3.3 SubGroups

To proceed further, we study the notion of subgroup of a given group. That is, if $(G, *)$ is a group and H is a non-empty subset of G then under what condition is $(H, *)$ a group in its own right (it is important to note that the binary operation is the same as that in G). Formally, we have the following definition.

Definition 3.3.1 (Subgroup)**.** *Let $(G, *)$ be a group. Then a non-empty subset H of G is said to be a subgroup of G, if H itself forms a group with respect to the binary operation $*$.*

Example 3.3.2.

1. *Let G be a group with identity element e. Then G and $\{e\}$ are themselves groups and hence they are subgroups of G. These two subgroups are called* **trivial subgroups**.

2. *$\mathbb{Z}$, the set of integers, and $\mathbb{Q}$, the set of rational numbers, are subgroups of $(\mathbb{R}, +)$, the set of real numbers with respect to addition.*

3. *The set $\{e, r^2, f, r^2f\}$ forms a subgroup of D_4.*

4. *Let $\sigma \in \mathcal{S}_4$. Then, using Theorem 3.1.7, we know that σ has a cycle representation. With this understanding it can be easily verified that the group D_4 is a subgroup of $\mathcal{S}_4$.*

5. *Consider $H = \{e, r, r^2, \ldots, r^{n-1}\}$ as a subset of D_n. Then it can be easily verified that H is a subgroup of D_4. This subgroup is also written as $\langle r \rangle$ to indicate that it is generated by the element r of D_4.*

Before proceeding further, let us look at the following two results which help us in proving "whether or not a given non-empty subset H of a group G is a subgroup of G"?

Theorem 3.3.3 (Subgroup Test)**.** *Let G be a group and let H be a non-empty subset of G. Then H is a subgroup of G if for each $a, b \in H$, $ab^{-1} \in H$.*

Proof. As H is non-empty, we can find an $x \in H$. Therefore, for $a = x$ and $b = x$, the condition $ab^{-1} \in H$ implies that $e = aa^{-1} \in H$. Thus, H has the identity element of G. Hence, for each $h \in H \subset G$, $eh = h = he$.

We now need to prove that for each $h \in H$, $h^{-1} \in H$. To do so, note that for $a = e$ and $b = h$ the condition $ab^{-1} \in H$ reduces to $h^{-1} = eh^{-1} \in H$.

As a third step, we show that H is closed with respect to the binary operation of G. So, let us assume that $x, y \in H$. Then by the previous paragraph, $y^{-1} \in H$. Therefore, for $a = x$ and $b = y^{-1}$ the condition $ab^{-1} \in H$ implies that $xy = x(y^{-1})^{-1} \in H$. Hence, H is also closed with respect to the binary operation of G.

Finally, we see that since the binary operation of H is same as that of G and since associativity holds in G, it holds in H as well. ■

We now give another result without proof that helps us in deciding whether a non-empty subset of a group is a subgroup or not.

Theorem 3.3.4. *[Two-Step Subgroup Test] Let H be a non-empty subset of a group G. Then H is a subgroup if the two conditions given below hold.*

1. *For each $a, b \in H$, $ab \in H$ (i.e., H is closed with respect to the binary operation of G).*
2. *For each $a \in H$, $a^{-1} \in H$.*

We now give a few examples to understand the above theorems.

Example 3.3.5. 1. *Consider the group $(\mathbb{Z}, +)$. Then in the following cases, the given subsets do not form a subgroup.*

   (a) *Let $H = \{0, 1, 2, 3, \ldots\} \subset \mathbb{Z}$. Note that, for each $a, b \in H$, $a + b \in H$ and the identity element $0 \in H$. But H is not a subgroup of $\mathbb{Z}$, as for all $n \neq 0$, $-n \notin H$.*

   (b) *Let $H = \mathbb{Z} \setminus \{0\} = \{\ldots, -3, -2, -1, 1, 2, 3, \ldots\} \subset \mathbb{Z}$. Note that, the identity element $0 \notin H$ and hence H is not a subgroup of $\mathbb{Z}$.*

   (c) *Let $H = \{-1, 0, 1\} \subset \mathbb{Z}$. Then H contains the identity element 0 of $\mathbb{Z}$ and for each $h \in H$, $h^{-1} = -h \in H$. But H is not a subgroup of $\mathbb{Z}$ as $1 + 1 = 2 \notin H$.*

2. *Let G be an abelian group with identity e. Consider the sets $H = \{x \in G : x^2 = e\}$ and $K = \{x^2 : x \in G\}$. Then prove that both H and K are subgroups of G.*

   Proof. *Clearly $e \in H$ and $\mathbf{e} \in K$. Hence, both H and K are non-empty subsets of G. We first show that H is a subgroup of G.*

   As H is non-empty, pick $x, y \in H$. Thus, $x^2 = e = y^2$. We will now use Theorem 3.3.3, to show that $xy^{-1} \in H$. But this is equivalent to showing that $\left(xy^{-1}\right)^2 = e$. But this is clearly true as G is abelian implies that

$$\left(xy^{-1}\right)^2 = x^2(y^{-1})^2 = e(y^2)^{-1} = e^{-1} = e.$$

   Thus, H is indeed a subgroup of G by Theorem 3.3.3.

   Now, let us prove that K is a subgroup of G. We have already seen that K is non-empty. Thus, we just need to show that for each $x, y \in K$, $xy^{-1} \in K$.

   Note that $x, y \in K$ implies that there exists $a, b \in G$ such that $x = a^2$ and $y = b^2$. As $b \in G, b^{-1} \in G$. Also, $xy^{-1} = a^2(b^2)^{-1} = a^2(b^{-1})^2 = (ab^{-1})^2 \in K$ as G is abelian and $ab^{-1} \in G$. Thus, K is also a subgroup of G.

As a last result of this section, we prove that the condition of the above theorems can be weakened if we assume that H is a finite, non-empty subset of a group G.

Theorem 3.3.6. *[Finite Subgroup Test] Let G be a group and let H be a non-empty finite subset of G. If H is closed with respect to the binary operation of G then H is a subgroup of G.*

Proof. By Theorem 3.3.4, we just need to show that for each $a \in H$, $a^{-1} \in H$. If $a = e \in H$ then $a^{-1} = e^{-1} = e \in H$. So, let us assume that $a \neq e$ and $a \in H$. Now consider the set $S = \{a, a^2, a^3, \ldots, a^n, \ldots\}$. As H is closed with respect to the binary operation of G, $S \subset H$. But H has only finite number of elements. Hence, all these elements of S cannot be distinct. That is, there exist positive integers, say m, n with $m > n$, such that $a^m = a^n$. Thus, using Remark 3.1.2, one has $a^{m-n} = e$. Hence, $a^{-1} = a^{m-n-1}$ and by definition $a^{m-n-1} \in H$. ■