Note If $G_1, G_2$ are groups and $H_1 \leq G_1$, $H_2 \leq G_2$ are subgroups, then $H_1 \times H_2 \leq G_1 \times G_2$ is a subgroup.

Next, we want to note that if one knows the kernel of a homomorphism, one essentially also knows its image.

**Prop** Suppose $\overline{\phi} : G \longrightarrow H$ is a homomorphism. Then there is an "induced" isomorphism

$$G/\ker(\overline{\phi}) \longrightarrow \text{Im}(\overline{\phi})$$

making

$$\begin{array}{ccc}
G & \xrightarrow{\overline{\phi}} & H \\
\pi \downarrow & & \downarrow \overline{\phi} \\
G/\ker(\overline{\phi}) & \cong & \text{Im}(\overline{\phi})
\end{array}$$

commute, i.e., $\overline{\phi} = \overline{\phi} \circ \pi$.

**Proof.** Let $K = \ker(\overline{\phi})$; this is a normal
Proof. Let $K = \ker(\phi)$; this is a normal subgroup of $G$. Define a function

$$\overline{\phi} = G/K \to \text{Im}(\phi)$$

by

$$\overline{\phi}(gK) = \overline{\phi}(g).$$

This is well-defined: if $g_1K = g_2K$, say $g_1g_1^{-1}e = g_2K$ for $K \in K$, then

$$\overline{\phi}(g_1) = \overline{\phi}(g_2K) = \overline{\phi}(g_2) \overline{\phi}(K) = \overline{\phi}(g_2).e = \overline{\phi}(g_2).$$
* $\bar{\pi}$ is a homomorphism:

$$\bar{\pi} (g_1, g_2, K) = \bar{\pi} (g_1 g_2 K) = \bar{\pi} (g_1 g_2)$$
$$= \bar{\pi} (g_1) \bar{\pi} (g_2) = \bar{\pi} (g_1 K) \bar{\pi} (g_2 K).$$

* $\text{Im}(\bar{\pi}) = \text{Im}(\bar{\pi}):$ this at least is clear.

* $\bar{\pi}$ is injective: we prove

**Lemma.** If $M \xrightarrow{\bar{\pi}} L$ is a homomorphism of groups and $\ker(\bar{\pi}) = \{e\}$ then $\bar{\pi}$ is injective.

**Proof.** Suppose $\bar{\pi}(g_1) = \bar{\pi}(g_2)$. Then

$$\bar{\pi}(g_1) \bar{\pi}(g_2)^{-1} = e,$$

so $\bar{\pi}(g_1 g_2^{-1}) = e$,

so $g_1 g_2^{-1} \in \ker(\bar{\pi}) = \{e\}$, so $g_1 = g_2$. ∎

* $\bar{\pi} \circ \pi = \bar{\pi}:$ \hspace{1cm} $\bar{\pi}(\pi(g)) = \bar{\pi}(g K) = \bar{\pi}(g),$

This proves the proposition. ∎
Corollary Suppose $G$ and $H$ are finite groups and that $|G|$ and $|H|$ have no common factor (i.e., $\gcd = 1$). Then there is no nontrivial homomorphism from $G$ to $H$.

Proof. Suppose $\varphi: G \to H$ is a homomorphism. Then $|G| = |G/\ker(\varphi)| \cdot |\ker(\varphi)|$ by Lagrange; but also $|G/\ker(\varphi)| = |\text{Im}(\varphi)|$, which divides $|H|$ by Lagrange. So $\gcd(|G|, |H|) \geq |\text{Im}(\varphi)|$.

If $\gcd = 1$, then $\text{Im}(\varphi) = \{e\}$. □

So when is there a nontrivial homomorphism $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$?

Suppose $k$ divides both $n$ and $m$. 
Write \( n = ka \) and \( m = kb \).

Then

(i) The image of \( bZ \) in \( Z/mZ \) is isomorphic to \( Z/kZ \).

