Examples of the homomorphism theorem

Example \( SL(2, \mathbb{Z}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a,b,c,d \in \mathbb{Z}, \ ad-bc = 1 \right\} \) 

integer 2x2 matrices with determinant 1

This is a group as \( (a \ b) \begin{pmatrix} 1 & \frac{d}{ad-bc} \\ -c & a \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \)

Another group is \( SL(2, \mathbb{Z}_n) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid [a],[b],[c],[d] \in \mathbb{Z}_n, \ ad-bc = [1] \right\} \)

\( \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \)

There is a homomorphism \( \varphi : SL(2, \mathbb{Z}) \rightarrow SL(2, \mathbb{Z}_n) \)

\( \varphi \left( \begin{pmatrix} a & b \\ c & d \end{pmatrix} \right) = \begin{pmatrix} [a] & [b] \\ [c] & [d] \end{pmatrix} \)

[Exercise: check \( \varphi(AB) = \varphi(A)\varphi(B) \); easy but tedious]

Let \( \overline{G} = \varphi(SL(2, \mathbb{Z})) \leq SL(2, \mathbb{Z}_n) \) be the image of \( \varphi \).

Then \( \varphi : SL(2, \mathbb{Z}) \rightarrow \overline{G} \) is surjective by construction.

What is \( \ker(\varphi) \)? \( \ker(\varphi) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid \begin{pmatrix} [a] & [b] \\ [c] & [d] \end{pmatrix} = \begin{pmatrix} [1] & [0] \\ [0] & [1] \end{pmatrix} \right\} \)

\( = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a \equiv 1, b \equiv 0, c \equiv 0, d \equiv 1 \pmod{n} \right\} =: \Gamma_n \).

The theorem then implies that there is an isomorphism \( \tilde{\varphi} : SL(2, \mathbb{Z})/\Gamma_n \rightarrow \overline{G} \).

Remark: It is a fact that \( \varphi : SL(2, \mathbb{Z}) \rightarrow SL(2, \mathbb{Z}_n) \)

is always surjective and \( \overline{G} = SL(2, \mathbb{Z}_n) \).

So in fact \( SL(2, \mathbb{Z})/\Gamma_n \cong SL(2, \mathbb{Z}_n) \).
Another example: Define $\mathbb{Z}_n \times \mathbb{Z}_m = \{ ([a]_n, [b]_m) \mid [a]_n \in \mathbb{Z}_n, [b]_m \in \mathbb{Z}_m \}$ with the group operation of coordinate-wise addition

$([a]_n, [b]_m) + ([a']_n, [b']_m) := ([a+a']_n, [b+b']_m)$

(\text{Check: this is a group.})

Now suppose $\gcd(n,m) = 1$

Define $\varphi : \mathbb{Z} \to \mathbb{Z}_n \times \mathbb{Z}_m$ \quad $\varphi(x) = ([x]_n, [x]_m)$

$\ker(\varphi) = \{ x : [x]_n = [0]_n \text{ and } [x]_m = [0]_m \} = \{ x : n \mid x \text{ and } m \mid x \}$

$= \{ x : (nm) \mid x \}$ since $\gcd(n,m) = 1$

I.e., $\ker(\varphi) = \langle nm \rangle$. Let $\overline{G} = \varphi(\mathbb{Z})$ be the image of $\varphi$. Then $\varphi : \mathbb{Z} \to \overline{G}$ is surjective, and its kernel is $\langle nm \rangle$

Thus there is an isomorphism $\tilde{\varphi} : \mathbb{Z}/\langle nm \rangle \to \overline{G}$

Now $\mathbb{Z}/\langle nm \rangle = \mathbb{Z}_{nm}$ has $nm$ elements, so $\overline{G}$ has $nm$ elements. But $\mathbb{Z}_n \times \mathbb{Z}_m$ has $nm$ elements, and $\overline{G}$ is a subset. So it must be that $\overline{G} = \mathbb{Z}_n \times \mathbb{Z}_m$, that is the original map $\varphi$ was surjective!

So $\tilde{\varphi} : \mathbb{Z}_{nm} \to \mathbb{Z}_n \times \mathbb{Z}_m$ is an isomorphism

This actually proves the Chinese remainder theorem!
More Theorems about quotient groups.

Theorem: If \( \varphi: G \to \tilde{G} \) is a surjective homomorphism with kernel \( N \), then \( \tilde{\varphi}: G/N \to \tilde{G} \) where \( \tilde{\varphi}(aN) = \varphi(a) \) is an isomorphism.

