Section 13 – Homomorphisms

Instructor: Yifan Yang

Fall 2006
Homomorphisms

Definition
A map \( \phi \) of a group \( G \) into a group \( G' \) is a homomorphism if

\[
\phi(ab) = \phi(a)\phi(b)
\]

for all \( a, b \in G \).
Examples

1. Let $\phi : G \to G'$ be defined by $\phi(g) = e'$ for all $g \in G$. Then clearly, $\phi(ab) = e' = e'e' = \phi(a)\phi(b)$ for all $a, b \in G$. This is called the **trivial homomorphism**.

2. Let $\phi : \mathbb{Z} \to \mathbb{Z}$ be defined by $\phi(n) = 2n$ for all $n \in \mathbb{Z}$. Then $\phi$ is a homomorphism.

3. Let $S_n$ be the symmetric group on $n$ letters, and let $\phi : S_n \to \mathbb{Z}_2$ be defined by

$$\phi(\sigma) = \begin{cases} 0, & \text{if } \sigma \text{ is an even permutation,} \\ 1, & \text{if } \sigma \text{ is an odd permutation.} \end{cases}$$

Then $\phi$ is a homomorphism. (Check case by case.)
1. Let $GL(n, \mathbb{R})$ be the set of all invertible $n \times n$ matrices over $\mathbb{R}$. Define $\phi : GL(n, \mathbb{R}) \rightarrow \mathbb{R}^\times$ by $\phi(A) = \det(A)$. Then $\phi$ is a homomorphism since $\det(AB) = \det(A) \det(B)$.

2. Let $F$ be the additive group of all polynomials with real coefficients. For a given real number $a$, the function $\phi_a : F \rightarrow \mathbb{R}$ defined by $\phi(f) = f(a)$ is a homomorphism, called an evaluation homomorphism.

3. Let $n$ be a positive integer. Define $\phi_n : \mathbb{Z} \rightarrow \mathbb{Z}_n$ by $\phi_n(r) = \bar{r}$. Then $\phi_n$ is a homomorphism.

4. Let $G = G_1 \times G_2 \times \ldots \times G_n$ be a direct product of groups. The projection map $\pi_i : G \rightarrow G_i$ defined by $\pi_i(a_1, a_2, \ldots, a_i, \ldots, a_n) = a_i$ is a homomorphism.
Definition
Let $\phi$ be a mapping of a set $X$ into a set $Y$. Let $A \subset X$ and $B \subset Y$. The image $\phi[A]$ of $A$ under $\phi$ is $\{\phi(a) : a \in A\}$. The set $\phi[X]$ is the range of $\phi$. The inverse image $\phi^{-1}[B]$ of $B$ in $X$ is $\{x \in X : \phi(x) \in B\}$. 
Properties of homomorphisms

Theorem (13.12)

Let $\phi$ be a homomorphism of a group $G$ into a group $G'$.

1. $\phi(e) = e'$.
2. $\phi(a^{-1}) = \phi(a)^{-1}$ for all $a \in G$.
3. If $H$ is a subgroup of $G$, then $\phi[H]$ is a subgroup of $G'$.
4. If $K'$ is a subgroup of $G'$, then $\phi^{-1}[K']$ is a subgroup of $G$. 
Proof of $\phi(e) = e'$.

Consider $\phi(a)$, where $a \in G$. We have

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

By the cancellation law, $\phi(e)$ must equal to the identity $e'$. \qed

Proof of $\phi(a^{-1}) = \phi(a)^{-1}$.

We have

$$\phi(a)\phi(a^{-1}) = \phi(aa^{-1}) = \phi(e) = e'.$$

Thus, $\phi(a^{-1}) = \phi(a)^{-1}$. \qed
Proof of Theorem 13.12

Proof of Theorem 13.12(3).

We need to prove

1. **Closed**: Suppose that $a', b' \in \phi[H]$. Then there exist $a, b \in H$ such that $\phi(a) = a'$ and $\phi(b) = b'$. Thus, $a'b' = \phi(a)\phi(b) = \phi(ab)$. Since $H$ is a subgroup, $ab \in H$. Therefore, $a'b'$ is in $\phi[H]$.

