7. Quotient groups III

We know that the kernel of a group homomorphism is a normal subgroup. In fact the opposite is true, every normal subgroup is the kernel of a homomorphism:

Theorem 7.1. *If H is a normal subgroup of a group G then the map*

$$\gamma\colon G \longrightarrow G/H \qquad \text{given by} \qquad \gamma(x) = xH,$$

is a homomorphism with kernel H.

Proof. Suppose that x and $y \in G$. Then

$$\begin{aligned} \gamma(xy) &= xyH \\ &= xHyH \\ &= \gamma(x)\gamma(y). \end{aligned}$$

Therefore γ is a homomorphism.

$eH = H$ plays the role of the identity. The kernel is the inverse image of the identity.

$$\gamma(x) = xH = H$$

if and only if $x \in H$. Therefore the kernel of γ is H. □

If we put all we know together we get:

Theorem 7.2 (First isomorphism theorem)**.** *Let $\phi\colon G \longrightarrow G'$ be a group homomorphism with kernel K. Then $\phi[G]$ is a group and*

$$\mu\colon G/H \longrightarrow \phi[G] \qquad \text{given by} \qquad \mu(gH) = \phi(g),$$

is an isomorphism.

If $\gamma\colon G \longrightarrow G/H$ is the map $\gamma(g) = gH$ then $\phi(g) = \mu\gamma(g)$.

The following triangle summarises the last statement:

$$\begin{tikzcd} G \arrow[r, "\phi"] \arrow[d, "\gamma"'] & G' \\ G/H \arrow[ur, "\mu"'] & \end{tikzcd}$$

Example 7.3. *Determine the quotient group*

$$\frac{\mathbb{Z}_3 \times \mathbb{Z}_7}{\mathbb{Z}_3 \times \{0\}}$$

Note that the quotient of an abelian group is always abelian. So by the fundamental theorem of finitely generated abelian groups the quotient is a product of abelian groups.

Consider the projection map onto the second factor $\mathbb{Z}_7$:

$$\pi\colon \mathbb{Z}_3 \times \mathbb{Z}_7 \longrightarrow \mathbb{Z}_7 \qquad \text{given by} \qquad (a, b) \longrightarrow b.$$

This map is onto and the kernel is $\mathbb{Z}_3 \times \{0\}$. So by the first isomorphism theorem the quotient group is isomorphic to the image which is $\mathbb{Z}_7$.

Theorem 7.4. *Let H be a subgroup of a group G.*

The following are equivalent:

(1) $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$.
(2) $gHg^{-1} = H$ for all $g \in G$.
(3) $gH = Hg$.

Proof. Suppose that (1) holds. Then

$$gHg^{-1} = \{\, ghg^{-1} \,|\, h \in H \,\} \subset H,$$

for any $g \in G$.

To prove (2) we have to establish that the RHS is a subset of the LHS. Pick $h \in H$. Then

$$g^{-1}hg \in H,$$

as we assuming (1), applied to the element $g^{-1} \in G$. Thus $g^{-1}hg = h_1$ for some $h_1 \in H$. Multiplying on the left by g and on the right by g^{-1} we get

$$h = gh_1g^{-1} \in gHg^{-1}.$$

Thus the RHS is a subset of the LHS and (2) holds.

Now suppose that (2) holds. We have to show that $gH = Hg$. We first show that the LHS is a subset of the RHS. Pick $x \in gH$. Then $x = gh$, for some $h \in H$. We have

$$xg^{-1} = ghg^{-1} \in gHg^{-1} = H,$$

so that $xg^{-1} = h_1 \in H$. But then $x = h_1g \in Hg$. Thus the LHS is a subset of the RHS. By symmetry the RHS is a subset of the LHS. Thus (3) holds.

Finally suppose that (3) holds. Pick $g \in G$ and $h \in H$ and let $x = ghg^{-1}$. Then

$$gh \in gH = Hg$$

so that $gh = h_1g \in Hg$, for some $h_1 \in H$. But then

$$x = ghg^{-1} = h_1gg^{-1} = h_1 \in H.$$

Thus (1) holds. $\square$

Corollary 7.5. *If G is abelian then every subgroup is normal.*

Proof. Suppose that H is a subgroup of G. If $h \in H$ and $g \in G$ then

$$ghg^{-1} = gg^{-1}h = h \in H.$$

Thus (1) of (7.4) holds. Therefore (3) holds and so H is normal. $\square$

Definition-Lemma 7.6. *An **automorphism** of G is an isomorphism $\phi \colon G \longrightarrow G$.*

Fix $g \in G$. Then the map

$$i_g \colon G \longrightarrow G \qquad \text{given by} \qquad a \longrightarrow gag^{-1}$$

*is an automorphism of G, called an **inner automorphism**.*

Proof. We have to check that i_g is a group homomorphism and that i_g is a one to one correspondence.

Suppose that a and $b \in G$. We have

$$\begin{aligned} i_g(ab) &= g(ab)g^{-1} \\ &= ga(g^{-1}g)bg^{-1} \\ &= (gag^{-1})(gbg^{-1}) \\ &= i_g(a)i_g(b). \end{aligned}$$

Thus i_g is a homomorphism.

There are two ways to check that i_g is a one to one correspondence.

To check that i_g is one to one, we just have to check that the kernel is trivial. Suppose that $a \in \operatorname{Ker} i_g$. Then

$$gag^{-1} = i_g(a) = e.$$

Multiplying on the left by g^{-1} and on the right by g we get

$$a = g^{-1}eg = e.$$

Thus the kernel is trivial and i_g is one to one.

Now we check that i_g is onto. Suppose that $b \in G$. Let $a = g^{-1}bg \in G$. Then

$$\begin{aligned} i_g(a) &= gag^{-1} \\ &= g(g^{-1}bg)g^{-1} \\ &= b. \end{aligned}$$

Thus i_g is onto. It follows that i_g is an automorphism.

Here is another way to show that i_g is an automorphism. Let's try to write down the inverse map. We guess that the inverse of i_g is $i_{g^{-1}}$.

We check

$$\begin{aligned}
i_{g^{-1}}(i_g(a)) &= i_{g^{-1}}(gag^{-1}) \\
&= g^{-1}(gag^{-1})g \\
&= (g^{-1}g)a(g^{-1}g) \\
&= a.
\end{aligned}$$

Thus the composition one way is the identity. If we replace g by g^{-1} we see that the composition the other way is the identity. It follows that i_g is an automorphism. $\square$