There is a correspondence of subgroups of \( G/N \) and \( \tilde{G} \), which amounts to

Prop. 2.7.1B: let \( \varphi: G \to \tilde{G} \) be a surjective homomorphism, with kernel \( N \).

(a) There is a bijective correspondence

\[
\{ \text{subgroups of } \tilde{G} \} \leftrightarrow \{ \text{subgroups of } G \text{ containing } N \}
\]

given by

\[ B \mapsto \varphi^{-1}(B) = \{ g \in G \mid \varphi(g) \in B \} \]

(b) This bijection preserves the property of being normal.

i.e., \( B \) is normal in \( \tilde{G} \) \( \iff \) \( \varphi^{-1}(B) \) is normal in \( G \).

Proof: let \( B \leq \tilde{G} \). Then \( \varphi^{-1}(B) \leq G \).

Since \( e \in B \), \( \varphi^{-1}(e) = \ker \varphi = N \) is contained in \( \varphi^{-1}(B) \).

So \( \varphi^{-1}(B) \) is indeed a subgroup containing \( N \).

Conversely, if \( A \leq G \) is a subgroup containing \( N \) \( (N \leq A) \) then \( \varphi(A) \) is a subgroup of \( \tilde{G} \).

So

\[
\{ \text{subgroups of } \tilde{G} \} \leftrightarrow \{ \text{subgroups of } G \text{ containing } N \}
\]

are two maps. We must check they are inverses.

Claim: \( \varphi(\varphi^{-1}(B)) = B \)

Proof:

\[
\varphi(\varphi^{-1}(B)) = \{ \varphi(a) \mid a \in \varphi^{-1}(B) \}
= \{ \varphi(a) \mid \varphi(a) \in B \} = B.
\]
Claim: \( \varphi^{-1}(\varphi(A)) = A \), provided \( N \leq A \).

Let \( x \in \varphi^{-1}(\varphi(A)) \) then \( \varphi(x) \in \varphi(A) \).

So there is \( a \in A \) such that \( \varphi(x) = \varphi(a) \).

Then \( \varphi(a)^{-1}(\varphi(x)) = e \), \( \varphi(a^{-1}x) = e \), so \( a^{-1}x \in N \leq A \).

So \( a^{-1}x = a' \) for some \( a' \in A \). Then \( x = aa' \in A \).

This shows \( \varphi^{-1}(\varphi(A)) \leq A \).

Conversely, if \( a \in A \), then \( \varphi(a) \in \varphi(A) \), so \( a \in \varphi^{-1}(\varphi(A)) \).

Thus \( A \leq \varphi^{-1}(\varphi(A)) \) as well, proving the claim.

This completes the proof of (a).

For (b), let \( K \) be a normal subgroup of \( G \) containing \( N \) \( (N \leq K \triangleleft G) \).

Want to show \( \varphi(K) \triangleleft \overline{G} \). Let \( \overline{g} \in \overline{G} \) be any element, and let \( \varphi(k) \in \varphi(K) \). Need \( \varphi(k) \overline{g} \varphi(k)^{-1} \in \varphi(K) \).

Since \( \varphi \) is surjective, \( \overline{g} = \varphi(g) \) for some \( g \in G \).

So \( \varphi(k) \overline{g} \varphi(k)^{-1} = \varphi(g) \varphi(k) \varphi(g)^{-1} = \varphi(gkg^{-1}) \).

And \( gkg^{-1} \in K \) since \( K \) is normal, so \( \varphi(gkg^{-1}) \in \varphi(K) \), as was to be shown.

Conversely let \( \overline{K} \triangleleft \overline{G} \) be a normal subgroup.

Let \( a \in \varphi^{-1}(\overline{K}) \) and \( g \in G \). Need \( gag^{-1} \in \varphi^{-1}(\overline{K}) \).

So \( \varphi(gag^{-1}) = \varphi(g) \varphi(a) \varphi(g)^{-1} \), and this is in \( \overline{K} \) since \( \varphi(a) \in \overline{K} \) and \( \overline{K} \) is normal. So \( \varphi(gag^{-1}) \in \varphi^{-1}(\overline{K}) \).

Example: What are the subgroups of \( \mathbb{Z}_n \)?

\( \varphi : \mathbb{Z} \rightarrow \mathbb{Z}_n \) is a surjective homomorphism with kernel \( \langle n \rangle \).