Proof. We have a homomorphism

\[
bZ \to Z/mZ
\]

with kernel \( mZ \), so its image is isomorphic to \( bZ/mZ \). There is also a homomorphism

\[
Z \to bZ/mZ
\]

given by \( \lambda(b) = cb + mZ \).

Its kernel is

\[
\{ b \in Z \mid b \in mZ \} = kZ,
\]

so \( \text{im}(\lambda) \cong Z/kZ \).
(ii) There is a surjective homomorphism

\[ \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/k\mathbb{Z}. \]

We may define it by taking \( \alpha(l + n\mathbb{Z}) = l + k\mathbb{Z} \).

[Why is it well-defined? We use that \( n = km \).]

Combining (i) and (ii), we get a homomorphism

\[ \mathbb{Z}/a\mathbb{Z} \to \mathbb{Z}/k\mathbb{Z} \cong \mathbb{Z}/(mn)\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}. \]

The image of the composite is isomorphic to \( \mathbb{Z}/k\mathbb{Z} \).

**Cor** \( k \mid (n, m) \iff \) there is a homomorphism \( \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \) with image of order \( k \).
We've noticed by now that if \( n = mq \),
then there is a surjective homomorphism
\[
\frac{\mathbb{Z}}{m\mathbb{Z}} \rightarrow \frac{\mathbb{Z}}{n\mathbb{Z}}
\]
with kernel
\[
\ker(\phi) = m\mathbb{Z}/n\mathbb{Z}, \quad \text{i.e.}
\]
\[
\frac{\mathbb{Z}}{m\mathbb{Z}/n\mathbb{Z}} \cong \frac{\mathbb{Z}}{n\mathbb{Z}}.
\]
This looks like a cancellation rule! And so it is.

**Theorem** Suppose \( N \) and \( K \) are normal subgroups of \( G \) with \( K \leq N \). Then
\[
G/K \cong G/N.
\]

**Proof.** Note that, since \( K \leq N \), we have
\[
KN = N.
\] So, given a coset \( gK \) in \( G \), we may form the coset
\[ gK \times gN \text{ in } G, \text{ and we get} \]
\[ g_1g_2K = g_1g_2N = g_1Ng_2N \]
\[ = g_1K \times g_2K. \text{ So, the function} \]
\[ \overline{\Phi} \colon \frac{G}{K} \rightarrow \frac{G}{N} \]
\[ \text{given by } \overline{\Phi}(gK) = gKN = gN \]
\[ \text{is a homomorphism. It is certainly surjective. If } gK \in \text{ker}\overline{\Phi}, \text{ i.e.} \]
\[ gKN = \overline{\Phi}(gK) = N, \text{ then } g \in N, \]
\[ \text{i.e. } gK \in N/K. \text{ Certainly } N/K \subseteq \text{ker}(\overline{\Phi}), \]
\[ \text{so we conclude that } N/K = \text{ker}(\overline{\Phi}). \]
\[ \text{It now follows from our proposition that} \]
\[ G/N = \text{Im}(\overline{\Phi}) \cong (G/K)/\text{ker}(\overline{\Phi}) = (G/K)/(N/K). \]
Example Consider the dihedral group $D_4$ with elements $1, y, y^2, y^3, x, xy, xy^2, xy^3$ that satisfy $x = x^{-1}$, $xyx^{-1} = y^{-1} = y^3$.

We saw that $K = \langle y^2 \rangle = \{1, y^2\}$ is normal, as is $N = \langle y \rangle$.

Now $D_4/K$ has order $\frac{|D_4|}{|K|} = \frac{8}{2} = 4$.

and its cosets are $K, yK, xK, xyK$ [check!].

$N/K$ consists of cosets $K, yK$.

$D_4/K \times N/K$ has order 2, and is isomorphic to $D_4/N$.

Claim $D_4/K \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and this identifies $N/K$ with $\langle 0, 1 \rangle$. 

m427-wk5 Page 9