3. Prove that a group $(G,\circ)$ is abelian if and only if $(a\circ b)^{-1} = a^{-1}\circ b^{-1}$ for all $a,b\in G$.

Proof: Let $(G,\circ)$ be abelian. Let $a,b\in G$

Then $(a\circ b)^{-1} = b^{-1}\circ a^{-1}$ (proved earlier)

$= a^{-1}\circ b^{-1}$ (As $(G,\circ)$ is abelian)

Conversely, let $(G,\circ)$ be a group such that $(a\circ b)^{-1} = b^{-1}\circ a^{-1}$ for all $a,b\in G$. We have to prove that $(G,\circ)$ is abelian. Let $a,b\in G$

Then $(a\circ b) = ((a\circ b)^{-1})^{-1}$ $[\text{As } (a^{-1})^{-1} = a]$

$= (a^{-1}\circ b^{-1})^{-1}$ (Given)

$= (b^{-1})^{-1}\circ(a^{-1})^{-1}$ $\left(\text{As } (a\circ b)^{-1} = b^{-1}\circ a^{-1}\right)$

$= b\circ a$ $[\text{As } (a^{-1})^{-1} = a]$

So, $(G,\circ)$ is abelian group.

4. Let $(G,\circ)$ be a group. A relation R on G defined by aRb if and only if $b = g\circ a\circ g^{-1}$ for some $g\in G$, $a,b\in G$. Prove that R is an equivalence relation on G.

Proof $a = e\circ a\circ e^{-1}$, e is the identity element in G and $e = e^{-1}$ also.

So, aRa, for all $a\in G$.

So, R is reflexive

Let aRb holds $\Rightarrow$ there exists $g\in G$ such that $b = g\circ a\circ g^{-1}$. Now $b = g\circ a\circ g^{-1} \Rightarrow g^{-1}\circ b = a\circ g^{-1}$

$\Rightarrow g^{-1}\circ b\circ g = a \Rightarrow a = g^{-1}\circ b\circ(g^{-1})^{-1}$

So bRa as $g^{-1}\in G$. So R is symmetric

Let aRb, bRc hold. Then $b = g \circ a \circ g^{-1}$ and $c = g' \circ b \circ g'^{-1}$ for $g, g' \in G$. Now $c = g' \circ b \circ g'^{-1} = g' \circ (g \circ a \circ g^{-1}) \circ g'^{-1}$

$= (g' \circ g) \circ a \circ (g' \circ g)^{-1}$ $[\text{As } (a \circ b)^{-1} = b^{-1} \circ a^{-1}]$

So, $c = g'' \circ a \circ g''^{-1}$ where $g'' = g' \circ g \in G$.

So aRc. So, R is transitive.

So, R is an equivalence relation on G.

5. Let $(G, \circ)$ be a group. Define a mapping $f : G \to G$ by $f(x) = x^{-1}$, $x \in G$. Prove that f is a bijection.

Proof: Let $f(x_1) = f(x_2) \Rightarrow x_1^{-1} = x_2^{-1} \Rightarrow (x_1^{-1})^{-1} = (x_2^{-1})^{-1} \Rightarrow x_1 = x_2$

So, f is injective.

Now take $x \in G$.

Then $f(x^{-1}) = (x^{-1})^{-1} = x$

So, f is surjective.

So, f is a bijection.

Exercise 1. Examine if the following system are groups:

(i) $(\mathbb{Z}, \circ)$ where $a \circ b = a + b - 2$, $a, b \in \mathbb{Z}$

(ii) $(\mathbb{R}^*, \circ)$ where $a \circ b = 3ab$, $a, b \in \mathbb{R}^* = \mathbb{R} - \{0\}$

(iii) $(\mathbb{R}, \circ)$ where $a \circ b = \frac{1}{2}(a+b)$, $a, b \in \mathbb{R}$.

Exercise 2 If each element in a group be its own inverse prove that the group is abelian.

Exercise 3 Let $(G, \circ)$ and $a \in G$. Define a mapping $f_a : G \to G$ by $f_a(x) = a \circ x$, $x \in G$. Prove that λ_a is a bijection.

Exercise 4 Let $(G, \circ)$ be a group and $a \in G$. Define a mapping $g_a : G \to G$ by $g_a(x) = a^{-1} \circ x \circ a$, $x \in G$. Prove that g_a is a bijection. What happens if $(G, \circ)$ be a commutative group.

