Quotient Groups and the Isomorphism Theorem

AMP Day 8

Jonathan Alcaraz

Here's a warm up proof following up on the stuff we discussed yesterday.

Lemma(?): Let $H \leqslant G$ and $x \in G$. Then

$$xH = xhH$$

for any $h \in H$.

> Let $y \in xhH$. Then $y = xhh_1$ for some $h_1 \in H$. Since H is a subgroup, $hh_1 \in H$, so $y \in xH$.
>
> Let $z \in xH$. Then $z = xh_2$ for some $h_2 \in H$. In particular, $z = xhh^{-1}h_2$. Since H is a subgroup, then $h^{-1}h_2 \in H$, so $z \in xhH$.

Let G be a group and $H \leqslant G$ a subgroup. The set of cosets is denoted by:

$$G/H = \{xH \,:\, x \in G\}$$

By the conjectures Mike discussed yesterday, if G is finite, then $|G/H| = |G|/|H|$. We can try to define a binary operation on G/H by

$$(xH)(yH) = (xy)H\,.$$

However, this would not be well-defined. We can explore specific counter-examples in the exercises, let's observe the main obstruction. If $y_1H = y_2H$, then $y_2 = y_1h$ for some $h \in H$. So $(xy_1)H = (xy_2h)H = (xy_2)H$. We might start to think this means the operation is well-defined, but if $x_1H = x_2H$, then $x_1 = x_2h$ for some $h \in H$. So $x_1yH = x_2hyH$, but there is no way to get the h out.

Definition
Let G be a group and $N \trianglelefteq G$ a normal subgroup. The set G/N with the operation given above forms a group called the **quotient group** of G by N.

This is a definition, but we're also claiming that this thing is actually a group. Here's a proof of this claim.

> WELL-DEFINED:Let $x_1, y \in G$ and $x_2 \in G$ such that $x_1N = x_2N$. We need to show that $x_1yN = x_2yN$. Since $x_1N = x_2N$, then in particular, $x_1 = x_2n$ for some $n \in N$. So
>
> $$x_1yN = x_2nyN$$

Since N is normal, then $Ny = yN$, so $ny = y\tilde{n}$ for some $\tilde{n} \in N$. So

$$x_2 nyN = x_2 y\tilde{n}N = x_2 yN$$

ASSOCIATIVITY: This follows from the fact that the operation on G is associative.

IDENTITY: The identity element in G/N is $eH = H$. Indeed:

$$(eN)(gN) = (eg)N = gN$$

and

$$(gN)(eN) = (ge)N = gN$$

INVERSES: Given $gN \in G/N$, the inverse element is $(g^{-1})N$. Indeed

$$(gN)(g^{-1}N) = (gg^{-1})N = eN$$

and

$$(g^{-1}N)(gN) = (g^{-1}g)N = eN$$

Let's see some examples:

Example

Consider the subgroup $N_2 = \{0, 3\} \leqslant \mathbb{Z}_6$ Recall that any subgroup of an abelian group is normal. Let's look at $\mathbb{Z}_6/N_2$. First of all, what are the cosets of N_2?

$$\{0 + N_2, 1 + N_2, 2 + N_2\}$$

We propose $\mathbb{Z}_6/N_2 \cong \mathbb{Z}_3$. Indeed,

$$\begin{aligned} \varphi\colon \mathbb{Z}_3 &\to \mathbb{Z}_6/N_2 \\ k &\mapsto k + N_2 \end{aligned}$$

is an isomorphism.

Definition

Given a normal subgroup $N \trianglelefteq G$, the **quotient map** is defined by

$$\begin{aligned} \pi \colon G &\to G/N \\ g &\mapsto gN \end{aligned}$$

Yesterday, we showed that the kernel of any homomorphism is normal. Which means we can take a quotient group of the domain by the kernel. Well, we get a dope fact:

The First Isomorphism Theorem If $\varphi \colon G \to H$ is a homomorphism, then there exists an injective homomorphism $\tilde{\varphi} \colon G/\ker(\varphi) \to H$ such that $\varphi = \tilde{\varphi} \circ \pi$. Moreover, if φ is surjective, then $\tilde{\varphi}$ is an isomorphism.

Let $K = \ker(\varphi)$. The picture you should have here is:

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "\pi"] & H \\ G/K \arrow[ur, dashed, "\tilde{\varphi}"] & \end{tikzcd}$$

but we need to cook up $\tilde{\varphi}$ ourselves. Let's give it a shot.

Define

$$\begin{aligned} \tilde{\varphi} \colon G/K &\to H \\ gK &\mapsto \varphi(g)\,. \end{aligned}$$

Now, there is a question whether this is even well-defined. This is where the magic happens. Suppose $g_1K = g_2K$. In particular, $g_1 = g_2k$ for some $k \in K$. So

$$\begin{aligned} \tilde{\varphi}(g_1K) &= \varphi(g_1) \\ &= \varphi(g_2k) \\ &= \varphi(g_2)\varphi(k) \\ &= \varphi(g_2) \\ &= \tilde{\varphi}(g_2K)\,. \end{aligned}$$

To prove that $\tilde{\varphi}$ is injective, recall that a homomorphism is injective if and only if it has trivial kernel. Suppose $gK \in \ker(\tilde{\varphi})$. We want to show that gK is secretly the trivial element. Indeed,

$$\tilde{\varphi}(gK) = \varphi(g) = e_H\,,$$

so $g \in K$ and hence $gK = eK$.

In the case where φ is surjective, then for any $h \in H$, there is some $g \in G$ such that $\varphi(g) = h$. In particular,

$$\tilde{\varphi}(gK) = \varphi(g) = h$$