CHAPTER II: GROUPS

Section 4: Homomorphisms

In the last section, we learned about isomorphisms. A group isomorphism is a bijection (a one-to-one and onto function) that preserves the group operations. Some functions between groups preserve the group operations but are not bijections. They have a name too.

Definition: A group ***homomorphism*** is a mapping $\varphi : G \to H$ for which $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$ for all $g_1, g_2 \in G$.

Notice that there is no one-to-one or onto requirement for homomorphisms. So in the definition of isomorphism, you can think of the two requirements as follows: there is (1) an "iso-" part (the bijection requirement) and (2) a "-morphism" part (operation preserving requirement).

Example 1: Recall from linear algebra that the determinant of an invertible matrix is nonzero, and $\det(AB) = \det(A)\det(B)$. Let $GL(n,\mathbb{R})$ be the group of $n \times n$ invertible matrices with real entries (under matrix multiplication). Then the mapping $\varphi : GL(n,\mathbb{R}) \to \mathbb{R}^*$ defined by $\varphi(A) = \det(A)$ is a homomorphism from the group of invertible matrices to the nonzero real numbers (under multiplication). This is clearly not one-to-one since many matrices can have the same determinant. Is it onto? For any nonzero real number, can you find an $n \times n$ matrix with that determinant?

Example 2: Let G be a group and let $a \in G$. The mapping $\varphi_a : \mathbb{Z} \to G$ defined by $\varphi_a(k) = a^k$ is a homomorphism from the integers to G. If G is not cyclic (or is cyclic but a is not a generator), then this will not be a surjection (an onto mapping), and if G is not infinite cyclic (generated by a) G won't be an injection (a one-to-one mapping).

We saw this next theorem in the last section, but it was stated for isomorphisms. It's true for homomorphisms too, so we restate it here (although without proof since the proof is the same).

Theorem 1: Let $\varphi: G \to H$ be a homomorphism of groups G and H and let e_G and e_H be the respective identity elements. Then $\varphi(e_G) = e_H$ and $\varphi(g^{-1}) = \varphi(g)^{-1}$ for each $g \in G$.

Theorem 2: Let $\varphi: G \to H$ and $\psi: H \to K$ be group homomorphisms. Then $\psi \circ \varphi: G \to K$ is also a homomorphism.

In the next theorem, we will discuss the effect of homomorphisms on subgroups. For this, we'll need a couple of definitions that are not specific to groups and homomorphisms.

Definition: Let $\varphi: G \to H$ be a function between sets G and H. Let A be any *subset* of G and B be any *subset* of H. We define the ***image*** of A to be the set $\varphi(A) = \{h \in H : h = \varphi(a) \text{ for some } a \in A\}$ and the ***inverse image*** of B to be the set $\varphi^{-1}(B) = \{g \in G : \varphi(g) \in B\}$.

$\varphi(A)$ is just the set of all images of elements in A and $\varphi^{-1}(B)$ is the set of all elements that get mapped into B. Be very careful not to think of φ^{-1} as the inverse of the function φ. The function φ might not be injective (i.e. one-to-one), so it may not be invertible. φ^{-1} is just convenient notation. Let's make this clear with an example.

Example 3: Define $G = \{1,2,3,4,5\}$ and $H = \{1,2,3\}$ and define $\varphi: G \to H$ by the rule: $\varphi(x) = 2$ if x is even and $\varphi(x) = 1$ if x is odd. If $A = \{1,3,5\}$, then $\varphi(A) = \{1\}$. If $B = \{2,3\}$, then $\varphi^{-1}(B) = \{2,4\}$. Note that φ is neither one-to-one nor onto.

Ok, we're ready for the next theorem.

Theorem 3: Let $\varphi: G \to H$ be a group homomorphism and let A be a subgroup of G and B be a subgroup of H. Then $\varphi(A)$ is a subgroup of H and $\varphi^{-1}(B)$ is a subgroup of G.

Proof: I'll prove the first part and leave the second part as an exercise. Recall from Theorem 4 of the last set of notes that we only have to show that these sets are closed under the respective group operations and contain their

inverses. Let $h_1, h_2 \in \varphi(A)$. Then there exist $a_1, a_2 \in A$ such that $\varphi(a_1) = h_1$ and $\varphi(a_2) = h_2$. Since A is a subgroup of G, $a_1 a_2 \in A$ and $a_1^{-1} \in A$. Therefore,

$$h_1 h_2 = \varphi(a_1)\varphi(a_2) = \varphi(a_1 a_2) \in \varphi(A), \text{ and}$$

$$h_1^{-1} = (\varphi(a_1))^{-1} = \varphi(a_1^{-1}) \in \varphi(A).$$

Definition: Let $\varphi : G \to H$ be a group homomorphism. The ***kernel*** of the homomorphism φ, denoted by $\ker(\varphi)$, is the set of all elements of G that get mapped to the identity in H. In other words,

$$\ker(\varphi) = \varphi^{-1}(e_H) = \{g \in G : \varphi(g) = e_H\}.$$

Definition: Let G be a group, let N be a subgroup of G and let $g \in G$. The set gNg^{-1} is defined to be $\{gng^{-1} : n \in N\}$. A subgroup is ***normal*** if $gNg^{-1} = N$ for all $g \in G$.

Theorem 4: Let $\varphi : G \to H$ be a group homomorphism. Then the $\ker(\varphi)$ is a normal subgroup of G.

Proof: By Theorem 3, $\ker(\varphi)$ is a subgroup of G. So we just need to show that $g\ker(\varphi)g^{-1} = \ker(\varphi)$ for all $g \in G$. To show this set equality, we'll show containment both directions. Let $gxg^{-1} \in g\ker(\varphi)g^{-1}$ (note: $x \in \ker(\varphi)$). Then $\varphi(gxg^{-1}) = \varphi(g)\varphi(x)\varphi(g^{-1}) = \varphi(g)e_H\varphi(g)^{-1} = e_H$, so $gxg^{-1} \in \ker(\varphi)$. So $g\ker(\varphi)g^{-1} \subseteq \ker(\varphi)$ for all $g \in G$. In particular, for any $g \in G$, $g^{-1}\ker(\varphi)g \subseteq \ker(\varphi)$ is also true. We'll need this in the second part.

Now suppose $x \in \ker(\varphi)$. Since $g^{-1}xg \in g^{-1}\ker(\varphi)g \subseteq \ker(\varphi)$, there must exist a $y \in \ker(\varphi)$ such that $g^{-1}xg = y$. So we have $x = gyg^{-1}$, and hence $\ker(\varphi) \subseteq g\ker(\varphi)g^{-1}$.

Clearly, if a homomorphism $\varphi : G \to H$ is injective (i.e. one-to-one) then $\ker(\varphi) = \{e_G\}$. The converse is also true.

Theorem 5: A homomorphism $\varphi : G \to H$ is injective if and only if $\ker(\varphi) = \{e_G\}$.

Proof: Suppose $\varphi : G \to H$ is injective. Since $\varphi(e_G) = e_H$ there cannot be any other element that also gets mapped to the identity. So $\ker(\varphi) = \{e_G\}$.

Now assume $\ker(\varphi) = \{e_G\}$. If $\varphi(g_1) = \varphi(g_2)$, then

$$\varphi(g_1^{-1} g_2) = \varphi(g_1^{-1})\varphi(g_2) = \varphi(g_1)^{-1}\varphi(g_1) = e_H .$$

So $g_1^{-1} g_2 = e_G$ which means that $g_2 = g_1$ and hence φ is injective.