Sri SAI RAM ENGINEERING COLLEGE

INSTITUTE OF TECHNOLOGY

West Tambaram, Chennai - 44

SAIRAM DIGITAL RESOURCES

YEAR II

SEM III

MA8351

DISCRETE MATHEMATICS

(Common to CSE & IT)

UNIT 4

ALGEBRAIC STRUCTURES

4.3 SUBGROUPS

SCIENCE & HUMANITIES

Subgroup

Let $(G,*)$ be a group. A non-empty subset H of G is said to be a subgroup of G if H itself is a group under the same operation $*$ of G.

Example: $(Q,+)$ is a group and Z is a subset of Q. We know that $(Z,+)$ is a group and so $(Z,+)$ is a subgroup of $(Q,+)$.

Example: The set of all even integers is a subgroup of set of all integers under the operation $'+'$.

Theorem:

A non-empty subset H of a group $(G,*)$ is a subgroup of G if and only if $a * b^{-1} \in H \quad \forall\, a, b \in H$.

Proof:

Let H be a subgroup of a G and $a, b \in H$.

$\Rightarrow a^{-1}, b^{-1} \in H$

Since $a \in H$ and $b^{-1} \in H$

$\Rightarrow a * b^{-1} \in H$ [Since H is closed under $' * '$]

Conversely, assume H is a subset of G satisfying $a * b^{-1} \in H \quad \forall\, a, b \in H$.

To prove H is a subgroup of G.

(i) Since H is a non-empty, Let $a \in H$.

$\Rightarrow a * a^{-1} \in H \quad \Rightarrow e \in H$.

Hence H satisfies Identity law.

(ii) Since $a \in H$ and $e \in H$

$$\Rightarrow e, a \in H$$

$$\Rightarrow e * a^{-1} \in H$$

$$\Rightarrow a^{-1} \in H$$

Hence H satisfies Inverse law.

(iii) Since $b \in H \Rightarrow b^{-1} \in H$

$$\Rightarrow a, b^{-1} \in H$$

$$a * (b^{-1})^{-1} \in H$$

$$a * b \in H.$$

Hence H satisfies closure law.

(iv) Associative law is always true for $'*'$.

Hence $(H, *)$ is a sub-group of G.

Theorem:

If H_1 and H_2 be the two subgroups of G, then P.T $H_1 \cap H_2$ is also a subgroup of G. In other words, intersection of any two subgroup of G is again a subgroup. Also verify, union of any two subgroups of G is again a subgroup.

Proof:

Let $(G,*)$ be a group.

Since H_1 is a subgroup of G

$\Rightarrow a * b^{-1} \in H_1, \quad \forall a, b \in H_1$

Since H_2 is a subgroup of G

$\Rightarrow a * b^{-1} \in H_2, \quad \forall a, b \in H_2$

Since $a, b \in H_1$ and $a, b \in H_2$

$\Rightarrow a, b \in H_1 \cap H_2$

Also $a * b^{-1} \in H_1$ and $a * b^{-1} \in H_2$

$\Rightarrow a * b^{-1} \in H_1 \cap H_2 \quad \forall a, b \in H_1 \cap H_2$

$\Rightarrow H_1 \cap H_2$ is a subgroup of G.

Clearly, $H_1 \cup H_2$ is not a subgroup of G.

Since $(Z, +)$ is a group,

$H_1 = \{ \dots -6, -4, -2, 0, 2, 4, \dots \}$

$H_2 = \{ \dots -10, -5, 0, 5, 10, \dots \}$

H_1 and H_2 are the two subgroups.

$2 \in H_1$ and $5 \in H_2$

$\Rightarrow \quad 2 + 5 \notin H_1 \cup H_2$

$\therefore$ Union is not satisfied.

Example:

If H_1 and H_2 are subgroups of $(G,*)$ then prove that $H_1 \cup H_2$ is a subgroup of H if and only if $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$.

Solution: Given H_1, H_2 are subgroups of $(G,*)$

Let $H_1 \cup H_2$ be a subgroup of $(G,*)$.

To prove $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$

Assume the contrary. ie. Assume $H_1 \nsubseteq H_2$ and $H_2 \nsubseteq H_1$.

Then there exists $a \in H_1$ and $a \notin H_2$; $b \in H_2$ and $b \notin H_1$.

Since $a \in H_1$ and $b \in H_2$, $a, b \in H_1 \cup H_2 \Longrightarrow a * b \in H_1 \cup H_2$

Since $H_1 \cup H_2$ is a subgroup of $(G,*)$

$\therefore \quad a * b \in H_1$ or $a * b \in H_2$

Case (i) : Let $a * b \in H_1$, since $a \in H_1$, $a^{-1} \in H_1$

$\therefore\ a^{-1} * (a * b) \in H_1$, as H_1 is a subgroup.

