Def: (Subgroup) : let $(G, \cdot)$ be a group.

A non-empty subset H of G is said to be a subgroup of G if H itself a group under the same binary operation defined on G.

Theorem: A non-empty subset H of G is a subgroup iff

(i) $a, b \in H \Rightarrow a \cdot b \in H$

(ii) $a \in H \Rightarrow a^{-1} \in H$

Theorem: A non-empty set H of G is a subgroup iff $\forall\, a, b \in H$ $ab^{-1} \in H$.

$\Downarrow$

Subgroup test

Proof: If H is a subgroup of H then clearly (i) and (ii) holds.

Conversely, Suppose (i) and (ii) holds.

We have to show that $(H, \underset{\substack{\Downarrow \\ \text{binary operation on } G.}}{\cdot})$ is a group

(i) $\Rightarrow$ If $a, b \in H$ then $a \cdot b \in H$.

(A) Associativity

(A) So, $a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad \forall a, b, c \in H$, and since $a, b, c \in G$, and '$\cdot$' is an associative binary operation on G.

(B) Existence of identity

let $a \in H \Rightarrow a^{-1} \in H$ (from (ii))

$\Rightarrow a \cdot a^{-1} \in H$ (from (i))

$\Rightarrow e \in H$.

(C) Existence of ~~identity~~ inverse :

Follows from (ii)

#

Example :(1) $(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{R}, +)$

(2) $(\mathbb{N}, +)$ is not a subgroup of $(\mathbb{Z}, +)$.

(3) $n\mathbb{Z} = \{n \cdot m : m \in \mathbb{Z}\}$ is a subgroup of $(\mathbb{Z}, +)$

$2\mathbb{Z}, 3\mathbb{Z}, 5\mathbb{Z}, 6\mathbb{Z}, \ldots$

Example : For any group G, $\{e\}$ and G are subgroups of G.

Example: $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$

$H_1 = \{e\}$, $H_2 = \{\pm 1\}$, $H_3 = \{\pm 1, \pm i\}$
$H_4 = \{\pm 1, \pm j\}$, $H_5 := \{\pm 1, \pm k\}$, Q_8.

T/F whether $H = \{1, i\}$ is a subgroup of Q_8.

Example: $G = GL_2(\mathbb{R})$: 2×2 invertible matrices with real entries.

$$G = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : ad - bc \neq 0 \right\}.$$

$$H = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : ad \neq 0 \right\}.$$

H is a subgroup of G.

Let $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}, \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix} \in H$.
$\Rightarrow ad \neq 0,\ a'd' \neq 0$

(i) $$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix} = \begin{pmatrix} aa' & ab' + bd' \\ 0 & dd' \end{pmatrix}$$

Now, since $aa'dd' \neq 0$
$ad \neq 0$, $a'd' \neq 0$

(ii) $$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}^{-1} = \begin{pmatrix} \frac{d}{ad} & \frac{-b}{ad} \\ 0 & \frac{a}{ad} \end{pmatrix} \in H.$$

Now, let $$K = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{R} \right\}.$$

Show that K is a subgroup of G.

Exercise: Find all the subgroups of S_3.

Thm: Intersection of two subgroups of a group G is also a subgroup.

Proof: let H_1 and H_2 be subgroups of a group G.

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

(i)
$\Rightarrow a, b \in H_1 \; , \; a, b \in H_2$
$\Rightarrow a \cdot b \in H_1 \; , \; a \cdot b \in H_2$
$\Rightarrow ab \in H_1 \cap H_2$

(ii)
$a \in H_1 \; , \; a \in H_2$
$\Rightarrow a^{-1} \in H_1 \; , \; a^{-1} \in H_2$
$\Rightarrow a^{-1} \in H_1 \cap H_2$

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

Note: Union of two subgroups may not be a subgroup.

Example: $G = \mathbb{Z}$

$H_1 = 2\mathbb{Z}$ $\quad$ $H_2 = 3\mathbb{Z}$

$3 \in 3\mathbb{Z}, \quad 2 \in 2\mathbb{Z}$

$\Rightarrow \quad 3, 2 \in 3\mathbb{Z} \cup 2\mathbb{Z}$

But $\quad 3 + 2 \notin 3\mathbb{Z} \cup 2\mathbb{Z}$

$5 \notin 3\mathbb{Z} \cup 2\mathbb{Z}$

Because '5' is neither multiple of 2 nor multiple of 3.