Subgroups: Definition Let (G, o) be a group and H be a non-empty subset of G. If (H, o) be a group where o is the restriction of o on H, then H is a said to be a ~~subgroup~~ sub-group of G.

Example 1. Let (G, o) be a group. If $H = \{e\}$, e is the identity element in G, then (H, o) is a group. So $\{e\}$ is a subgroup of G. Similarly G is also a subgroup of G. $\{e\}$ is called the trivial subgroup of G and G is said to be improper subgroup of G. Other subgroups are called non-trivial proper subgroups.

NOTE: the identity element of a subgroup is same as the identity of the group

Example 2 $(\mathbb{Q}, +)$ is a group. $\mathbb{Z}$ is a non-empty subset of $\mathbb{Q}$ and $(\mathbb{Z}, +)$ is a group. So, $(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Q}, +)$.

Example 3 $(\mathbb{Z}, +)$ is a group. $2\mathbb{Z} = \{2k : k \in \mathbb{Z}\}$ is a non-empty subset of $\mathbb{Z}$ and $(2\mathbb{Z}, +)$ is a group. So, $(2\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Z}, +)$

Example 4 Let $G = \{1, -1, i, -i\}$ Then G is a group with respect to complex multiplication. $H = \{1, -1\}$ is a non-empty subset of G and it is also a group with respect to the same operation on H. So H is a subgroup of G.

Example 5 Let (G, o) be an abelian group and (H, o) is a subgroup of (G, o). Then (H, o) is an abelian group, since o, being commutative on G is also commutative on H.

Statement of necessary and sufficient condition for a subgroup:

Theorem 1 Let (G, o) be a group. A non-empty subset H of G forms a subgroup of (G, o) if and only if
(i) $a \in H, b \in H \Rightarrow a o b \in H$ (ii) $a \in H \Rightarrow a^{-1} \in H$

Result 6 Let $(G, \circ)$ be a group and H and K are subgroups of $(G, \circ)$. Then $H \cap K$ is a subgroup of $(G, \circ)$

Proof: Here $H \cap K$ is nonempty as the identity element e of G ~~which~~ belongs to both H and K and so belongs to $H \cap K$.

Let $a, b \in H \cap K$. Then $a, b \in H$ and $a, b \in K$

Since H is a subgroup, $a \circ b \in H$

Since K is a subgroup, $a \circ b \in K$

So, $a \circ b \in H \cap K$

Let $a \in H \cap K \Rightarrow a \in H$ and $a \in K$

Since H is a subgroup, $a^{-1} \in H$

Since K is a subgroup, $a^{-1} \in K$

So, $a^{-1} \in H \cap K$

So, $H \cap K$ is a subgroup of $(G, \circ)$

Note: The union of two subgroups may not be a subgroup.

Consider the group $G = (\mathbb{Z}, +)$ and the subgroups $H = (2\mathbb{Z}, +)$ and $K = (3\mathbb{Z}, +)$, now $2 \in H \cup K$ and $3 \in H \cup K$ but $2 + 3 = 5 \notin H \cup K$. So, $H \cup K$ is not a subgroup.

Result 7 Let $(G, \circ)$ be a group and H be the subset defined by $H = \{x \in G : x \circ g = g \circ x \text{ for all } g \in G\}$. Then H is a subgroup of $(G, \circ)$.

The identity element e of G is in H as $e \circ g = g \circ e = g$ for all $g \in G$. So, H is non-empty.

Let $p, q \in H \Rightarrow p \circ g = g \circ p$ for all $g \in G$
and $q \circ g = g \circ q$ for all $g \in G$.

Now $(p \circ q) \circ g = p \circ (q \circ g) = p \circ (g \circ q) = (p \circ g) \circ q = (g \circ p) \circ q$
$= g \circ (p \circ q)$
for all $g \in G$.

So, $p \circ q \in H$

* Hence H is a subgroup.

Now, let $p \in H \Rightarrow p \circ g = g \circ p$ for all $g \in G$.

So, $g^{-1} \circ (p \circ g) = g^{-1} \circ (g \circ p)$ or, $(g^{-1} \circ p) \circ g = (g^{-1} \circ g) \circ p$ or, $(g^{-1} \circ p) \circ g = p$
or, $((g^{-1} \circ p) \circ g) \circ g^{-1} = p \circ g^{-1}$ or, $(g^{-1} \circ p) \circ (g \circ g^{-1}) = p \circ g^{-1}$
or $g^{-1} \circ p = p \circ g^{-1}$ for all $g \in H$ *