Section 14: Quotient Groups and Section 15: Simple Groups

Definition 0.1. A subgroup H of a group G is called a **normal** subgroup if, for any $g \in G$ and $h \in H$, $ghg^{-1} \in H$.

Definition 0.2. Let G be a group and let H be a normal subgroup of G. Then, the set of distinct cosets of H, denoted by G/H, is called the **quotient group** of G by H. The binary operation is defined by $(aH)(bH) = (ab)H$.

Example 0.3. Let G be any group. Show that $\{e\}$ is a normal subgroup. What is $G/\{e\}$?

To show $\{e\}$ is normal, we just need to show that $geg^{-1} \in \{e\}$ for any $g \in G$, but $geg^{-1} = e$, so $\{e\}$ is normal. Then, $G/\{e\}$ is the set of cosets of $\{e\}$, but for any element $g \in G$, the coset $g\{e\} = \{g\}$, so each element g determines the unique coset $\{g\}$. Hence, $G/\{e\}$ is just G, because the set of cosets is exactly the set of elements in G.

Show that G is a normal subgroup. What is G/G?

G is a normal subgroup of G because, for any $g, h \in G$, $ghg^{-1} \in G$. G/G is the set of cosets of G, but there is only one coset G, so G/G consists of a single element, which is the identity in the group, so $G/G \cong \{e\}$.

Here's where we ended last time:

Proposition 0.4. *Let H be a normal subgroup of G. The function $\phi : G \to G/H$ given by $\phi(a) = aH$ is an onto homomorphism with $\ker \phi = H$.*

Proof. This is a homomorphism because $\phi(ab) = abH = (aH)(bH) = \phi(a)\phi(b)$. It is onto because, given any coset aH, then $\phi(a) = aH$. Finally, because $H = eH$ is the identity in G/H, $\ker \phi = \{a \mid \phi(a) = H\}$, so $\ker \phi = \{a \mid aH = H\}$. But, $aH = H$ if and only if $a \in H$, so $\ker \phi = H$. □

Theorem 0.5. *Let $\phi : G \to G'$ be any homomorphism. Then, $G/\ker \phi \cong \phi[G]$.*

Proof. Let $H = \ker \phi$ and define the map $\mu : G/H \to \phi[G]$ by $\mu(aH)\phi(a)$. This is well defined, because if b is another element $b \in aH$, then $b = ah$ for some $h \in H = \ker \phi$. Then, $\mu(bH) = \phi(b) = \phi(ah) = \phi(a)\phi(h) = \phi(a) = \mu(aH)$. This is a homomorphism because ϕ is a homomorphism, so for any $a, b \in G$, $\mu(abH) = \phi(ab) = \phi(a)\phi(b) = \mu(aH)\mu(bh)$. This is also one-to-one: if $\mu(aH) = \mu(bH)$, then $\phi(a) = \phi(b)$, so $\phi(a^{-1}b) = e$, hence $a^{-1}b \in H$. Therefore, $b \in aH$, so $aH = bH$. Finally, it is onto because, for any $g \in \phi[G]$, $g = \phi(a)$ for some $a \in G$, hence, $\mu(aH) = \phi(a) = g$. Therefore, $G/\ker \phi \cong \phi[G]$.

In fact, we can say even more: let $\psi : G \to G/\ker \phi$ be the homomorphism in the previous proposition. Then, $\phi = \mu \circ \psi$, because $\phi(a) = \mu \circ \psi(a) = \mu(aH) = \phi(a)$. □

Example 0.6. Show that $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}_6$.

We can define a homomorphism $\phi : \mathbb{Z} \to \mathbb{Z}_6$ by $\phi(n) = n \mod 6$. This is onto, so $\phi[\mathbb{Z}] = \mathbb{Z}_6$, and the kernel is all elements n such that $n = 0 \mod 6$, so $\ker \phi = 6\mathbb{Z}$. Therefore, the previous theorem says $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}_6$.

Example 0.7. If G_1 and G_2 are groups, let $H = \{(g_1, e_2) \mid g_1 \in G_1\}$. Show that H is a normal subgroup of $G_1 \times G_2$. Show that $G_1 \times G_2/H$ is isomorphic to G_2.

We study $G_1 \times G_2/H$. We define a homomorphism $\psi : G_1 \times G_2 \to G_2$ by $\psi(g_1, g_2) = g_2$. You can (and should!) check that this is an onto homomorphism. What is the kernel? We know $\ker \psi = \{(g_1, g_2) \mid \psi(g_1, g_2) = e_2\}$, so $\ker \psi = H$. But, kernels are *always* normal subgroups, so this proves that H is a normal subgroup. Therefore, the previous theorem shows that $G_1 \times G_2/H$ is isomorphic to G_2.

The previous examples indicate that many groups have normal subgroups. Groups that do not are special!

Definition 0.8. A group G is **simple** if it has no proper nontrivial normal subgroups.

Example 0.9. If p is prime, $\mathbb{Z}_p$ is simple because it has no proper nontrivial subgroups (by Lagrange's Theorem!). If p is not prime, $\mathbb{Z}_n$ has a proper nontrivial subgroup for each divisor $d \neq 1, n$ of n. Because $\mathbb{Z}_n$ is abelian, each of these subgroups is normal, so $\mathbb{Z}_n$ is not simple.