oups and semigroups :-

Binary operation :

A binary operation on a non-empty set A is an function defined from $A \times A$ to A. That is, a binary operation on a non-empty set A that assigns to every ordered pair of elements of A a unique element of A. A binary operation is denoted by $*$ and the element of A that is assigned to the pair (a,b) is denoted by $a*b$. If $*$ is a binary operation on A, we say that A is closed under $*$. A nonempty set on which a binary operation is defined is called a groupoid under that operation.

Ex①: On the set Z of all integers, the usual addition, subtraction and multiplication are binary operations because, for any $a,b \in Z$, $a+b \in Z$, $a-b \in Z$, $a \times b \in Z$. Similarly, the usual addition, subtraction and multiplications are binary operations on set of real and complex numbers.

Ex②: On the set Z^+ of non-negative integers, the usual addition and multiplication are binary operations but the usual subtraction is not a binary operation. Because, for any $a,b \in Z^+$ $a+b \in Z^+$, and $a \times b \in Z^+$, whereas $a-b$ need not belong to Z^+. Hence, Z^+ is closed under addition and multiplication operations but not closed under subtraction operation.

Ex③: On the power set $P(S)$ of a non-empty set S, the set union and the set intersection are binary operations. Because, of $A, B \in P(S)$, then $A \cup B \in P(S)$ and $A \cap B \in P(S)$.

Properties of binary operations:

Let $*$ be a binary operation on a set A. Then $*$ is said to be (i) Commutative if $a*b = b*a$ for all $a, b \in A$.
(ii) Associative if $a*(b*c) = (a*b)*c$ for all $a, b, c \in A$.
(iii) Idempotent if $a*a = a$ for $a \in A$.

Ex ①: On the set Z, the usual addition and multiplication operations are commutative and associative. On the same set, the subtraction operation is neither commutative nor associative. for ex, $(2-3) \neq (3-2)$ and $(2-3)-5 \neq 2-(3-5)$.

Ex ②: On a power set, the set union and set intersection are commutative, associative and Idempotent operation.

Ex ③: On the set R of all real numbers, suppose a binary operation $*$ is defined by $a*b = a*|b|$. Then $b*a = b*|a|$. Evidentaly, $b*a \neq a*b$, for ex, $a=2$ & $b=-3$, then $a*b = 2\times 3 = 6$ and $b*a = -3\times 2 = -6$. Therefore, the operation is not commutative. But it is associative.

$$\begin{aligned}(a*b)*c &= (a*|b|)*|c| \\ &= a*(|b|*|c|) \\ &= a*|b|*|c| \\ &= a*(b*c)\end{aligned}$$

If the set A is finite on which the binary operation $*$ is defined, then it can be represented by a multiplication table. for ex, $A = \{a_1, a_2, a_3, a_4\}$

$*$	a_1	a_2	a_3	a_4
a_1	a_1	a_3	a_2	a_4
a_2	a_4	a_1	a_2	a_3
a_3	a_3	a_2	a_4	a_1
a_4	a_4	a_2	a_1	a_3

Semigroup, Abelian semigroup and Monoids :-

A non-empty set which is closed under an associative binary operation is called a semigroup under that operation.

If the binary operation is also commutative in addition to the associative operation, then it is called as Abelian semigroup.

If S be semigroup under a binary operation $*$ then S is said to be monoid if there exists an element $e \in S$ such that $e*a = a*e = a$, for all $a \in S$. This e is called identity element in S.

Ex(1) ①: $(\mathbb{Z}, +)$: Semigroup and also Abelian semigroup because $+$ is associative & commutative.

$(\mathbb{Z}, \times)$: This is also commutative semigroup as of $(\mathbb{Z}, +)$

$(\mathbb{Z}, -)$: This is not semigroup.

