4. Let G be a finite commutative group such that G contains two distinct elements of order 2. Show that $o(G)$ is a multiple of 4. Also, show that this result need not be true if G is not commutative.

Proof: Let a and b be two distinct elements of order 2 in G.

Let $H = \{e, a\}$ and $K = \{e, b\}$, e is the identity element in G.

Now H and K are two subgroups of G. Since G is commutative, $HK = \{e, a, b, ab\}$ is a subgroup of G of order 4.

Now $o(HK) = 4$ divides $o(G)$. Thus $o(G)$ is a multiple of 4.

The symmetric group S_3 is non-commutative, $\rho_4 = (1,3)$ and $\rho_5 = (1,2)$ are elements of S_3 and each is of order 2. But 4 does not divide $6 = o(S_3)$.

5. Normal Subgroups

Definition: Let G be a group. A subgroup H of G is said to be a normal subgroup of G if $aH = Ha \quad \forall a \in G$.

From the definition, of a normal subgroup, it follows that for any group G, G and $\{e\}$ are normal subgroups of G.

If G be a commutative group, then every subgroup of G is normal.

Let $G = S_3$ and $H = \{\rho_0, \rho_1, \rho_2\}$. We now compute the left cosets and right cosets of H in S_3. The left cosets of H in S_3 are $\rho_0 H = \rho_1 H = \rho_2 H = H$ and $\rho_3 H = \rho_4 H = \rho_5 H = \{\rho_3, \rho_4, \rho_5\}$

and the right cosets of H in S_3 are

$H\rho_0 = H\rho_1 = H\rho_2 = H$ and $H\rho_3 = H\rho_4 = H\rho_5 = \{\rho_3, \rho_4, \rho_5\}$

Thus $aH = Ha, \forall a \in S_3$

So, H is a normal subgroup of S_3. Here $H = A_3$

Now consider the subgroup $H' = \{\rho_0, \rho_3\}$

Then $\rho_0 H' = \rho_3 H' = H'$, $\rho_2 H' = \rho_4 H' = \{\rho_4, \rho_2\}$

and $\rho_1 H' = \rho_5 H' = \{\rho_1, \rho_5\}$ are the left cosets of H' in S_3

The right cosets of H' in S_3 are

$$H'\rho_0 = H'\rho_3 = H', \quad H'\rho_1 = H'\rho_4 = \{\rho_1, \rho_4\}$$

and $H'\rho_2 = H'\rho_5 = \{\rho_2, \rho_5\}$

So, we see that $\rho_2 H' \neq H'\rho_2$

So, H' is not a normal subgroup of S_3.

The following theorem gives a necessary and sufficient condition for a subgroup to be a normal subgroup. For $a \in G$, $\phi \neq H \subseteq G$, let $aHa^{-1} = \{aha^{-1} : h \in H\}$

Theorem 5.1 Let H be a subgroup of a group G. Then H is a normal subgroup of G if and only if $aHa^{-1} \subseteq H$ for each $a \in G$.

Proof: Suppose H is a normal subgroup of G. Let $a \in G$. We show that $aHa^{-1} \subseteq H$. Let $aha^{-1} \in aHa^{-1}$, where $h \in H$. Since H is a normal subgroup of G, $aH = Ha$. Also, since $ah \in aH$, we have $ah \in Ha$ and so $ah = h'a$ for some $h' \in H$. Thus $aha^{-1} = h' \in H$. Hence, $aHa^{-1} \subseteq H$.

Conversely, suppose $aHa^{-1} \subseteq H$ for each $a \in G$. Let $a \in G$. We show that $aH = Ha$ Let $ah \in aH$, where $h \in H$. Now $aha^{-1} \in aHa^{-1}$ and so $aha^{-1} \in H$. Thus, $aha^{-1} = h'$ for some $h' \in H$. This implies that $ah = h'a \in Ha$. So, $aH \subseteq Ha$. Similarly, we can show that $Ha \subseteq aH$. Hence $aH = Ha$. Consequently, H is a normal subgroup of G.

Theorem 5.2 Let H and K be two normal subgroups of a group G. Then

(i) $H \cap K$ is a normal subgroup of G,

(ii) $HK = KH$ is a normal subgroup of G.

Proof: (i) Since the intersection of subgroups is a subgroup, $H \cap K$ is a subgroup of G. Let $a \in G$. Consider $a(H \cap K)a^{-1}$. Let aba^{-1} be an element of $a(H \cap K)a^{-1}$, where $b \in H \cap K$. Since $b \in H \cap K$, we have $b \in H$ and $b \in K$. Hence $aba^{-1} \in H$ and $aba^{-1} \in K$ as H and K are normal subgroups of G. Thus, $aba^{-1} \in H \cap K$. This shows that $a(H \cap K)a^{-1} \subseteq H \cap K$. Hence $H \cap K$ is a normal subgroup by Theorem 5.1.

