Every subgroup of $\mathbb{Z}$ is cyclic. Because every subgroup of a cyclic group is cyclic. For Problem 13.18, since $5 \in \ker \phi$, $\ker \phi$ is cyclic, 5 as the smallest positive integer is a generator.

Red flags: inputs to ψ are cosets (equivalent classes). We worry that if we call $g \ker \phi$ by a different name, will the output be different?

Proof: FHT

Let's first show that ψ is well-defined.

Let $K = \ker \phi, k \in K$. To give $\psi : gK \mapsto \phi(g)$ a different name, we can write

$$\begin{aligned} \psi : (gk)K \mapsto \phi(gk) \\ &= \phi(g)\phi(k) \text{ since } \phi \text{ is a homomorphism} \\ &= \phi(g)e_H = \phi(g) \end{aligned}$$

So a different name gives us the same answer!

To prove bijectivity, we are going to show that ψ is injective and surjective.

Injective: $\psi(g_1K) = \psi(g_2K) \Rightarrow \phi(g_1) = \phi(g_2) \Rightarrow$

$$\begin{aligned} \phi(g_1^{-1}g_2) &= \phi(g_1^{-1})\phi(g_2) \\ &= \phi(g_1)^{-1}\phi(g_2) \\ &= e_H \end{aligned}$$

Thus, $g_1^{-1}g_2 \in K \Leftrightarrow g_1K = g_2K$.

Surjective: Take $y \in \operatorname{im} \phi$, then $y = \phi(x)$ for some $x \in G$ by definition of image. Then choose $\psi(xK) = \phi(x) = y$.

It remains to show that ψ is a homomorphism:

$$\begin{aligned} \psi(xK *_{G/K} yK) &= \psi(xyK) \\ &= \phi(xy) \\ &= \phi(x) *_H \phi(y) \\ &= \psi(xK) *_H \psi(yK) \end{aligned}$$

Therefore, ψ is an isomorphism. $\square$

Why are quotient groups useful?

Answer: to construct things, *i.e.* $\mathbb{Z}_6$. Also to conceptualize certain complicated construction more easily.

Example. What is this group? $GL_n(\mathbb{R})/SL_n(\mathbb{R})$. Let $\phi : GL_n(\mathbb{R}) \to \mathbb{R}^*$ be the determinant map. Then $\operatorname{im}\phi = \mathbb{R}^*$ since it's surjective. $\ker\phi = SL_n(\mathbb{R})$. Then the 1st isomorphism theorem states, $G/\ker\phi \simeq \operatorname{im}\phi, GL_n(\mathbb{R})/SL_n(\mathbb{R}) \simeq \mathbb{R}^*$. There is also an isomorphism $gSL_n(\mathbb{R}) \mapsto \det g$.

Example. In D_4, $\{\rho_0, \rho_2\}$ is a normal subgroup. The cosets are $\{\rho_1, \rho_3\}, \{\rho_1, \rho_3\}, \{\mu_1, \mu_2\}, \{\delta_1, \delta_2\}$. Because ρ_2 commutes with everything, and ρ_0 does nothing. Then $(\rho_1 N) * (\mu_1 N) = \rho_1\mu_1 N = \delta_1 N$. This is a group of order 4. We can look at the diagonal to identify if it's V_4. So $D_4/N \simeq V_4$.