Proposition: (subgroups of $\mathbb{Z}$) Let $H \leq \mathbb{Z}$.

Then H is cyclic, and either

$H = \langle n \rangle$ where

$n \in \mathbb{N}$ is the smallest natural

number in H or $H = \{0\}$.

proof: Suppose $H \neq \{0\}$. Then $\exists\, m \in \mathbb{Z}$,

$m \in H$ and $m \neq 0$. Since $H \leq \mathbb{Z}$,

so $-m \in H$. Therefore, we may

assume that $H \cap \mathbb{N} \neq \emptyset$.

By the Well-Order Principle,

$\exists\ n \in H \cap \mathbb{N}$ such that

$\forall\ m \in H \cap \mathbb{N},\ n \leq m.$

Then since $H \leq \mathbb{Z}$ and $n \in H$,

$\langle n \rangle \leq H$. Now suppose

$\exists\ k \in H,\ k \notin \langle n \rangle.$

Then by the division algorithm,

$\exists\ q, r \in \mathbb{Z},\ 0 \leq r < n,$

with

$k = nq + r.$

Since $k \in H$ and $nq \in \langle n \rangle \leq H$,

we know

$$k - nq \in H$$

Note $nq \in \langle n \rangle$ since

$$nq = \underbrace{n + n + n + \cdots + n}_{q \text{ times}} \quad \text{if } q > 0$$

or $$-nq = \underbrace{n + n + n + \cdots + n}_{q \text{ times}} \quad \text{if } q < 0.$$

But

$$r = k - nq \in H.$$

We assumed that n was the smallest positive integer in H, and since $0 \leq r < n$, we must have $r = 0$. Therefore, $k = nq \in \langle n \rangle$, so $H = \langle n \rangle$. $\square$

Observation: If $n \in \mathbb{N}$, then in $\mathbb{Z}$, $\langle n \rangle = n\mathbb{Z}$. So by the previous proposition, every subgroup of $\mathbb{Z}$ is of the form $n\mathbb{Z}$ for $n \in \mathbb{N} \cup \{0\}$.

Proposition: (subgroups of $\mathbb{Z}_n$) Let $H \leq \mathbb{Z}_n$. Let $d \in \{1, 2, \dots, n-1\}$ be the smallest positive integer such that $[d] \in H$. Then either $H = \langle d \rangle$ or no such d exists, in which case, $H = \{[0]\}$.

proof: Identical to that for $\mathbb{Z}$, with a bit more care taken with the modulus.

$\square$

Corollary: (subgroups of cyclic groups)

Every subgroup of a cyclic group is cyclic.

proof: Let G be a cyclic group.

Suppose $H \leq G$. Let

$$\varphi : G \to \{\mathbb{Z}, \mathbb{Z}_{|G|}\}$$

be an isomorphism

($\varphi : G \to \mathbb{Z}$ if $|G| = \infty$ and

$\varphi : G \to \mathbb{Z}_{|G|}$ if $|G| < \infty$).

Then $\varphi(H) \leq \varphi(G)$,

Since

$\varphi(H)$ nonempty

1) $e_G \in H$, so

$$0 = \varphi(e_G) \in \varphi(H) \text{ if } |G| = \infty$$

$$[0] = \varphi(e_G) \in \varphi(H) \text{ if } |G| < \infty.$$

$\varphi(H)$ is closed under "+"

2) If $x, y \in \varphi(H)$, then $\exists\ a, b \in H$, $x = \varphi(a)$, $y = \varphi(b)$. Then

$$x + y = \varphi(a) + \varphi(b)$$

$$x + y = \varphi(a \cdot b) \in \varphi(H)$$

Inverses of elements in $\varphi(H)$ are in $\varphi(H)$

3) If $x \in \varphi(H)$, $x = \varphi(a)$ for $a \in H$, then $a^{-1} \in H$ since $H \leq G$, and $x^{-1} = \varphi(a)^{-1} = \varphi(a^{-1}) \in \varphi(H)$

By the subgroup test,

$\varphi(H) \leq \varphi(G)$.

Every subgroup of $\mathbb{Z}$ or $\mathbb{Z}_n$ is cyclic, so $\exists\ x \in \varphi(H)$, $\varphi(H) = \langle x \rangle$. Applying φ^{-1},

$H = \langle \varphi^{-1}(x) \rangle$.

Note: $\forall\ z, y \in \varphi(G)$,

$$\varphi^{-1}(z+y) = \varphi^{-1}(\varphi(a) + \varphi(b))$$

for some $a, b \in G$.

Since φ is an isomorphism,

$$\varphi^{-1}(z+y) = \varphi^{-1}(\varphi(a)+\varphi(b))$$

$$\varphi^{-1}(z+y) = \cancel{\varphi^{-1}}(\cancel{\varphi}(a\cdot b))$$

$$\varphi^{-1}(z+y) = a\cdot b$$

$$\varphi^{-1}(z+y) = \varphi^{-1}(z)\cdot\varphi^{-1}(y)$$ ✓

Therefore, φ^{-1} is an isomorphism onto G, so

$$H = \varphi^{-1}(\varphi(H)) = \varphi^{-1}(\langle x\rangle)$$

But $\varphi^{-1}(\langle x\rangle) = \{\varphi^{-1}(nx) \mid n\in\mathbb{Z}\}$

$$= \{(\varphi^{-1}(x))^n \mid n\in\mathbb{Z}\}$$

□

Corollary: (generators of $\mathbb{Z}_n$) Let $x \in \{1, 2, \dots, n-1\}$. Then $\langle [x] \rangle = \mathbb{Z}_n$ if and only if $\gcd(x, n) = 1$. In particular, if n is prime, every nonzero element is a generator of $\mathbb{Z}_p$!

proof: $\Rightarrow$) If $\langle [x] \rangle = \mathbb{Z}_n$, then $[1] \in \langle [x] \rangle$. If this is so, then $\exists\ m \in \mathbb{N}$,

$$[1] = m[x].$$

Unravelling,

$$1 \equiv mx \pmod{n},$$

So $\exists\ l \in \mathbb{Z}$,

$$1 - mx = ln, \text{ and}$$

$$1 = ln + mx$$

$$\Rightarrow \gcd(n, x) = 1.$$

$\Leftarrow$ Suppose $\gcd(n, x) = 1$.

Then $\exists\ l, m \in \mathbb{Z}$,

$$1 = ln + mx.$$

Then

$$1 - mx = \ell n$$

$$\Rightarrow \quad 1 \equiv mx \pmod{n}$$

$$\Rightarrow \quad [1] = m[x]$$

$$\Rightarrow \quad [1] \in \langle [x] \rangle$$

$\square$

Note: the only generators of $\mathbb{Z}$ are $n=1$ and $n=-1$.