Math 403 Chapter 10: Homomorphisms

1. **Introduction:** If quotient groups are useful then any way of obtaining or understanding them is also useful. We will see that mappings which are similar to, but weaker than, isomorphisms, correspond to quotient groups.

2. **Homomorphisms:**

   (a) **Definition:** A *homomorphism* ϕ from a group G to a group H is a mapping $\phi : G \to H$ which satisfies $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in G$.

   In other words it's as if we take an isomorphism and remove the 1-1 and onto requirements.

   It turns out that as with an isomorphism we must have $\phi(e) = e$ (as we'll see) but because we've eliminated the 1-1 requirement we may have other things mapping to e, too. From this arises the following essential definition:

   (b) **Definition:** The *kernel* of a homomorphism $\phi : G \to H$ is the set:

   $$\text{Ker}\phi = \{g \in G \mid \phi(g) = e\}$$

   Example: The mapping $\phi : GL_2\mathbb{R} \to \mathbb{R}^*$ given by $\phi(M) = \det(M)$ is a homomorphism with $\text{Ker}\phi = SL_2\mathbb{R}$.

   Example: The mapping $\phi : \mathbb{Z} \to \mathbb{Z}_n$ given by $\phi(x) = x \bmod n$ is a homomorphism with $\text{Ker}\phi = \langle n \rangle$.

   Example: The mapping $\phi : \mathbb{R}^* \to \mathbb{R}^*$ given by $\phi(x) = x^2$ is a homomorphism with $\text{Ker}\phi = \{-1, 1\}$.

3. **Definition of the Inverse:** Due to the lack of surjectivity and injectivity the inverse of a homomorphism is usually not a mapping. However we can still define, for $h \in H$ and $H' \leq H$:

$$\phi^{-1}(h) = \{g \in G \mid \phi(g) = h\}$$
$$\phi^{-1}(H) = \{g \in G \mid \phi(g) \in H\}$$

4. **Theorem (Properties of Homorphisms):** Let $\phi : G \to H$ be a homomorphism and let $g \in G$ and $G' \leq G$. Then we have:

   (a) $\phi(e) = e$.

   (b) $\phi(g^n) = \phi(g)^n$.

   (c) If $|g|$ is finite then $|\phi(g)|$ divides $|g|$.

   (d) $\text{Ker}\phi \leq G$.

   (e) $\phi(a) = \phi(b)$ iff $a\text{Ker}\phi = b\text{Ker}\phi$.

   (f) If $\phi(g) = h$ then $\phi^{-1}(h) = g\text{Ker}\phi$.

   (g) $\phi(G') \leq H$.

   (h) If G' is cyclic then $\phi(G')$ is cyclic.

   (i) If G' is Abelian then $\phi(G')$ is Abelian.

   (j) If $G' \triangleleft G$ then $\phi(G') \triangleleft \phi(G)$.

   (k) If $|\text{Ker}\phi| = n$ then ϕ is an n-1 mapping from G onto $\phi(G)$.

   (l) If G' is finite then $|\phi(G')|$ divides $|G'|$.

   (m) If $H' \leq H$ then $\phi^{-1}(H') \leq G$.

   (n) If $H' \triangleleft H$ then $\phi^{-1}(H') \triangleleft G$.

   (o) If ϕ is onto and $\text{Ker}\phi = \{e\}$ then ϕ is an isomorphism.

   Proof: Many of the proofs are similar to those for an isomorphism or are straightforward and so we'll omit those and focus on the ones which are not.

   (c) If $|g| = n$ then we have $\phi(g)^n = \phi(g^n) = \phi(e) = e$ and so $|\phi(g)|$ divides n.

   (d) If $a, b \in \text{Ker}\phi$ then $\phi(ab^{-1}) = \phi(a)\phi(b)^{-1} = e$ so the kernel is a subgroup by the one-step subgroup test.

   (e) We have $\phi(a) = \phi(b)$ iff $\phi(ab^{-1}) = \phi(a)\phi(b)^{-1} = e$ iff $ab^{-1} \in \text{Ker}\phi$ iff $a\text{Ker}\phi = b\text{Ker}\phi$ by an earlier theorem.

