Lecture 14 

## Examples of the homomorphism Theorem

<u>Example</u> $SL(2,\mathbb{Z}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \begin{array}{l} a,b,c,d \in \mathbb{Z} \\ ad-bc = 1 \end{array} \right\}$

integer $2\times 2$ matrices with determinant 1

This is a group as $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \underbrace{\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}}_{\text{integer entries}}$

Another group is

$$SL(2,\mathbb{Z}_n) := \left\{ \begin{pmatrix} [a] & [b] \\ [c] & [d] \end{pmatrix} \middle| \begin{array}{l} [a],[b],[c],[d] \in \mathbb{Z}_n \\ [ad-bc] = [1] \end{array} \right\}$$

$$\begin{pmatrix} [a] & [b] \\ [c] & [d] \end{pmatrix}^{-1} = \begin{pmatrix} [d] & [-b] \\ [-c] & [a] \end{pmatrix}$$

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

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

[ 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 $\varphi : SL(2,\mathbb{Z}) \longrightarrow \overline{G}$ is surjective by construction.

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

$$= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a \equiv 1, b \equiv 0, c \equiv 0, d \equiv 1 \pmod n \right\} =: \Gamma_n .$$

The Theorem then implies that there is an isomorphism

$$\tilde{\varphi} : SL(2,\mathbb{Z})/\Gamma_n \longrightarrow \overline{G}$$

<u>Remark</u>: It is a fact that $\varphi : SL(2,\mathbb{Z}) \longrightarrow SL(2,\mathbb{Z}_n)$ 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 $\mathbb{Z}_n \times \mathbb{Z}_m = \left\{ ([a]_n, [b]_m) \,\middle|\, \begin{matrix} [a]_n \in \mathbb{Z}_n \\ [b]_m \in \mathbb{Z}_m \end{matrix} \right\}$
with the group operation of coordinate-wise addition

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

(Check: this is a group.)

Now suppose $\gcd(n,m)=1$
Define $\varphi : \mathbb{Z} \to \mathbb{Z}_n \times \mathbb{Z}_m$ $\quad \varphi(x) = ([x]_n, [x]_m)$

$$\ker(\varphi) = \{x : [x]_n = [0]_n \text{ and } [x]_m = [0]_m\} = \{x : n|x \text{ and } m|x\}$$
$$= \{x : (nm)|x\} \text{ since } \gcd(n,m)=1$$

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 <u>proves</u> the Chinese remainder theorem!

# More Theorems about quotient groups.

**Main Theorem** if $\varphi : G \to \overline{G}$ is a surjective homomorphism with kernel $N$, then $\tilde{\varphi} : G/N \to \overline{G}$
$\tilde{\varphi}(aN) = \varphi(a)$ is an isomorphism.

There is a correspondence of subgroups of $G/N$ and $\overline{G}$, which amounts to

**Prop. 2.7.B:** Let $\varphi : G \to \overline{G}$ be a surjective homomorphism, with kernel $N$.

(a) There is a bijective correspondence
$$\{\text{subgroups of } \overline{G}\} \longrightarrow \{\text{subgroups of } G \text{ containing } N\}$$
given by
$$B \longmapsto \varphi^{-1}(B) = \{g \in G \mid \varphi(g) \in B\}$$

(b) This bijection preserves the property of being normal.
i.e., $B$ is normal in $\overline{G} \iff \varphi^{-1}(B)$ is normal in $G$.

**Proof**: Let $B \le \overline{G}$. Then $\varphi^{-1}(B) \le G$.
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 $A \le G$ is a subgroup containing $N$ ($N \le A$) then $\varphi(A)$ is a subgroup of $\overline{G}$.

So
$$\{\text{subgroups of } \overline{G}\} \underset{A \mapsto \varphi(A)}{\overset{B \mapsto \varphi^{-1}(B)}{\rightleftarrows}} \{\text{subgroups of } G \text{ containing } N\}$$
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 $\varphi^{-1}(\varphi(A)) \subseteq A$

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

thus $A \subseteq \varphi^{-1}(\varphi(A))$ as well, proving the claim.

This completes the proof of (a).

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

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

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

so $\bar{g}\varphi(k)\bar{g}^{-1} = \varphi(g)\varphi(k)\varphi(g)^{-1} = \varphi(gkg^{-1})$

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

Conversely let $\bar{K} \trianglelefteq \bar{G}$ be a normal subgroup.

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

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

<u>Example</u>: What are the subgroups of $\mathbb{Z}_n$?

