphi(40) = \varphi(2^3 \cdot 5)$

$= \varphi(2^3)\varphi(5) = (2^3 - 2^2)(5-1) = 16$

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?

By Lagrange's theorem $|a| = |\langle a \rangle|$ divides $|G|$

$\left(|G| = |\langle a \rangle| \cdot \underbrace{[G : \langle a \rangle]}_{\text{index (call it } q)} \right)$

$\downarrow$

$|a| \cdot q = n$ $\qquad a^n = (a^{|a|})^q = e^q = e$:)

If n is prime, $|a| = 1$ or $|a| = n$

If $|a| = 1$, $a = e$:) $\qquad$ If $|a| = n$, $G = \langle a \rangle$

$\therefore$ Groups of prime order are cyclic and any nontrivial element generates G

$\rightarrow \quad G \cong \mathbb{Z}_n$

(Also G is simple)

6. Let $\mathbf{C}^*$ denote the multiplicative group of nonzero complex numbers. Define $\varphi\colon \mathbf{R} \to \mathbf{C}^*$ by $\varphi(t) = e^{2\pi i t}$. Prove that φ is a group homomorphism. What are its kernel and image? What conclusion can you draw from the First Isomorphism Theorem?

$$\phi(s+t) = e^{2\pi i(s+t)} = e^{2\pi i s + 2\pi i t}$$

$$= e^{2\pi i s} \cdot e^{2\pi i t} = \varphi(s)\varphi(t) \quad \therefore \varphi \text{ is a hom}$$

$$s \in \ker \varphi \iff \phi(s) = 1$$
$$\iff e^{2\pi i s} = 1$$
$$\iff \exists k \quad 2\pi s = 2\pi k$$
$$\iff s \in \mathbb{Z}$$

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

$$z \in \operatorname{im} \varphi \iff \exists s \quad \phi(s) = z$$
$$\iff \exists s \quad e^{2\pi i s} = z$$
$$\iff |z| = 1$$

$$\therefore \operatorname{im} \varphi = S^1 \text{ (unit circle)}$$

$$1^{\text{st}} \text{ iso: } \frac{\mathbb{R}}{\ker \varphi} \cong \operatorname{im} \varphi \qquad \therefore \text{unit circle} \cong \frac{\mathbb{R}}{\mathbb{Z}}$$

7. Suppose F is a field and p is polynomial in $F[x]$ of degree 2 or 3. Prove that p irreducible if and only if p has no roots in F. Give an explicit counter example for degree 4.

p is reducible $\iff$ p has a root in F

If p is reducible, write $p = fg$ where

$\deg f, g \geq 1$ If $\deg p = \deg f + \deg g \leq 3$

One of f and g has deg 1, so has a root,

so p has a root ☺

Conversely suppose $p(a) = 0$

Div. alg.: $\exists!\, q(x), r(x)$ $\quad p(x) = (x-a)q(x) + r(x)$

$r \equiv 0$ or $\deg r < 1$

If $r \equiv 0$, done. If not r is a nonzero const

so $p(x) = (x-a)q(x) + r$

Plug in $x = a$: $\quad 0 = p(a) = 0 \cdot q(a) + r$

$\therefore r \equiv 0$ ☺

For deg 4 let $p(x) = (1+x^2)^2$, then

p is reducible, but has no roots.

8. Let J be the ideal generated by x and 3 in $\mathbf{Z}[x]$. Prove that J is a maximal ideal.

$$J = \{ 3 \cdot p(x) + x \cdot q(x) : p, q \in \mathbb{Z}[x] \}$$
$$= \{ a_0 + a_1 x + \dots + a_n x^n : a_0 \equiv 0 \bmod 3 \}$$

Suppose K is an ideal of $\mathbb{Z}[x]$, $J \subsetneq K$.

Let $p(x) \in K \setminus J$. Then $p(0) \not\equiv 0 \bmod 3$

Then $p(0) = \pm 1 \bmod 3$

Case: $p(0) = -1 \bmod 3$

$\exists k \quad p(0) = -1 + 3k$

$$\underbrace{p(x)}_{\in K} = -1 + 3k + a_1 x + a_2 x^2 + \dots + a_n x^n$$
$$= -1 + \underbrace{3k + x(a_1 + a_2 x + \dots + a_n x^{n-1})}_{\in J \subset K}$$

$\therefore \underbrace{-1}_{\text{unit in } \mathbb{Z}[x]} \in K \quad \therefore K = \mathbb{Z}[x] \quad \therefore J$ is max.

Alt: $\varphi : \mathbb{Z}[x] \xrightarrow{\varepsilon_0} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}_3$ is an onto hom

with $\ker \varphi = J$ $\left[\varphi(p(x)) = \pi(\varepsilon_0(p(x))) = \pi(p(0)) \right.$
$\left. \therefore \varphi(p(x)) = 0 \iff p(0) = 0 \bmod 3 \right]$

$$\frac{\mathbb{Z}[x]}{\langle 3, x \rangle} = \mathbb{Z}_3 \leftarrow \text{field} \quad \therefore J \text{ is max}$$