2. **identity**: By Part (1), $e' = \phi(e) \in \phi[H]$.

3. **inverse**: Suppose that $a' \in \phi[H]$. Then $a' = \phi(a)$ for some $a \in H$. By Part (b), $(a')^{-1} = \phi(a)^{-1} = \phi(a^{-1})$, and thus $(a')^{-1} \in \phi[H]$.

$\square$
Proof of Theorem 13.12(4).

We need to show

1. **Closed**: Suppose that $a, b \in \phi^{-1}[K']$. We have $\phi(a), \phi(b) \in K'$. Then $\phi(ab) = \phi(a)\phi(b) \in K'$ because $\phi(a), \phi(b) \in K'$ and $K'$ is a subgroup of $G'$.

2. **Identity**: By Part (1), we have $\phi(e) = e' \in K'$. It follows that $e \in \phi^{-1}[K']$ since $K'$ is a subgroup.

3. **Inverse**: Let $a \in \phi^{-1}[K']$. We have $\phi(a) \in K'$. By Part (2), $\phi(a^{-1}) = \phi(a)^{-1}$. Since $K'$ is a subgroup, $\phi(a) \in K'$ implies $\phi(a)^{-1} \in K'$.
Why are group homomorphisms important in group theory?

Let $G = \mathbb{Z}_{12}$ and $G' = \mathbb{Z}_7$. How many homomorphisms from $G$ to $G'$ are there?

**Solution.** Let $\phi$ be a homomorphism from $\mathbb{Z}_{12}$ to $\mathbb{Z}_7$. On the one hand, we have $\phi(0) = 0$, by Theorem 13.11. On the other hand, we have $0 = 12$ in $\mathbb{Z}_{12}$, and thus

$$
\phi(0) = \phi(12) = \phi(1) + \cdots + \phi(1) = 12\phi(1).
$$

Since 12 is relatively prime to 7, $\phi(1)$ must be equal to 0 in $\mathbb{Z}_7$. It follows that $\phi(n) = n\phi(1) = 0 \mod 7$ for all $n \in \mathbb{Z}_{12}$. In other words, there is only one homomorphism, the trivial homomorphism, from $\mathbb{Z}_{12}$ to $\mathbb{Z}_7$. 

Why are group homomorphisms important in group theory?

Now consider $G = G' = \mathbb{Z}_{12}$. It can be shown that for all $a \in \mathbb{Z}_{12}$, the function $\phi_a : \mathbb{Z}_{12} \rightarrow \mathbb{Z}_{12}$ defined by $\phi_a(r) = ar \ mod \ 12$ is a homomorphism. From these two examples, we see that group homomorphisms are closely related to group structures. Thus, group homomorphisms are very important in studying structural properties of groups.
Kernel

Since \( \{ e' \} \) is a subgroup of \( G' \), Theorem 13.11 shows that \( \phi^{-1}[\{ e' \}] \) is a subgroup of \( G \). This subgroup is of great importance.

**Definition**

Let \( \phi : G \rightarrow G' \) be a group homomorphism. The subgroup

\[
\phi^{-1}[\{ e' \}] = \{ g \in G : \phi(g) \}
\]

is called the kernel of \( \phi \), and denoted by \( \text{Ker}(\phi) \).
Theorem (13.15)

Let $\phi : G \to G'$ be a group homomorphism, and let $H = \ker(\phi)$. Let $a \in G$. Then the set

$$\{ x \in G : \phi(x) = \phi(a) \} = \phi^{-1}[\{ \phi(a) \}]$$

is the left coset $aH$, and is also the right coset $Ha$. Consequently, the partition of $G$ into left cosets is the same as the partition into right cosets.

Corollary (13.18)

A group homomorphism $\phi : G \to G'$ is one-to-one if and only if $\ker(\phi) = \{ e \}$. 
Example

Question
Are there any non-trivial homomorphisms from $A_4$ to $\mathbb{Z}_2$?