$\Longrightarrow\ (a^{-1} * a) * b \in H_1 \ \Longrightarrow\ e * b \in H_1 \ \Longrightarrow\ b \in H_1$,

which contradicts the assumption $b \notin H_1$.

Case (ii) : Let $a * b \in H_2$, since $b \in H_2$, $b^{-1} \in H_2$

$(a * b) * b^{-1} \in H_2$, as H_2 is a subgroup.

$\Longrightarrow\ a * (b * b^{-1}) \in H_2 \ \Longrightarrow a * e \in H_2 \ \Longrightarrow\ a \in H_2$,

which contradicts the assumption $a \notin H_2$.

Hence in either case we have a contradiction.

$\therefore$ Our assumption $H_1 \nsubseteq H_2$ and $H_2 \nsubseteq H_1$ is wrong.

$\therefore\ H_1 \subseteq H_2$ or $H_2 \subseteq H_1$

Conversely, let $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$.

If $H_1 \subseteq H_2$ then $H_1 \cup H_2 = H_2$. $\therefore H_1 \cup H_2$ is a subgroup.

If $H_2 \subseteq H_1$ then $H_1 \cup H_2 = H_1$. $\therefore H_1 \cup H_2$ is a subgroup.

Thus $H_1 \cup H_2$ is a subgroup of $(G,*)$.

Example: Prove that $nZ = \{nx \mid x \in Z\}$ is a subgroup of $(Z, +)$.

Solution: Given $nZ = \{nx \mid x \in Z\}$.

If $x = 0$ then $nx = 0 \Longrightarrow 0 \in nZ$, So nZ is non-empty.

Let $a, b \in nZ$ then $a = nx$, $b = ny$ for some integers x, y.

Then $a - b = nx - ny = n(x - y) \in nZ$.

Hence $(nZ, +)$ is a subgroup of $(Z, +)$.

Example: Find all the non-trivial subgroups of $(Z_6, +_6)$.

Solution: $Z_6 = \{ [0], [1], [2], [3], [4], [5] \}$

$H_1 = \{ [0], [3] \}, H_2 = \{ [0], [2], [4] \}$ are all the non-trivial subgroup of $(Z_6, +_6)$

$+_6$	[0]	[3]
[0]	[0]	[3]
[3]	[3]	[0]

$+_6$	[0]	[2]	[4]
[0]	[0]	[2]	[4]
[2]	[2]	[4]	[0]
[4]	[4]	[0]	[2]

Since H_1, H_2 are finite subsets of G, H_1 and H_2 are closed under $+_6$, $(H_1, +_6)$, $(H_2, +_6)$ are subgroups of $(Z_6, +_6)$.

Theorem: Every subgroup of a cyclic group is cyclic.

Proof: Let $(G,*)$ be a cyclic group generated by a

Then $G = \{a^n | n \in Z\} = \langle a \rangle$

Let H be a subgroup of G.

Since H is a subset of G, every element of H is of the form a^r for some $r \in Z$.

Since H is a group, if $a^r \in H$, then its inverse $(a^r)^{-1} = a^{-r} \in H$.

so either r or $-r$ is a positive integer.

Hence H contains positive integer powers of a.

Let m be the least positive integer such that $a^m \in H$.

We shall prove a^m is a generator of H.

Let $x \in H$ be any element, then $x = a^n$ for some $n \in Z$.

For the integers n and m, by Euclidean algorithm, we can find integers q and r such that $n = mq + r\,, 0 \le r < m$

Then $\quad x = a^n = a^{mq+r} = a^{mq} * a^r = (a^m)^q * a^r$

$\Longrightarrow \quad (a^m)^{-q} * x = (a^m)^{-q} * (a^m)^q * a^r = e * a^r = a^r$

$a^r = (a^m)^{-q} * x = a^{-mq} * x$

Now $\quad a^m \in H \quad \Longrightarrow (a^m)^q \in H$, by closure.

$\Longrightarrow \quad a^{mq} \in H \quad \Longrightarrow \quad a^{-mq} \in H \quad$ [Since H is a group.]

$\therefore \quad a^{-mq} * x \in H \quad$ [by closure]

$\Longrightarrow \quad a^r \in H$, where $r < m$

If $r \neq 0$, then $a^r \in H$ is a contradiction to the fact that m is the least positive integer such that $a^m \in H$. Hence $r = 0$

$\therefore \quad n = mq \quad \Longrightarrow \quad x = (a^m)^q$

Thus, any element of H is an integral power of a^m.

So, H is cyclic group generated by a^m.

i.e., $H = \langle a^m \rangle$

Theorem: If $(G,*)$ is a cyclic group generated by a, then prove that a^{-1} is also a generator.

Proof: Given $G = \langle a \rangle$

So, any element $x \in G$ is $x = a^n$ for some integer n.

Now $x = a^n = (a^{-1})^{-n}$

Thus, x is an integral power of a^{-1} and so a^{-1} is also a generator of G.