(ii) First we show that $HK = KH$. Let $hk \in HK$, where $h \in H$, $k \in K$. Since K is a normal subgroup of G and and $h \in G$, we have $hK = Kh$. Thus $hk \in hK = Kh$. Since $Kh \subseteq KH$, we have $hk \in KH$. Hence, $HK \subseteq KH$. Similarly, $KH \subseteq HK$ and so $HK = KH$. Since H and K are subgroups and $HK = KH$, HK is a subgroup of G by Theorem 2.4. To show that HK is a normal subgroup, let $a \in G$, Then $aHa^{-1} \subseteq H$ and $aKa^{-1} \subseteq K$ since H and K are normal subgroups. Let $a(hk)a^{-1} \in a(HK)a^{-1}$ where $h \in H$, $k \in K$ Now $a(hk)a^{-1} = (aha^{-1})(aka^{-1})$. As H and K are normal subgroups of G, $aha^{-1} \in H$ and $aka^{-1} \in K$. So, $a(hk)a^{-1} \in HK$ So, $a(HK)a^{-1} \subseteq HK$. So, HK is a normal subgroup of G.

worked out Exercises: 1. Let H be a subgroup of a group G. and $[G:H] = 2$. Then show that H is normal in G.

Proof: Since $[G:H] = 2$, there are exactly two distinct left cosets of H in G. They are H and $G - H$. ~~Since $G-H$ is the only left~~ Also there are two distinct right cosets of H in G and they are H and $G - H$. Let $a \in H$. Then $aH = H$ and also $Ha = H$, Clearly $aH = Ha$. Let $a \in G - H$ Then $aH = G - H$, Since $G - H$ is the only left coset other than H. Also $Ha = G - H$, Since $G - H$ is the only right coset other than H. So $aH = Ha$. It follows that $aH = Ha$, $\forall a \in G$. So, H is a normal subgroup of G.

2. The centre $Z(G)$ of a group G is a normal subgroup of G. Prove it.

Proof: $Z(G) = \{x \in G : xa = ax \ \forall a \in G\}$ is a subgroup of G. Let $a \in G$ and let $axa^{-1} \in aZ(G)a^{-1}$ for some $x \in Z(G)$. As $x \in Z(G)$, $ax = xa$.

So, $axa^{-1} = (xa)a^{-1} = x(aa^{-1}) = xe = x \in Z(G)$, e being the identity element of G. So $aZ(G)a^{-1} \subset Z(G)$. Hence $Z(G)$ is a normal subgroup of G.

Theorem 5.3 Let H be a normal subgroup of a group G. Denote the set of all left cosets $\{aH : a \in G\}$ by G/H and define $*$ on G/H by $aH * bH = abH$

Then $(G/H, *)$ is a group

Proof: Proof: First we show that $*$ is well defined. Let $aH, bH, a'H, b'H \in G/H$ and suppose $(aH, bH) = (a'H, b'H)$. Then $aH = a'H$ and $bH = b'H$. We need to show that $aH * bH = a'H * b'H$ or, $abH = a'b'H$. As $aH = a'H$, $a^{-1}a' = h_1$ for some $h_1 \in H$ and $bH = b'H \Rightarrow b^{-1}b' = h_2$ for some $h_2 \in H$

Now $(ab)^{-1}(a'b') = b^{-1}a^{-1}a'b' = b^{-1}h_1b' = b^{-1}b'h_3$ (since $Hb' = b'H$ for some $h_3 \in H$)

$= h_2h_3 = h_4 \in H$ for some $h_4 \in H$.

So, $abH = a'b'H$.

Next, we show that $*$ is associative. Let $aH, bH, cH \in G/H$

Now $(aH * bH) * cH = abH * eH = (ab)cH = a(bc)H$

$= aH * bcH = aH * (bH * cH)$. Hence $*$ is associative

Now $eH = H \in G/H$, e is the identity element in G.

Now $aH * eH = (ae)H = (ea)H = eH * aH = aH$ (as $\{ae = a\}$ for all $a \in G$.)

So, $eH = H$ is the identity element in G/H.

Also for any $aH \in G/H$, $\exists\ a^{-1}H \in G/H$ such that

$aH * a^{-1}H = (aa^{-1})H = eH = H = (a^{-1}a)H = a^{-1}H * aH$.

So $a^{-1}H$ is the inverse of aH. So, $(G/H, *)$ is a group.

Definition: Let G be a group and H be a normal subgroup of G. The group $(G/H, *)$ is called the quotient group of G by H.