Solution
Suppose that $\phi : A_4 \to \mathbb{Z}_2$ is a non-trivial homomorphism. Then there is a $\sigma$ in $A_4$ such that $\phi(\sigma) = 1$. By Theorem 13.15, $\text{Ker}(\phi)$ and $\sigma \text{Ker}(\phi)$ are left cosets, and form a partition of $A_4$. In other words, $(A_4 : \text{Ker}(\phi)) = 2$, and $|\text{Ker}(\phi) = 6|$. However, we see earlier that $A_4$ does not have a subgroup of order 6. Thus, there is no non-trivial homomorphism from $A_4$ to $\mathbb{Z}_2$. 
Proof of Theorem 13.15

We will show that

1. \(aH \subset \phi^{-1}[[\phi(a)]]\): Let \(x = ag \in aH\). Since \(\phi\) is a homomorphism, we have \(\phi(x) = \phi(a)\phi(h)\). By assumption that \(H = \text{Ker}(\phi)\), it follows that \(\phi(x) = \phi(a)\), and \(x \in \phi^{-1}[[\phi(a)]]\).

2. \(\phi^{-1}[[\phi(a)]] \subset aH\): Suppose that \(x \in \phi^{-1}[[\phi(a)]]\). We have \(\phi(x) = \phi(a)\), and thus \(\phi(a)^{-1}\phi(x) = e'\). By Theorem 13.12(2), \(\phi(a)^{-1} = \phi(a^{-1})\). It follows that \(\phi(a^{-1}x) = e'\), and \(a^{-1}x \in H\). We see that \(x \in aH\).

The proof of \(\phi^{-1}[[\phi(a)]] = Ha\) is similar.
Examples

1. Let $n$ be a positive integer. Let $\phi : \mathbb{Z} \to \mathbb{Z}_n$ be defined by $\phi(a) = \bar{a}$, the residue class modulo $n$ containing $n$. Then $\text{Ker}(\phi) = n\mathbb{Z}$. Also, for each $\bar{b} \in \mathbb{Z}_n$, the set $\phi^{-1}[\{\bar{b}\}] = \{\ldots, b - 2n, b - n, b, b + n, \ldots\} = b + n\mathbb{Z}$, which is indeed a coset.

2. Let $U$ be the set of all complex number $z$ of unit length, i.e., $|z| = 1$. Consider $\phi : \mathbb{R} \to U$ defined by $\phi(x) = e^{ix}$. The kernel is $\text{Ker}(\phi) = \{x : e^{ix} = 1\} = \{2n\pi : n \in \mathbb{Z}\}$, and the sets $\phi^{-1}[\{\phi(a)\}]$ are equal to $\{a + 2n\pi : n \in \mathbb{Z}\} = a + \text{Ker}(\phi)$. 
Normal subgroups

**Definition**
A subgroup $H$ of a group $G$ is **normal** if its left cosets and right cosets coincide, that is, if

$$gH = Hg \quad \text{for all } g \in G.$$  

(Alternatively, $gHg^{-1} = H$ for all $g \in G$, or $ghg^{-1} \in H$ for all $h \in H$ and $g \in G$.)

**Corollary (13.20)**
If $\phi : G \to G'$ is a group homomorphism, then $\ker(\phi)$ is a normal subgroup.
Example

Let $G = S_3$. There are 6 subgroups, namely, $\{e\}$, $\{e, (1, 2)\}$, $\{e, (1, 3)\}$, $\{e, (2, 3)\}$, $\{e, (1, 2, 3), (1, 3, 2)\}$, and $G$. Among them, it is easy to see that $\{e\}$ and $G$ are normal. The subgroup $\{e, (1, 2, 3), (1, 3, 2)\}$ is normal since it is of index 2 in $S_3$. The three subgroups of order 2 are not normal. For example, we have

$$(1, 3)(1, 2)(1, 3) = (2, 3) \not\in \{e(1, 2)\}.$$ 

Thus, $\{e, (1, 2)\}$ is not a normal subgroup.
Homework

Do Problems 18, 24, 27, 38, 40, 44, 47, 50, 51, 53 of Section 13.