Section I.2. Homomorphisms and Subgroups

Note. Recall that, in a general sense, an “isomorphism” between two mathematical structures is a one to one and onto mapping which preserves the structure. In a semigroup, the structure is the binary operation. In this section we define homomorphisms and related mappings and explore subgroups generated by sets of elements of a group.

Definition I.2.1. Let \( G \) and \( H \) be semigroups. A function \( f : G \to H \) is a homomorphism if \( f(ab) = f(a)f(b) \) for all \( a, b \in G \). A one to one (injective) homomorphism is a monomorphism. An onto (surjective) homomorphism is an epimorphism. A one to one and onto (bijective) homomorphism is an isomorphism. If there is an isomorphism from \( G \) to \( H \), we say that \( G \) and \( H \) are isomorphic, denoted \( G \cong H \). A homomorphism \( f : G \to G \) is an endomorphism of \( G \). An isomorphism \( f : G \to G \) is an automorphism of \( G \).

Note. If \( f : G \to H \) and \( g : H \to K \) are homomorphisms on semigroups \( G, H, K \), then the composition \( g \circ f = gf : G \to K \) is a homomorphism. Similarly, compositions of monomorphisms, epimorphisms, isomorphisms, and automorphisms are respectively monomorphisms, epimorphisms, isomorphisms, and automorphisms. You are probably familiar with the fact that a group homomorphism maps identities to identities and inverses to inverses. However, a monoid homomorphism may not preserve identities (see Exercise I.2.1).
Example. Let $G = \mathbb{Z}$ and $H = \mathbb{Z}_m$. Define $f : \mathbb{Z} \to \mathbb{Z}_m$ as $x \to \overline{x}$ (that is, $f(x)$ is the equivalence class of $\mathbb{Z}_m$ containing $x$). Then $f$ is a homomorphism. Of course, $f$ is not one to one, however $f$ is onto. So $f$ is an epimorphism (called the “canonical epimorphism” of $\mathbb{Z}$ onto $\mathbb{Z}_m$).

Example. If $A$ is an abelian group, then $f : A \to A$ defined as $f(a) = a^{-1}$ is an automorphism of $A$. $g : A \to A$ defined as $g(a) = a^2$ is an endomorphism of $A$.

Example. Let $m, k \in \mathbb{N}$, $m \neq 1 \neq k$. Then $f : \mathbb{Z}_m \to \mathbb{Z}_{mk}$ defined as $f(x) = \overline{kx}$ is a monomorphism.

Note. The following definitions are similar to the definitions of set valued functions encountered in analysis.

Definition I.2.2. Let $f : G \to H$ be a homomorphism of groups. The kernel of $f$ is $\text{Ker}(f) = \{g \in G \mid f(g) = e_H \in H\}$. If $A \subseteq G$, then the image of $A$ is $f(A) = \{h \in H \mid h = f(a) \text{ for some } a \in A\}$. The set $f(G)$ is called the image of homomorphism $f$, denoted $\text{Im}(f)$. If $B \subseteq H$, the inverse image of $B$ is the set $f^{-1}(B) = \{g \in G \mid f(g) \in B\}$. We denote the identity $i : G \to G$ defined as $i(g) = g$ for all $g \in G$ as $1_G$. 
**Note.** Of course, the inverse image of a set makes sense even if the inverse function may not exist. For example, the endomorphism \( f : \mathbb{Z} \to \mathbb{Z} \) defined as \( f(x) = x^2 \) does not have an inverse (since it is not one to one), but we can still consider \( f^{-1}(\{9\}) = \{-3, 3\} \).

**Note 1.** Let \( A, B, C \) be sets with \( f : A \to B \) and \( g : B \to C \). Then we have:

(a) if \( f \) and \( g \) are one to one then \( gf \) is one to one;

(b) if \( f \) and \( g \) are onto then \( gf \) is onto;

(c) if \( gf \) is one to one then \( f \) is one to one; and

(d) if \( gf \) is onto then \( g \) is onto.

Notice that the identity map \( 1_A \) is one to one and onto by definition. These results are on page 5 of Hungerford.