   (f) Assume $\phi(g) = h$. We show the double inclusion:
   $\phi^{-1}(h) \subseteq g\text{Ker}\phi$: If $x \in \phi^{-1}(h)$ then $\phi(x) = h$ and so $\phi(x) = h = \phi(g)$ and then by (e) we have $x\text{Ker}\phi = g\text{Ker}\phi$ and since $x \in x\text{Ker}\phi$ we have $x \in g\text{Ker}\phi$.
   $g\text{Ker}\phi \subseteq \phi^{-1}(h)$: If $gk \in g\text{Ker}\phi$ then $\phi(kg) = \phi(k)\phi(g) = eh = h$ and so $gk \in \phi^{-1}(h)$.

   (j) Let $\phi(g') \in \phi(G')$ and let $\phi(g) \in \phi(G)$. Then $\phi(g)\phi(g')\phi(g)^{-1} = \phi(gg'g^{-1}) \in \phi(G')$ since $G' \triangleleft G$ and so $\phi(G') \triangleleft \phi(G)$ by the normal subgroup test.

   (k) Follows from (f) and the fact that all cosets have the same size.

   (l) Consider that $\phi_{G'} : G' \to phi(G')$ is a surjective homomorphism. By (k) we know that this $\phi_{G'}$ is a $|\text{Ker}\phi_{G'}|$-1 mapping and so $|G'| = |\text{Ker}\phi_{G'}| \cdot |\phi(G')|$ so that $|\phi(G')|$ divides $|G'|$ and since $|G'|$ divides $|G|$ we have our result.

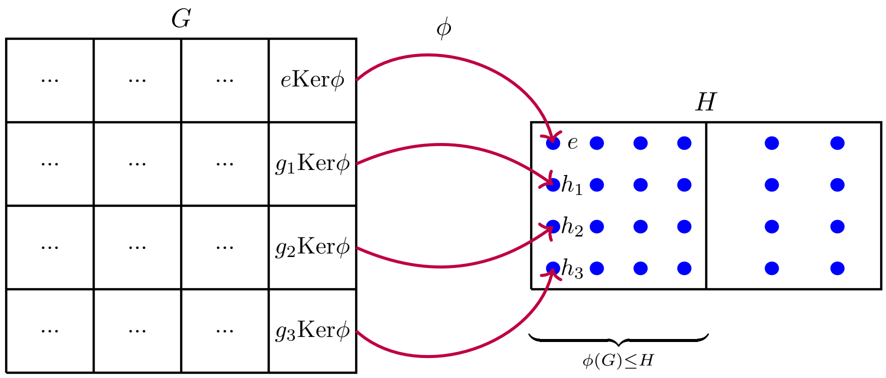
   (o) We only need to show that ϕ is 1-1. In light of that suppose $\phi(g_1) = \phi(g_2)$, then $\phi(g_1 g_2^{-1}) = \phi(g_1)\phi(g_2)^{-1} = e$ so that $g_1 g_2^{-1} \in \text{Ker}\phi = \{e\}$ and so $g_1 = g_2$.

Intuition: The intuition here is that structures are preserved but orders are not, and orders generally shrink to a divisor of the original order. This can be seen in (c), (k), (l). In addition the kernel gives us a wealth of information about the homomorphism - it tells us the "shrink factor" and (d),(e) give us information about what happens to things not in the kernel.

This can be thought of as follows: If we divide G into cosets of Kerϕ then each coset is mapped to a single element in H.

