16. HOMOMORPHISMS

16.1. Basic properties and some examples.

Definition. Let $G$ and $H$ be groups. A map $\varphi : G \to H$ is called a homomorphism if

$$\varphi(xy) = \varphi(x)\varphi(y) \text{ for all } x, y \in G.$$ 

Example 1. Let $G = (\mathbb{Z}, +)$ and $H = (\mathbb{Z}_n, +)$ for some $n > 1$. Define $\varphi : G \to H$ by $\varphi(x) = [x]$. Then $\varphi$ is a homomorphism.

Since operation in both groups is addition, the equation that we need to check in this case is $\varphi(x + y) = \varphi(x) + \varphi(y)$. Verification is given below:

$$\varphi(x) + \varphi(y) = [x] + [y] = [x + y] = \varphi(x + y)$$

(where equality $[x] + [y] = [x + y]$ holds by definition of addition in $\mathbb{Z}_n$).

Example 2. Let $F$ be a field, $n > 1$ and integer, $G = \text{GL}_n(F)$ and $H = (F \setminus \{0\}, \cdot)$. Define the map $\varphi(A) = \det(A)$.

In this example $\varphi$ is a homomorphism thanks to the formula $\det(AB) = \det(A)\det(B)$. Note that while this formula holds for all matrices (not necessarily invertible ones), in the example we have to restrict ourselves to invertible matrices since the set $\text{Mat}_n(F)$ of all $n \times n$ matrices over $F$ does not form a group with respect to multiplication.

Example 3. Unlike the situation with isomorphisms, for any two groups $G$ and $H$ there exists a homomorphism $\varphi : G \to H$, called the trivial homomorphism. It is given by $\varphi(x) = e_H$ for all $x \in G$ (where $e_H$ is the identity element of $H$).

The following theorem shows that in addition to preserving group operation, homomorphisms must also preserve identity element and inversion.

Theorem 16.1. Let $G$ and $H$ be groups and $\varphi : G \to H$ a homomorphism. Then

(a) $\varphi(e_G) = e_H$ where $e_G$ is the identity element of $G$ and $e_H$ is the identity element of $H$.

(b) $(\varphi(x))^{-1} = \varphi(x^{-1})$ for all $x \in G$.

Proof. (a) Since $e_G = e_G \cdot e_G$, we have $\varphi(e_G) = \varphi(e_G \cdot e_G) = \varphi(e_G) \cdot \varphi(e_G)$.

Multiplying both sides by $\varphi(e_G)^{-1}$ on the left (or on the right), we get $e_H = \varphi(e_G)$. 

(b) We need to prove that \( \varphi(x^{-1}) \) is the inverse of \( \varphi(x) \) in \( H \). By Theorem 11.1(d) it suffices to show that \( \varphi(x^{-1}) \cdot \varphi(x) = e_H \) which follows from the result of (a): \( \varphi(x^{-1}) \cdot \varphi(x) = \varphi(x^{-1}x) = \varphi(e_G) = e_H \) where the last equality holds by (a).

Next we introduce two fundamental subgroups which can be associated to every homomorphism.

So let \( G \) and \( H \) be groups and \( \varphi : G \to H \) a homomorphism. The first subgroup associated to \( \varphi \) is the range (image) of \( \varphi \):

\[
\text{Range}(\varphi) = \varphi(G) = \{ h \in H : h = \varphi(g) \text{ for some } g \in G. \}
\]

From the definition it is clear that \( \varphi(G) \) is a subset of \( H \), but below we will show that it is actually a subgroup.

The second subgroup if the kernel of \( \varphi \), which is defined to be the set of all elements of \( G \) which get mapped to the identity element of \( H \) by \( \varphi \):

\[
\text{Ker}(\varphi) = \{ g \in G : \varphi(g) = e_H \}.
\]

**Theorem 16.2.** Let \( G \) and \( H \) be groups and \( \varphi : G \to H \) a homomorphism. Then

(a) \( \varphi(G) \) is a subgroup of \( H \)
(b) \( \text{Ker}(\varphi) \) is a subgroup of \( G \)

**Proof.** (a) First note that by Theorem 16.1(a) we have \( e_H = \varphi(e_G) \), so \( e_H \in \varphi(G) \).

Next we check that \( \varphi(G) \) is closed under group operation: take any \( u, v \in \varphi(G) \). By definition of \( \varphi(G) \) there exist \( x, y \in G \) such that \( u = \varphi(x) \) and \( v = \varphi(y) \). Hence \( uv = \varphi(x)\varphi(y) = \varphi(xy) \in \varphi(G) \).