**Theorem I.2.3.** Let \( f : G \to H \) be a homomorphism of groups. Then:

(i) \( f \) is a monomorphism if and only if \( \text{Ker}(f) = \{e_G\} \);

(ii) \( f \) is an isomorphism if and only if there is a homomorphism \( f^{-1} : H \to G \) such that \( ff^{-1} = 1_H \) and \( f^{-1}f = 1_G \).
I.2. Homomorphisms and Subgroups

**Definition I.2.4.** Let $G$ be a semigroup and $H$ a nonempty subset of $G$. If for every $a, b \in H$ we have $ab \in H$ then $H$ is closed under the binary operation of $G$. Let $G$ be a group and $H$ a nonempty subset of $G$ that is closed under the binary operation of $G$. If $H$ itself is a group under the binary operation then $H$ is a subgroup of $G$. This is denoted $H < G$. For group $G$, the trivial subgroup is $\{e_G\}$. Subgroup $H < G$ is a proper subgroup if $H \neq G$ and $H \neq \{e_G\}$.

**Examples.** In $\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$, both $H_1 = \{\overline{0}, \overline{3}\}$ and $H_2 = \{\overline{0}, \overline{2}, \overline{4}\}$ are proper subgroups of $\mathbb{Z}_6$. In $\mathbb{Z}$, for a given $n \in \mathbb{N}$, $n \neq 0$, $n\mathbb{Z} = \{nx \mid x \in \mathbb{Z}\}$ is a subgroup of $\mathbb{Z}$ (in fact, $n\mathbb{Z} \cong \mathbb{Z}$—see Exercise I.2.7).

**Example.** In the symmetric group $S_n$, the set $\{\sigma \in S_n \mid \sigma(n) = n\}$ (i.e., the set of permutations of $\{1, 2, \ldots, n\}$ which leave $n$ fixed) is a subgroup of $S_n$ which is isomorphic to $S_{n-1}$ (see Exercise I.2.8).

**Example.** If $f : G \to H$ is a homomorphism of groups, then Ker$(f)$ is a subgroup of $G$ (see Exercise I.2.9(a)). This is an important example, as we’ll see when we explore cosets and normal subgroups in Sections I.4 and I.5.

**Example.** If $G$ is a group, then the set Aut$(G)$ of all automorphisms of $G$ is itself a group under the binary operation of function composition (see Example I.2.15). This will be an important idea when we study field theory and Galois theory in Chapter V.
**Theorem I.2.5.** Let $H$ be a nonempty subset of a group $G$. Then $H$ is a subgroup of $G$ if and only if $ab^{-1} \in H$ for all $a, b \in H$.

**Corollary I.2.6.** If $G$ is a group and $\{H_i \mid i \in I\}$ is a nonempty set of subgroups of $G$, then $\bigcap_{i \in I} H_i$ is a subgroup of $G$.

**Proof.** This is homework Exercise I.2.A. Notice that index set $I$ may not be finite... it may not even be countable! □

**Definition I.2.7.** Let $G$ be a group and $X$ a subset of $G$. Let $\{H_i \mid i \in I\}$ be the set of all subgroups of $G$ which contain $X$. Then $\bigcap_{i \in I} H_i$ is the **subgroup of $G$ generated by the set $X$**, denoted $\langle X \rangle$.

**Note.** You are probably familiar with the special case where $G = \langle \{a\} \rangle$. That is, the case when $G$ is generated by a single element. Then $G$ is “cyclic” and, in fact, such $G$ is either isomorphic to $\mathbb{Z}_n$ for some $n \in \mathbb{N}$ or $G \cong \mathbb{Z}$ (see Section I.3).

**Definition.** For group $G$, the elements of $X \subset G$ are called **generators** of subgroup $\langle X \rangle$. If $G = \langle a_1, a_2, \ldots, a_n \rangle$ (notice the set brackets are dropped by convention) then $G$ is **finitely generated**. If $G = \langle a \rangle$ then $G$ is **cyclic**.
Theorem I.2.8. If $G$ is a group and $X$ is a nonempty subset of $G$, then the subgroup $\langle X \rangle$ generated by $X$ consists of all finite products $a_1^{n_1}a_2^{n_2}\cdots a_t^{n_t}$ (where $a_i \in X$ and $n_i \in \mathbb{Z}$ for $i = 1, 2, \ldots, t$). In particular, for every $a \in G$, $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$.

Definition. Let $\{H_i \mid i \in I\}$ be a set of subgroups of group $G$. The subgroups $\langle \bigcup_{i \in I} H_i \rangle$ is called the group generated by the groups $\{H_i \mid i \in I\}$. If $H$ and $K$ are subgroups of $G$ then the subgroup generated by $H \cup K$, $\langle H \cup K \rangle$, is called the join of $H$ and $K$, denoted $H \vee K$ (if $H$ and $K$ are multiplicative groups) or $H + K$ (if $H$ and $K$ are additive groups).

Note. If $G$ is an abelian group and $H < G$, $K < G$, then $H \vee K = \{hk \mid h \in H, k \in K\}$ (see Exercise I.2.17).