However,:

Thm: Union of two subgroups is a subgroup iff one of them is contained in other.

Proof: Let G be a group and let H_1 and H_2 be subgroups of G.

We have to show that $H_1 \cup H_2$ is a subgroup iff either $H_1 \subseteq H_2$ or $H_2 \subseteq H$.

Clearly, if $H_1 \subseteq H_2$ or $H_2 \subseteq H$ then $H_1 \cup H_2 = H_1$ or H_2, which is a subgroup.

Conversely, let $H_1 \cup H_2$ is a subgroup of G.

Claim $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$.

So, assume $H_1 \not\subseteq H_2$. We show that $H_2 \subseteq H_1$.

Now, since $H_1 \not\subseteq H_2$ so $\exists\, a \in H_1$ s.t. $a \notin H_2$.

Claim: $H_2 \subseteq H_1$

So, let $b \in H_2$

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

$\Rightarrow ab^{-1} \in H_1 \cup H_2$ (since $H_1 \cup H_2$ is a subgroup).

$\Rightarrow ab^{-1} \in H_1$ or $ab^{-1} \in H_2$

If $ab^{-1} \in H_2$

$\Rightarrow ab^{-1} b \in H_2$ (since $b \in H_2$)

$\Rightarrow a \in H_2$

This is absurd to our assumption.

Hence, $ab^{-1} \notin H_2$

So, $ab^{-1} \in H_1$

$\Rightarrow a^{-1} a \cdot b^{-1} \in H_1$ (since $a \in H_1$)

$\Rightarrow b^{-1} \in H_1 \Rightarrow (b^{-1})^{-1} \in H_1$

$\Rightarrow b \in H_1$

$\Rightarrow b \in H_2 \Rightarrow b \in H_1$

$\Rightarrow \boxed{H_2 \subseteq H_1}$

#.

Thm: let G be a group. A non-empty finite subset H of G is a subgroup iff $a, b \in H \Rightarrow a \cdot b \in H$.

Proof: If H is a subgroup then clearly $a, b \in H \Rightarrow a \cdot b \in H$.

Conversly, now suppose H is a finite subset of G such that $a, b \in H \Rightarrow a \cdot b \in H$.

We just need to show that if $a \in H$ then $a^{-1} \in H$ to show H is a subgroup.

let $H = \{a_1, a_2, \dots, a_n\}$

Consider, $a_i, a_i^2, a_i^3, \dots$ —(1)

Since, H is finite and all of $a_i^n \in H$, so so some terms among (1) will be repeated.

So, $a_i^m = a_i^n$ for some m and n. with $m > n \geq 1$

$\Rightarrow a_i^{m-n} = e$ [Because cancellation holds in H]

$\Rightarrow a_i \cdot a_i^{m-n-1} = e$

$\Rightarrow (a_i)^{-1} = a_i^{m-n-1}$ Hence result. #.

Def: Number of elements present in a group is called order of the group ($O(G)$).

Def: (order of an element) : let G be a group, and $a \in G$. If there is a positive integer 'n' s.t. $a^n = e$, then we say 'a' has finite order.

The smallest among such positive integers is called order of 'a'. If order of 'a' is m then we say $O(a) = m$.

Example:

If no such positive integer exists such that $a^n = e$, then we say that 'a' has infinite order.

Example: $O\left(\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\right) = ?$

2.

$$O\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = 3.$$

Example: $\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{6}\}$

$O(\bar{1}) = 6, \quad O(\bar{2}) = 3, \quad \ldots$

Example:

$G = Q_8$

$O(-1) = 1, \quad O(i) = 4, \ldots$

Def: (Cyclic group): Let G be a group. If there exists an element $a \in G$ such that $G = \{a^i : i \in \mathbb{Z}\}$ then G is called a cyclic group, and 'a' is called the generator of G.

If G is a cyclic group with generator 'a', then we denote this as $G = \langle a \rangle$.

Example: $(\mathbb{Z}, +)$

$\mathbb{Z} = \langle 1 \rangle$.

Example: $(\mathbb{Z}_4, +_4)$

$\langle \bar{1} \rangle$

Example: $(\mathbb{Z}_n, +_n)$

$\mathbb{Z}_n = \langle \bar{1} \rangle$.