Ex ②: $(P(S), \cap)$: } Commutative semigroups.
$(P(S), \cup)$: }

Ex ③: $(\mathbb{Z}, +)$ is a monoid with identity element 0.
$(\mathbb{Z}, \times)$ is a monoid with identity elmt 1.
$(P(S), \cup)$ is a monoid with ϕ as identity.

Groups: Definition, Examples and Elementary properties.

Definition:- If G is a nonempty set and $*$ is a binary operation on G, then $(G, *)$ is said to be a group if the following conditions are satisfied.

1) For all $a, b \in G$, $a * b \in G$ (G is closed under $*$).
2) For all $a, b, c \in G$, $a * (b * c) = (a * b) * c$ (The associative property)
3) There exists $e \in G$ with $a * e = e * a = a$, for all $a \in G$. (The existence of an Identity)
4) For each $a \in G$ there is an element $b \in G$ such that $a * b = b * a = e$ (Existence of Inverse).

In addition to the above, if $a * b = b * a$ for all $a, b \in G$, then G is called a Commutative or Abelian group.

Ex①: $(Z, +)$ is a monoid with 0 as the identity. With each $a \in Z$, there is $-a$, the negative of a, such that $a + (-a) = (-a) + a = 0$. Therefore $(Z, +)$ is a group, with 0 as the identity and $-a$ as an inverse of a. This is also an abelian group because $a + b = b + a$.

Ex②: $(Z, -)$ is not a group because, it is not associative.

Ex③: $(Z, \times)$ is not a group because there is no element $a^{-1} \in Z$ such that $a \times a^{-1} = a^{-1} \times a = 1$, where 1 is the identity element for multiplication.

Ex④: $(Q, \times)$: The set of all non-zero rational numbers (real) is an abelian group under multiplication with 1 as the identity and $1/a$ as the inverse of a.

Ex⑤: Let $A = \{0, 1\}$ and the operation $*$ on A defined by the following operation table:

$*$	0	1
0	0	1
1	1	0

This is an abelian group, with 0 as identity and each element is inverse to itself.

Ex (6): Let $A = \{1, -1, i, -i\}$, the set of all fourth roots of unity. The operation table for the usual multiplication on A is as shown below.

×	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

* From the above table, it is evident that A is closed under ×.
* Complex numbers are ~~closed~~ associative under multiplication, and as well as commutative.
* By observing in the table, it is seen that 1 is the identity element.
* for each element of A there is an inverse

for 1, inverse is 1
-1 inverse is -1
i inverse is $-i$
$-i$ inverse is i

∴ $(A, \times)$ is an abelian group.

Ex (7): For $n \in Z^+$, $n > 1$, then $(Z_n, +)$ is an abelian group.

for instance $n = 6$.

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Inverse of $0 \to 0$
$1 \to 5$
$2 \to 4$
$3 \to 3$
$4 \to 2$
$5 \to 1$

$(Z_6, +)$ is closed under +. associative, commutative and the identity is 0.

Finite groups :- For every group G the number of elements in G is called the order of G and this is denoted by $|G|$. When the number of elements in a group is not finite we say that G has infinite order.

Theorem ①: For every group G

a) the identity of G is unique.
b) the inverse of each element of G is unique.
c) if $a, b, c \in G$ and $ab = ac$, then $b = c$. [Left cancellation property]
d) if $a, b, c \in G$ and $ba = ca$, then $b = c$ [Right cancellation property]

Proof : (a) If $(G, *)$ has two identity elements e_1 & e_2.
Since e_1 is an identity element, then for all $a \in G$, $a * e_1 = e_1 * a = a$. Since $e_2 \in G$

$$e_1 * e_2 = e_2 * e_1 = e_2$$

Similarly, e_2 is also identity elemt of G & $e_1 \in G$

$$e_2 * e_1 = e_1 * e_2 = e_1$$

$\therefore e_1 = e_2$ // There is only one identity element.

