1.2 Homomorphism and Subgroups

Definition. Let G and H be semigroups. A function $f : G \mapsto H$ is a homomorphism if $f(ab) = f(a)f(b)$ for $a, b \in G$.

Note.

$$\begin{array}{lll} f \text{ is } 1-1 & \Leftrightarrow & f \text{ is monomorphism.} \\ f \text{ is onto} & \Leftrightarrow & f \text{ is epimorphism.} \\ f \text{ is } 1-1 \text{ and onto.} & \Leftrightarrow & f \text{ is isomorphism.} \\ f \text{ is } 1-1 \text{ and onto, } G = H. & \Leftrightarrow & f \text{ is automorphism.} \end{array}$$

We always write G as a group.

Definition. $H \subseteq G$ is a subgroup of G if H is a group under the same operation of G.

Example. $2\mathbb{Z}$ is a subgroup of $\mathbb{Z}$ under $+$.

Note. *We write $H < G$ if H is a subgroup of G.*

Theorem. *$H < G \Leftrightarrow \phi \neq H \subseteq G$ and $ab^{-1} \in H$ for $a, b \in H$*

Proof.
- *($\Rightarrow$) Clear.*
- *($\Leftarrow$) We need to check H is a group:*
  1. *Associate to check H is a group.*
  2. *Pick $h \in H$.*
  3. *For any $a \in H$,$a^{-1} = ea^{-1} \in H$.*
  4. *For $a, b \in H, ab = a(b^{-1})^{-1}$.*□

Theorem. *$f : G \mapsto H$ is a group homomorphism.*
$\Rightarrow$ The kernal of f,$Kerf := \{g \in G | f(g) = e\}$,is a subgroup of G.

Proof. *Note:$f(e) = f(ee) = f(e)f(e)$*
Hence $f(e)$ is the identity in H.
That is $Kerf \neq \phi$
Also $f(b)f(b^{-1}) = f(bb^{-1}) = f(e)$
By uniqueness of $f(b)^{-1}$.
we find $f(b^{-1}) = f(b)^{-1}$ for any a,b $\in Kerf$.
we have $f(ab^{-1}) = f(a)f(b^{-1})$ is the identity in H.
Thus $ab^{-1} \in Kerf$.
Hence $Kerf$ is a subgroup of G by previous theorem.□

Note. 1. *$f(G)$ is a subgroup of H.*

2. *The center $Z(G)$ of G is a subgroup of G,where$Z(G) := \{g \in G | gh = hg$ for $h \in G\}$.*

3. *Fix $a \in G$. The centralizer $C_G(a)$ of G is a subgroup of G,where $C_G(a) := \{g \in G | ga = ag\}$*
   $Z(G) := \bigcap_{a \in G} C_G(a)$.$\square$

Definition. Fix $X \subseteq G$. Let $< X >$ be the intersection of all subgroups contain X. $< X >$ is called the subgroup of G generated by X.

Theorem. *Fix $X \subseteq G$. Then $< X >= \{a_1^{n_1} a_2^{n_2} \cdots a_t^{n_t} | a_i \in X, n_i \in \mathbb{Z}\}$*

Proof. *($\subseteq$) This is clear since RHS is a subgroup containing X.*
(Note $(a_1^{n_1} a_2^{n_2} \cdots a_t^{n_t})^{-1} = a_t^{-n_t} a_{t-1}^{-n_{t-1}} \cdots a_1^{-n_1}$)

($\supseteq$) This is clear. Since such $a_1^{n_1} a_2^{n_2} \cdots a_t^{n_t}$ is contained in each subgroup of G contain X.$\square$

Example. $X = \{0, 2\} \subseteq \mathbb{Z}$. X does not generate a group under multiplication.

Example. If X is a set of invertible elements, then X generates a group. In fact, this group is $< X >= \{a_1^{n_1} a_2^{n_2} \cdots a_t^{n_t} | a_i \in X$ and $n_i \in \mathbb{Z}\}$.