Examples: 1. Consider the subgroup $(n\mathbb{Z}, +)$ of the group $(\mathbb{Z}, +)$, where n is a fixed positive integer. Since $\mathbb{Z}$ is commutative, $n\mathbb{Z}$ is a normal subgroup of $\mathbb{Z}$. Hence $(\mathbb{Z}/n\mathbb{Z}, +)$ is a group where $(a+n\mathbb{Z}) + (b+n\mathbb{Z}) = (a+b) + n\mathbb{Z}$ for any, $a+n\mathbb{Z}, b+n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$

2. Consider the normal subgroup $H = \{\rho_0, \rho_1, \rho_2\}$ of S_3. Since $o(S_3) = 6$ and $o(H) = 3$, $[S_3 : H] = 2$ by Lagrange's theorem. Hence, S_3/H has two elements. Here $S_3/H = \{H, \rho_3 H\}$ We also note that S_3/H is a cyclic group and $\rho_3 H$ is a generator of S_3/H.

2. Consider $\mathbb{Z}_8$ and let $H = \{\bar{0}, \bar{4}\}$. Then H is a normal subgroup of $\mathbb{Z}_8$. Now $o(H) = 2$ and $o(\mathbb{Z}_8) = 8$. Thus, $o(\mathbb{Z}_8/H) = \frac{o(\mathbb{Z}_8)}{o(H)} = 4$. Hence $\mathbb{Z}_8/H$ has four elements.

Now $\bar{0} + H = H = \bar{4} + H$,
$\bar{1} + H = \{\bar{1}, \bar{5}\} = \bar{5} + H$
$\bar{2} + H = \{\bar{2}, \bar{6}\} = \bar{6} + H$
And $\bar{3} + H = \{\bar{3}, \bar{7}\} = \bar{7} + H$
Hence $\mathbb{Z}_8/H = \{\bar{0}+H, \bar{1}+H, \bar{2}+H, \bar{3}+H\}$

Definition: Let G be a group. Then G is called a simple group if $G \neq \{e\}$ and the only normal subgroups of G are $\{e\}$ and G, e is the identity element of G.

Examples: 1. Let G be a cyclic group of order p, p a prime. Since the only subgroups of G are $\{e\}$ and G, G is simple.

Some more worked out exercises: 1. Let H be a subgroup of a group G. If $x^2 \in H$ for any $x \in G$, prove that H is a normal subgroup of G and G/H is commutative.

Proof: Let $g \in G$ and $h \in H$. Consider ghg^{-1} and note that $ghg^{-1} = (gh)^2 h^{-1} g^{-2}$. Now $h^{-1} \in H$ and by our hypothesis $(gh)^2, g^{-2} \in H$. This implies that $ghg^{-1} \in H$. So, $gHg^{-1} \subseteq H$. Hence H is a normal subgroup of G. To show that G/H is commutative, we wish to show that

$xH * yH = yH * xH$ or, $xyH = yxH$. Now consider $(xy)^{-1}(yx)$

Now $(xy)^{-1}(yx) = (y^{-1}x^{-1})(yx) = (y^{-1}x^{-1})^2 (xyx^{-1})^2 x^2$. Since $a^2 \in H$ for any $a \in G$. It follows that $(y^{-1}x^{-1})^2 (xyx^{-1})^2 x^2 \in H$ and so, $(xy)^{-1}(yx) \in H$. So, $xyH = yxH$. So, G/H is commutative.

~~2. Let H be a subgroup of a group~~

2. Let G be a group such that every cyclic subgroup of G is a normal subgroup of G. Prove that every subgroup of G is a normal subgroup of G.

Proof: Let H be a subgroup of G. Let $g \in G$ and $a \in H$. Then $g^{-1}ag \in \langle a \rangle \subseteq H$. Hence, H is normal in G.

3. Let G be a group. Show that if $G/Z(G)$ is cyclic, then G is commutative. ($Z(G)$ is the centre of the group G)

Proof: We write $Z = Z(G)$. Let $G/Z = \langle gZ \rangle$. Let $a, b \in G$. Then $aZ, bZ \in G/Z$. Hence $aZ = g^n Z$ and $bZ = g^m Z$ for some $n, m \in \mathbb{Z}$. Then $a \in g^n Z$ and $b \in g^m Z$.

Thus $a = g^n d_1$ and $b = g^m d_2$ for some $d_1, d_2 \in Z$.

Now $ab = g^n d_1 g^m d_2 = g^n g^m d_1 d_2$ (since $d_1 \in Z$) $= g^{n+m} d_2 d_1 = g^{m+n} d_2 d_1$ ($\because m+n = n+m$)

$= g^m g^n d_2 d_1 = g^m d_2 g^n d_1 = ba$ (as $d_2 \in Z$). Hence G is commutative