Proposition 3.6. *A subset H of a group G is a subgroup of G if, and only if,* *all $a, b \in H$.*

Proof The $\Rightarrow$ implication is true by the definition of a subgroup.

To show that the $\Leftarrow$ implication is true,

Choose $b = a$. Then $aa^{-1} = e \in H$ i.e. H contains the identity.

Choose $a = e$. Then $eb^{-1} = b^{-1} \in H$ i.e. H contains inverses.

Choose $b = b^{-1}$. Then $a(b^{-1})^{-1} = ab \in H$ i.e. H is closed.

Associativity follows since H is a subset of G.

□

Definition 3.7. The *right cosets* of a subgroup H of a group G are the subsets of G of the form

$$Ha = \{ha \in G \, : \, h \in H\}$$

for any $a \in G$.

Remark 3.8. To compute the right cosets of a subgroup H of a group G, we choose $a \in G$ to be each of the elements of G in turn and find the corresponding right coset Ha. We will see later on that these right cosets provide a *partition* of G (i.e. they divide G into mutually disjoint subsets), and hence can be found more efficiently.

Example 3.9. Consider the set $G = \{1,\, a,\, b,\, c,\, d,\, e\}$ with product table (3.1) in Example 3.5.

The right cosets of the subgroup $H = \{1,\, a,\, b\}$ of G are

$$\begin{aligned}
H1 &= \{1,\, a,\, b\}\,1 = \{1,\, a,\, b\}\,, \\
Ha &= \{1,\, a,\, b\}\,a = \{a,\, b,\, 1\}\,, \\
Hb &= \{1,\, a,\, b\}\,b = \{b,\, 1,\, a\}\,, \\
Hc &= \{1,\, a,\, b\}\,c = \{c,\, e,\, d\}\,, \\
Hd &= \{1,\, a,\, b\}\,d = \{d,\, c,\, e\}\,, \\
He &= \{1,\, a,\, b\}\,e = \{e,\, d,\, c\}\,.
\end{aligned}$$

Hence the right cosets of the subgroup $H = \{1,\, a,\, b\}$ of the group $G = \{1,\, a,\, b,\, c,\, d,\, e\}$ are $\{1,\, a,\, b\}$ and $\{c,\, d,\, e\}$, giving the partition of G.

Definition 3.10. An *equivalence relation* on a set G is a relation $\sim$ between pairs of elements of G satisfying

(i) $\forall\, a \in G,\ a \sim a$ **(reflexivity)**,

(ii) $\forall\, a,\, b \in G,\ a \sim b \Rightarrow b \sim a$ **(symmetry)**,

(iii) $\forall\, a,\, b,\, c \in G,\ a \sim b,\, b \sim c \Rightarrow a \sim c$ **(transitivity)**.

The *equivalence class* of $a \in G$ is defined to be $\{b \in G \, : \, b \sim a\}$.