Finally, we check that \( \varphi(G) \) is closed under inversion: take any \( u \in \varphi(G) \). Then \( u = \varphi(x) \) for some \( x \in G \), so \( u^{-1} = (\varphi(x))^{-1} = \varphi(x^{-1}) \in \varphi(G) \) where the second equality holds by Theorem 16.1(b).

(b) The proof for the kernel is rather similar. Again Theorem 16.1(a) implies that \( e_G \in \text{Ker}(\varphi) \).

Next take any \( x, y \in \text{Ker}(\varphi) \). Then \( \varphi(x) = \varphi(y) = e_H \), so \( \varphi(xy) = \varphi(x)\varphi(y) = e_H \cdot e_H = e_H \), so \( xy \in \text{Ker}(\varphi) \) as well. Thus, \( \text{Ker}(\varphi) \) is closed under group operation.

(c) Finally, for any \( x \in \text{Ker} \varphi \) we have \( \varphi(x) = e_H \), so by Theorem 16.1(b) we have \( \varphi(x^{-1}) = (\varphi(x))^{-1} = e_H^{-1} = e_H \), so \( x^{-1} \in \text{Ker}(\varphi) \). Hence \( \text{Ker}(\varphi) \) is closed under inversion.

**Example 4.** Let \( G = H = \langle \mathbb{Z}_{10}, + \rangle \), and define \( \varphi : G \to H \) by \( \varphi([x]) = 2[x] = [2x] \) for all \( x \in \mathbb{Z} \).
It is straightforward to check that \( \varphi \) is a homomorphism. The range of \( \varphi \) is \( \varphi(G) = \{ h \in H : h = [2x] \text{ for some } x \in \mathbb{Z} \} = \{ [0], [2], [4], [6], [8] \} = \{ [2] \} \).

The kernel of \( \varphi \) is \( \{ [x] \in G : [2x] = e_H \} = \{ [x] \in G : [2x] = [0] \} \). Since 
\[ [2x] = [0] \iff 2x = 10k \text{ for some } k \in \mathbb{Z} \iff x = 5k \text{ for some } k \in \mathbb{Z}. \]
Thus, \( \ker(\varphi) = \{ [5k] : k \in \mathbb{Z} \} = \langle [5] \rangle = \{ [0], [5] \} \).

The following theorem shows that one can check whether a homomorphism is injective simply by computing its kernel.

**Theorem 16.3.** Let \( G \) and \( H \) be groups and \( \varphi : G \to H \) a homomorphism. Then \( \varphi \) is injective if and only if \( \ker(\varphi) = \{ e_G \} \).

**Proof.** “\( \Rightarrow \)” Suppose \( \varphi \) is injective. We know that \( \varphi(e_G) = e_H \), so \( \ker(\varphi) \) contains \( e_G \), and if \( \ker(\varphi) \) contained another element besides \( e_G \), then \( \varphi \) would not be injective. Thus, \( \ker(\varphi) = \{ e_G \} \).

“\( \Leftarrow \)” We argue by contrapositive (if \( \varphi \) is not injective, then \( \ker(\varphi) \neq \{ e_G \} \)). Suppose \( \varphi \) is not injective, so there exist \( x \neq y \) in \( G \) with \( \varphi(x) = \varphi(y) \). Then \( \varphi(xy^{-1}) = \varphi(x)\varphi(y^{-1}) = \varphi(x)\varphi(y)^{-1} = e_H \), so \( xy^{-1} \) is an element of \( \ker(\varphi) \) different from \( e_G \). \( \square \)

16.2. Some analogies with linear algebra and Range-Kernel Theorem. The notions of group, homomorphism, range and kernel have direct analogues in linear algebra:

<table>
<thead>
<tr>
<th>group theory</th>
<th>linear algebra</th>
</tr>
</thead>
<tbody>
<tr>
<td>group</td>
<td>vector space</td>
</tr>
<tr>
<td>homomorphism</td>
<td>linear transformation</td>
</tr>
<tr>
<td>range of a homomorphism</td>
<td>range of a linear transformation</td>
</tr>
<tr>
<td>kernel of a homomorphism</td>
<td>nullspace of a linear transformation</td>
</tr>
</tbody>
</table>