\( \varphi(x) = [x]_n \).

So the subgroups of \( \mathbb{Z}_n \) are \( \langle d \rangle \) for \( d \) divides \( n \).

So there are \( \mathbb{Z} / \langle d \rangle \) for \( d \) divides \( n \).
Proposition 2.7.14: Let \( \varphi : G \to \overline{G} \) be a surjective homomorphism with kernel \( N \). Let \( \overline{K} \triangleleft \overline{G} \) be normal and let \( K = \varphi^{-1}(\overline{K}) \) then \( G/K \cong \overline{G}/\overline{K} \).

Since \( \overline{G} \cong G/N \), and \( \overline{K} \cong K/N \), we can also write this as \( G/K \cong (G/N)/(K/N) \).

Proof: Define a homomorphism \( \psi : G \to \overline{G}/\overline{K} \) as
\[
\psi = \overline{\pi} \circ \varphi
\]
where \( G \xrightarrow{\varphi} \overline{G} \xrightarrow{\overline{\pi}} \overline{G}/\overline{K} \)

Then \( \psi \) is surjective since both \( \varphi \) and \( \overline{\pi} \) are surjective. Now
\[
\ker(\psi) = \{ x \in G \mid \psi(x) = e \} = \{ x \in G \mid \overline{\pi}(\varphi(x)) = e \overline{K} \}
\]
\[
= \{ x \in G \mid \varphi(x) \in \overline{K} \} = \varphi^{-1}(\overline{K}) = K
\]
So by the main theorem, there is an isomorphism
\[
\tilde{\psi} : G/K \to \overline{G}/\overline{K}
\]
\[
\tilde{\psi}(x) = \psi(x)
\]

Proposition 2.7.15: Let \( N \triangleleft G \) and \( \varphi : G \to \overline{G} \) a homomorphism with kernel \( K \). If \( N \triangleleft K \), there is a homomorphism \( \overline{\varphi} : G/N \to \overline{G} \) such that \( \overline{\varphi} \circ \overline{\pi} = \varphi \).

Try to prove this yourself, or see textbook. See also Cor. 2.7.16.

Next problem: If \( A \subseteq G \), \( B \subseteq G \), is \( AB = \{ ab \mid a \in A, b \in B \} \) a subgroup of \( G \)? Not necessarily.
Ex. \( G = S_4 \)
\[ A = \langle (12) \rangle = \{ e, (12) \} \]
\[ B = \langle (234) \rangle = \{ e, (234), (243) \} \]

\[ AB = \{ e, (234), (243), (12), (12,34), (12,43) \} \]

Not a subgroup since \((234)(12) = (1342)\) is not in \(AB\)

But if \(N \triangleleft G\) is normal, and \(A \leq G\), then \(AN \leq G\):

Take \(a_1n_1, a_2n_2 \in AN\). Then
\[ a_1n_1a_2n_2 = a_1a_2(a_2^{-1}n_1a_2)n_2 \in AN \]
Since \(N\) is normal

If \(a \in AN\) then \((aN)^{-1} = a^{-1}n^{-1} = a^{-1}(an^{-1}a^{-1}) \subseteq AN\)

Proposition 2.7.19 (Diamond isomorphism theorem)

Let \(N \triangleleft G\), \(A \leq G\). Then \(AN \triangleleft A\) and \(N \triangleleft AN\)
and \(A/AN \cong AN/N\)

Proof:
If \(n \in AN\) and \(a \in A\)
then \(an^{-1}A\) since \(A\) is a subgroup
and \(an^{-1}N\) since \(N\) is normal. So \(AN \triangleleft A\)

If \(n \in N\) and \(g \in AN\) then \(gn^{-1} \in N\) since \(N \triangleleft G\).

Since \(N \triangleleft AN\) there is a surjective homomorphism
\[ \pi : AN \rightarrow AN/N. \]

There is also a homomorphism \(\iota : A \rightarrow AN\), \(\iota(a) = a\).

Then \(\varphi : A \rightarrow AN/N\)
\[ \varphi = \pi \circ \iota \]

is a homomorphism.

It is surjective \((\pi N)\) \(N = aN = \varphi(a)\). For any \(aN \in AN/N\).

The kernel of \(\varphi\) is \(\{ a \in A | \varphi(a) = 1 \} = N\).

So by the main theorem there is an isomorphism \(\varphi : A/AN \rightarrow AN/N.\)