To see this note that the coset eKerϕ is mapped to $e \in H$. For another coset, say g_0Kerϕ, note that if $g \in g_0$Kerϕ then $g = g_0 k$ for some $k \in$ Kerϕ in which case $\phi(g) = \phi(g_0 k) = \phi(g_0)\phi(k) = \phi(g_0)e = \phi(g_0)$ so the entire of g_0Kerϕ goes to the element that g_0 goes to. Moreover if $\phi(g) = \phi(g_0)$ then $\phi(gg_0^{-1}) = e$ and so $gg_0^{-1} \in$ Kerϕ and so $gg_0^{-1} = k$ for some $k \in$ Kerϕ and so $g = g_0 k$ and so $g \in g_0$Kerϕ so that g_0Kerϕ is all that is mapped to $\phi(g_0)$.

What is happening can be illustrated by this picture:



On the left all of G has been subdivided to cosets of Kerϕ. Each coset consists of $|\text{Ker}\phi|$ elements (since they are all the same size) and each coset (all elements in it) is matched to a single to an element in H. Some elements in H are possibly missed since ϕ is not necessily onto and so really the mapping is to $\phi(G) \leq H$.

5. **Connection to Isomorphisms:**

   (a) **Theorem:** If $\phi : G \to H$ is a homomorphism then $\text{Ker}\phi \lhd G$.
   Proof: The fact that it's a subgroup is (d) above. The fact that it's normal follows from (n) above since $\text{Ker}\phi = \phi^{-1}(e)$. $\mathcal{QED}$

   The only reason we list this separately is that it is so important.

   (b) **Theorem (First Isomorphism Theorem):** Suppose $\phi : G \to H$ is a homomorphism. Then the mapping:

   $$G/\text{Ker}\phi \to \phi(G)$$

   given by:

   $$g\text{Ker}\phi \mapsto \phi(g)$$

   is an isomorphism. That is, $G/\text{Ker}\phi \approx \phi(G)$.
   Proof: Define $\psi : G/\text{Ker}\phi \to \phi(G)$ by $\psi(g\text{Ker}\phi) = \phi(g)$. Part (e) of the theorem above shows this is well-defined, meaning independent of the coset representative, and also that it is 1-1. It is onto by construction. To show it preserves the operation observe that:

   $$\psi(g_1\text{Ker}\phi g_2\text{Ker}\phi) = \psi(g_1g_2\text{Ker}\phi) = \phi(g_1g_2) = \phi(g_1)\phi(g_2) = \psi(g_1\text{Ker}\phi)\psi(g_2\text{Ker}\phi)$$

   $\mathcal{QED}$

   Example: The mapping $\phi : \mathbb{Z} \to \mathbb{Z}_5$ given by $\phi(x) = x \bmod 5$ is a homomorphism and has $\text{Ker}\phi = 5\mathbb{Z}$ and consequently $\mathbb{Z}/5\mathbb{Z} \approx \mathbb{Z}_5$.

   Intuition: In the picture earlier we can see what is happening. There is a 1-1 correspondance between the group of cosets in G and the image $\phi(G)$ and this correspondance is an isomorphism.

   (c) **Theorem:** Suppose $\phi : G \to H$ is a homomorphism. Then $|\phi(G)|$ divides both $|G|$ and $|H|$.
   Proof: Since G is a subgroup of itself, part (g) of the theorem above implies that $\phi(G) \leq H$ and so $|\phi(G)|$ divides $|H|$ by Lagrange's Theorem and part (l) of the theorem above implies that $|\phi(G)|$ divides $|G|$.

   Example: If $|G| = 20$ and $|H| = 32$ and if $\phi : G \to H$ is a homomorphism then $|\phi(G)|$ can oly be 1 or 2.

   Example: If $\gcd(|G|, |H|) = 1$ then the only homomorphism must take everything to $e \in H$.

   (d) **Theorem (Normal Subgroups are Kernels)**: Suppose $N \lhd G$. Then there is a mapping ϕ from G to another group with $N = \text{Ker}\phi$.
   Proof: Define $\phi : G \to G/N$ by $\phi(g) = gN$. First note that:

   $$\phi(xy) = xyN = xNyN = \phi(x)\phi(y)$$

   Then note that:

   $$g \in \text{Ker}\phi \text{ iff } \phi(g) = eN \text{ iff } gN = eN \text{ iff } g \in N$$

   $\mathcal{QED}$