Example: Find all the generators of $(\mathbb{Z}_6, +_6)$.

Remark: A cyclic group may have many generators. In particular if 'a' is a generator of G, then a^{-1} is also a generator.

Thm: Every cyclic group is abelian.

Recall: A group $(G, *)$ is called abelian iff $\forall\, a, b \in G$, $a * b = b * a$.

Proof: Let G be a cyclic group having 'a' as a generator.

i.e. $G = \langle a \rangle$.

Let $x, y \in G$, $\Rightarrow$ $x = a^m$, $y = a^n$ for some $m, n \in \mathbb{Z}$.

$\Rightarrow x \cdot y = a^m \cdot a^n = a^{m+n} = a^{n+m} = a^n \cdot a^m = y \cdot x$.

$\Rightarrow$ G is abelian.

However, note that not every abelian group is cyclic.

Example: $G = \{e, a, b, c\}$, $a^2 = e = b^2 = c^2$

$ab = c = ba$

$ac = b = ca$

$bc = a = cb$.

Recall:

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

This group does not have any generator.

This group has a particular name,

Klein Four group

V_4. Klein Four group

$\Rightarrow$.

Result: An infinite cyclic group has exactly two generators.

Proof: Let G be an infinite cyclic group. Let a and b be generators of G, i.e.

$$G = \langle a \rangle = \langle b \rangle$$

$$\Rightarrow \quad \begin{matrix} a = b^m \\ b = a^n \end{matrix} \quad \text{for some } m, n \in \mathbb{Z}.$$

$$\Rightarrow \quad a = (a^n)^m = a^{nm}$$

$$\Rightarrow \quad a^{nm-1} = e$$

$$\Rightarrow \quad nm - 1 = 0$$

$$\Rightarrow \quad nm = 1$$

$$\Rightarrow \quad n = m = 1 \quad -(\text{I})$$

$$\text{or,} \quad n = m = -1 \quad -(\text{II})$$

$$(\text{I}) \Rightarrow a = b$$

$$(\text{II}) \Rightarrow \underline{a = b^{-1}}$$

So, G has only two generators.

Note: (1) Let G be a group. Let $a \in G$ with $o(a) = n$. Then $|\{a^i : i \in \mathbb{Z}\}| = n$.

Claim: $\{a^i : i \in \mathbb{Z}\} = \{e, a, a^2, a^3, \dots, a^{n-1}\}$.

Clearly, $\{e, a, a^2, \dots, a^{n-1}\} \subseteq \{a^i : i \in \mathbb{Z}\}$.

Now, let $x \in \{a^i : i \in \mathbb{Z}\}$.

$\Rightarrow$ $x = a^t$ for some $t \in \mathbb{Z}$.

Now, $\underbrace{t = nt + r}_{\Downarrow}$ $0 \leq r < n$

Division algorithm

$\Rightarrow$ $a^t = a^{nt+r} = a^{nt} \cdot a^r$

$\Rightarrow$ $a^t = (a^n)^t \cdot a^r$

$= e \cdot a^r$

$= a^r$

$\Rightarrow$ $x = a^t = a^r \in \{e, a, a^2, \dots, a^{n-1}\}$.

Hence, $\{a^i : i \in \mathbb{Z}\} = \{e, a, a^2, \dots, a^{n-1}\}$.

Result: Let G be a finite cyclic group of order n. Then order of generators of G is n.

Proof: Let $a \in G$ be the generator of G, i.e.

$G = \langle a \rangle = \{a^i : i \in \mathbb{Z}\}$.

Let $O(a) = m$. If $m < n$ then by the previous result $\{a^i : i \in \mathbb{Z}\}$ has just m elements, but we have assumed G has n-elts. This is absurd.

$\Rightarrow m = O(a) \geq n$.

If $m > n$, then using the same argument, we arrive at a contradiction.

Hence, $m = n$.

Result: Order of a finite cyclic group is equal to the order of its generator.

Result: If a finite group of order n contains an element of order n, then the group is cyclic.

Proof: let $O(G) = n$, and $a \in G$ s.t. $O(a) = n$

Claim: $G = \langle a \rangle = \{a^i : i \in \mathbb{Z}\}$.