$\varphi: \mathbb{Z} \to \mathbb{Z}_n$ is a surjective homomorphism w/ kernel $\langle n \rangle$

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

$\{\text{subgroups of } \mathbb{Z} \text{ containing } \langle n \rangle\} = \{\langle d \rangle \mid d \text{ divides } n\}$

so $\{\text{subgroups of } \mathbb{Z}_n\} = \{\langle [d] \rangle \mid d \text{ divides } n\}$

<u>Proposition 2.7.14</u> 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 $G/K \cong (G/N)/(K/N)$.

<u>Proof</u>: Define a homomorphism $\psi : G \to \overline{G}/\overline{K}$ as $\psi = \overline{\pi} \circ \varphi$ where

$$G \xrightarrow{\varphi} \underbrace{\overline{G} \xrightarrow{\overline{\pi}} \overline{G}/\overline{K}}_{\text{quotient homomorphism for } \overline{G}/\overline{K}}$$

Then $\psi$ is surjective since both $\varphi$ and $\overline{\pi}$ are surjective. Now

$$\ker(\psi) = \{x \in G \mid \psi(x) = e\} = \{x \in G \mid \overline{\pi}(\varphi(x)) = \overline{K}\}$$
$$= \{x \in G \mid \varphi(x) \in \overline{K}\} = \varphi^{-1}(\overline{K}) = K$$

So by the main theorem, there is an isomorphism

$$\tilde{\psi} : G/K \to \overline{G}/\overline{K}$$
$$\tilde{\psi}(x) = \psi(x) \qquad \blacksquare$$

<u>Proposition 2.7.15</u>: Let $N \triangleleft G$ and $\varphi : G \to \overline{G}$ a homomorphism with kernel $K$. If $N \leq K$, there is a homomorphism $\tilde{\varphi} : G/N \to \overline{G}$ such that $\tilde{\varphi} \circ \pi = \varphi$

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

Next problem: If $A \leq G$, $B \leq G$, is $AB = \{ab \mid a \in A, b \in B\}$ a subgroup of $G$? Not necessarily.

<u>Ex</u> $G = S_4$ $\quad A = \langle (12) \rangle = \{e, (12)\}$

$B = \langle (234) \rangle = \{e, (234), (243)\}$

$AB = \{e, (234), (243), (12), (1234), (1243)\}$

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

But if $N \trianglelefteq G$ is normal, and $A \leq G$, then $AN \leq G$:

Take $a_1 n_1, a_2 n_2 \in AN$. Then

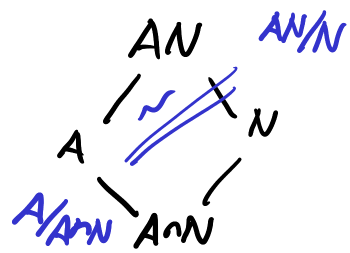
$$a_1 n_1 a_2 n_2 = \underbrace{a_1 a_2}_{\in A} \underbrace{(a_2^{-1} n_1 a_2)}_{\substack{\in N \\ \text{since } N \text{ is normal}}} \underbrace{n_2}_{\in N} \in AN$$

If $an \in AN$ then $(an)^{-1} = n^{-1}a^{-1} = \underbrace{a^{-1}}_{\in A}\underbrace{(an^{-1}a^{-1})}_{\in N} \in AN$

<u>Proposition 2.7.19</u> (Diamond isomorphism theorem)

Let $N \trianglelefteq G$, $A \leq G$. Then $A \cap N \trianglelefteq A$ and $N \trianglelefteq AN$

and $A/A\cap N \cong AN/N$




<u>Proof</u> if $n \in A \cap N$ and $a \in A$

- then $ana^{-1} \in A$ since $A$ is a subgrp

and $ana^{-1} \in N$ since $N$ is normal. So $A \cap N \trianglelefteq A$

If $n_1 \in N$ and $g = an_2 \in AN$ then $gn_1g^{-1} \in N$ since $N \trianglelefteq G$.

Since $N \trianglelefteq AN$ there is a surjective homomorphism

$$\pi : AN \to AN/N.$$

There is also a homomorphism $i : A \to AN$, $i(a) = a$.

Then $\varphi : A \to AN/N$ $\quad \varphi = \pi \circ i$ is a homomorphism.

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

The kernel of $\varphi$ is $\{a \in A \mid aN = N\} = \{a \in A \mid a \in N\} = A \cap N$

So by the main theorem there is an isomorphism $\tilde{\varphi} : A/A\cap N \to AN/N$.