One of the fundamental results in linear algebra is the rank-nullity theorem which asserts the following:

**Rank-Nullity Theorem.** Let \( F \) be a field, let \( V \) and \( W \) be finite-dimensional vector spaces over \( F \), and let \( T : V \to W \) be a linear transformation. Then
\[
\dim(\varphi(T)) + \dim(\text{Nullspace}(T)) = \dim(V)
\]
(The number \( \dim(\varphi(T)) \) is called the rank of \( T \) and the number \( \dim(\text{Nullspace}(T)) \) is called the nullity of \( T \), so the theorem says that the sum of the rank of \( T \) and the nullity of \( T \) is equal to the dimension of the vector space on which \( T \) is defined).

The following theorem, which we call the Range-Kernel Theorem, is a group-theoretic analogue of rank-nullity theorem.
**Theorem 16.4** (Range-Kernel Theorem). Let $G$ and $H$ be finite groups and $\varphi : G \to H$ a homomorphism. Then

$$|\varphi(G)| \cdot |\text{Ker}(\varphi)| = |G|.$$  

In Example 4 we have $|G| = 10$, $|\varphi(G)| = 5$ and $|\text{Ker}(\varphi)| = 2$.

We finish this lecture with an example showing how the Range-Kernel Theorem can be used to compute the order of some group.

**Problem 16.5.** Let $p$ be a prime. Compute the order of the group $|SL_2(\mathbb{Z}_p)|$.

We will solve this problem in two steps. First we will compute $|GL_2(\mathbb{Z}_p)|$ and then use the Range-Kernel Theorem to compute $|SL_2(\mathbb{Z}_p)|$.

**Step 1:** By definition $GL_2(\mathbb{Z}_p) = \{A \in \text{Mat}_2(\mathbb{Z}_p) : \det(A) \neq [0]\}$.

By a theorem from linear algebra, $\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} \neq [0] \iff$ the vectors $(a, b)$ and $(c, d)$ are not proportional (that is, are not multiples of each other). Using this observation, we can count the number of ways to choose a $2 \times 2$ invertible matrix with entries in $\mathbb{Z}_p$.

The first row of a matrix in $GL_2(\mathbb{Z}_p)$ can be any vector of length 2 except $(\begin{smallmatrix} 0 \\ 0 \end{smallmatrix})$, so there are $p^2 - 1$ choices for the first row. Once the first row $(a, b)$ is chosen, the second row can be any vector which is not a scalar multiple of $(a, b)$. Since any nonzero vector with entries in $\mathbb{Z}_p$ has precisely $p$ distinct multiples, there are $p^2 - p$ choices for the second row. Overall we have $(p^2 - 1)(p^2 - p)$ choices, so $|GL_2(\mathbb{Z}_p)| = (p^2 - 1)(p^2 - p) = (p - 1)^2 p(p + 1)$.

**Step 2:** By Example 2, the map $\varphi : GL_2(\mathbb{Z}_p) \to \mathbb{Z}_p \setminus \{[0]\}$ given by $\varphi(A) = \det(A)$, is a homomorphism.

The range of $\varphi$ is the entire group $\mathbb{Z}_p \setminus \{[0]\}$ since every nonzero $a \in \mathbb{Z}_p$ is the determinant of some $2 \times 2$ matrix: $a = \det \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$. The kernel of $\varphi$ is the set $\{A \in GL_2(\mathbb{Z}_p) : \det(A) = [1]\}$ which is precisely $SL_2(\mathbb{Z}_p)$. Therefore, by the Range-Kernel Theorem we have

$$|SL_2(\mathbb{Z}_p)| = |\text{Ker}(\varphi)| = \frac{|G|}{|\varphi(G)|} = \frac{|GL_2(\mathbb{Z}_p)|}{|\mathbb{Z}_p \setminus \{[0]\}|} = \frac{(p - 1)^2 p(p + 1)}{p - 1} = (p - 1)p(p + 1).$$

16.3. **Book references.** The general references for this lecture are [Pinter, Chapter 14] and [Gilbert, 3.6].