(b) Suppose a' and a'' are two inverse of an element $a \in G$. Then

$$\begin{aligned} a' &= a'e \quad (\text{because } x = xe \text{ in a group}) \\ &= a'(aa'') \quad (\text{because } a'' \text{ is an inverse of } a) \\ &= (a'a)a'' \quad (\text{because } * \text{ is associative}) \\ &= ea'' \quad (\text{because } a' \text{ is inverse of } a) \\ &= a'' \end{aligned}$$

$\therefore$ The two inverses cannot be different.

(c) $ab = ac$

$\Rightarrow a^{-1}(ab) = a^{-1}(ac)$

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

$\Rightarrow eb = ec$

$\Rightarrow b = c$

(d) $ba = ca$

$\Rightarrow (ba)a^{-1} = (ca)a^{-1}$

$\Rightarrow b(aa^{-1}) = c(aa^{-1})$

$\Rightarrow be = ce$

$\Rightarrow b = c$

Problem ①: Let G be the set of all non-zero real numbers and let $a*b = \frac{1}{2}ab$. S.T. $(G, *)$ is an abelian group.

Soln: For any two non-zero real numbers a and b, $\frac{1}{2}(ab)$ is also non-zero real number. Therefore, for any $a, b \in G$, $a*b \in G$. That is G is closed under $*$.

For any $a, b, c \in G$, we have

$$a*(b*c) = a*(\tfrac{1}{2}bc) = \tfrac{1}{2}(\tfrac{1}{2}a(bc)) = \frac{a(bc)}{4}$$

$$= \tfrac{1}{2}((\tfrac{1}{2}ab)c) = \tfrac{1}{2}(a*b)c = (a*b)*c$$

$\therefore *$ is associative.

For any $a \in G$, we have

$$a*2 = 2*a = \tfrac{1}{2}(2a) = a$$

$\therefore 2$ is identity under $*$, and $2 \in G$.

For any $a \in G$, if we choose $a' = 4/a$, then $a' \in G$ & $a*a' = \frac{1}{2}(aa') = \frac{1}{2}4 = 2 =$ identity elmt.

$\therefore \frac{4}{a}$ is inverse for all $a \in G$. Hence $(G, *)$ is group

Problem ②: Let G be the set of real numbers not equal to -1 and $*$ be the binary operation defined by $a*b = a+b+ab$. S.T. $(G,*)$ is an abelian group.

Soln: when $a \neq -1$ & $b \neq -1$, w.k.t $a+b+ab \neq -1$.
Hence, G is closed under $*$.

For any $a,b,c \in G$, we have

$$a*(b*c) = a*(b+c+bc)$$
$$= a+(b+c+bc)+a(b+c+bc)$$
$$= a+b+c+bc+ab+ac+abc$$
$$= [\{a+b+ab\}+c]+(a+b+ab)c$$
$$= (a+b+ab)*c$$
$$= (a*b)*c \quad \therefore * \text{ is associative.}$$

For any $a \in G$, we have

$$a*0 = a+0+a0 = a = 0+a+0.a = 0*a$$
$\therefore 0$ is the identity in G.

For any $a \in G$, if we choose $a' = \frac{-a}{(1+a)}$, then $a' \in G$

$$a*a' = a+a'+aa' = a-\frac{a}{1+a}-\frac{a^2}{1+a}$$
$$= \frac{a(1+a)-a-a^2}{1+a} = \frac{0}{1+a} = 0 = a'*a$$

$\therefore a' = -a/1+a$, is the inverse of a under $*$.

finally, $a*b = a+b+ab = b+a+ba = b*a$

$\therefore$ Commutative.

Hence, $(G,*)$ is abelian group.

Problem ③: Let G_1 be a finite group with ~~identity e~~ binary operation $*_1$ and G_2 is a group with binary operation $*_2$. Consider the cartesian product $G_1 \times G_2$ and on this product define a binary operation $*_3$ by $(a,b) *_3 (c,d) = ((a *_1 c), (b *_2 d))$. S.T $(G_1 \times G_2, *_3)$ is a group. If G_1 & G_2 are abelian, then $G_1 \times G_2$ is abelian.