But $O(a) = n$

$\Rightarrow \langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$.

We have proved that $|\langle a \rangle| = n$.

Now, $\langle a \rangle$ is a subgroup of G having n elts, and G has also n elements.

So, $G = \langle a \rangle$ and G is cyclic.

#.

Theorem : let G be a cyclic group. Then every subgroup of G is also cyclic.

Proof: let $G = \langle a \rangle$, and H be a subgroup of G.

If $H = \{e\}$, then clearly H is cyclic.

So, assume H is a non-trivial subgroup of G.

Note that each element of H is a power of 'a'.

let, 'n' be the least positive s.t. $a^n \in H$.

Claim, $H = \langle a^n \rangle$.

Clearly, $\langle a^n \rangle = \{(a^n)^i : i \in \mathbb{Z}\} \subseteq H$, since H is a subgroup of G.

Now, we show that $H \subseteq \langle a^n \rangle$.

So, let $x \in H$, but since $x \in G$, so

$x = a^{n_1}$ for some $n_1 \in \mathbb{Z}$.

Now, since division is possible in $\mathbb{Z}$, so

So,

$$n_1 = n\cdot q + r, \quad \text{where,} \quad 0 \le r < n.$$

Hence,

$$a^{n_1} = a^{nq+r} = a^{nq} \cdot a^{r}$$

$$\Rightarrow \quad a^{r} = a^{n_1} \cdot a^{-nq}$$

If $0 < r < n$, so $a^r \in H$ since

$a^{-nq} \in H$, $a^{n_1} \in H$

But this is absurd, since we have choosen 'n' smallest s.t. $a^n \in H$.

But we are getting $r < n$ s.t. $a^r \in H$.

Hence $r = 0$ and $a^{n_1} = a^{nq} = (a^n)^q$

$$\Rightarrow \quad x = (a^n)^q$$

$$\Rightarrow \quad x \in \langle a^n \rangle.$$

Hence $H = \langle a^n \rangle$

//

Some results on order :

(1) Let G be a group and $a \in G$. Assume ~~$a^n = e$~~ ~~and~~ $O(a) = m$, then $a^n = e$ iff $m | n$ (m divides n).

If $m | n \Rightarrow n = m \cdot q$

$\Rightarrow a^n = a^{m \cdot q} = (a^m)^q = e^q = e$

Conversely, let $a^n = e$. Now, $n = mq + r$, $0 \leq r < m$

$\Rightarrow a^n = a^{mq} \cdot a^r = e$

$\Rightarrow \underbrace{(a^m)^q}_{e} \cdot a^r = e \Rightarrow$

$\Rightarrow a^r = e$

If $0 < r < m$, then $a^r = e$. But this is obsurd to the fact that 'm' is the least positive integer s.t. $a^m = e$.

Hence, $r = 0$ and $n = mq$. So, $m | n$.

(2) Let G be a group and $a \in G$. If $O(a) = m$ then $\forall x \in G$ $O(xax^{-1}) = m$.

Assume $O(xax^{-1}) = n$.

Since, $O(a) = m$, so $\underbrace{xax^{-1} \cdot xax^{-1} \cdots \cdot xax^{-1}}_{m}$

$= x a^m x^{-1} = x \cdot e x^{-1} = e$

$\Rightarrow (xax^{-1})^m = e$

$\Rightarrow n \mid m$ from result-1.

Now, Since $O(xax^{-1}) = n$

$\Rightarrow \underbrace{xax^{-1} \cdot xax^{-1} \cdots xax^{-1}}_{n} = e$

$\Rightarrow x a^n x^{-1} = e$

$\Rightarrow \cancel{x} a^n \cancel{x^{-1}} = \cancel{x x^{-1}}$

$\Rightarrow a^n = e$

$\Rightarrow m/n$

Hence n/m, $m/n \Rightarrow m = n$.

(3) Let G be a group, $a, b \in G$. If $O(ab)$ is finite then $O(ab) = O(ba)$.

Note that $ba = a^{-1} \underline{ab} a = a^{-1}(ab)a^{-1}$

From previous result $O(ab) = O(ba)$.

(4) Let G be an abelian group, and $a, b \in G$. If $O(a) = m$, $O(b) = n$ then $O(ab) / lcm(m, n)$.