Soln: When $(a,b), (c,d) \in G_1 \times G_2$, we have $a, c \in G_1$ & $b, d \in G_2$. so that $a *_1 c \in G_1$ & $b *_2 d \in G_2$ $\therefore (a *_1 c, b *_2 d) \in G_1 \times G_2$

$\therefore (a,b) *_3 (c,d) \in G_1 \times G_2$ $\therefore G_1 \times G_2$ is closed under $*_3$.

For $(a,b), (c,d), (h,k) \in G_1 \times G_2$, then

$$(a,b) *_3 ((c,d) *_3 (h,k)) = (a,b) *_3 (c *_1 h, d *_2 k)$$
$$= (a *_1 (c *_1 h), b *_2 (d *_2 k))$$
$$= ((a *_1 c) *_1 h, (b *_2 d) *_2 k)$$
$$= (a *_1 c, b *_2 d) *_3 (h,k)$$
$$= ((a,b) *_3 (c,d)) *_3 (h,k)$$

$\therefore G_1 \times G_2$ is associative.

Let e_1 and e_2 be identity elements in G_1 & G_2 respectively, then for any $(a,b) \in G_1 \times G_2$, we have

$$(a,b) *_3 (e_1, e_2) = (a *_1 e_1, b *_2 e_2) = (a,b)$$

and $(e_1, e_2) *_3 (a,b) = (e_1 *_1 a, e_2 *_2 b) = (a,b)$

hence, (e_1, e_2) is the identity in $G_1 \times G_2$ under $*_3$

for any $(a,b) \in G_1 \times G_2$, $(a^{-1}, b^{-1}) \in G_1 \times G_2$ where a^{-1} is the inverse of G_1 and b^{-1} is in G_2, inverse of b.

$$(a,b) *_3 (a^{-1}, b^{-1}) = (a *_1 a^{-1}, b *_2 b^{-1}) = (e_1, e_2)$$

& $(a^{-1}, b^{-1}) *_3 (a,b) = ((a^{-1} *_1 a), (b^{-1} *_2 b)) = (e_1, e_2)$

Suppose G_1 & G_2 are abelian groups. Take any
$(a,b) *_3 (c,d) = (a *_1 c \quad b *_2 d) = (c *_1 a, d *_2 d) = (c,d) *_3 (a,b)$
$\therefore$ it is commutative. Therefore $G_1 \times G_2$ is abelian.

SUBGROUPS :-

A non-empty subset H of a group G is called subgroup of G whenever H is a group under the binary operation of G.

NOTE: ① For any group G, $e \in G$, Hence $\{e\} \subseteq G$. Also $\{e\}$ is a group under the operation in G.
$\therefore \{e\}$ is a subgroup of G.

② For any group G, $G \subseteq G$. Since G is a group it follows that G is a subgroup of G. Hence, every group is a subgroup to itself.

Ex ①: Under the usual addition, the set of all even integers is a subgroup of all integers.

Ex ②: Under the usual multiplication, the set of all non-zero rational numbers is a subgroup of the group of all non-zero real numbers.

Theorem - ①:- If H is a non-empty subset of a group G, then H is a subgroup of G iff for all $a,b \in H$, $ab \in H$ & for all $a \in H$, $a^{-1} \in H$.

Proof: If H is a subgroup of G, according to definition, H is group under the same binary operation of G. Hence, it satisfies all the group conditions. Conversely, Let $H \subseteq G$ $\neq \phi$ with satisfying the above two conditions. for all $a,b,c \in H$, $(ab)c = a(bc)$ in G
$\therefore (ab)c = a(bc)$ in H. (H is associative). Finally, as $H \neq \phi$, let $a \in H$. By condition $a^{-1} \in H$ & $aa^{-1} = e \in H$, so H contains the identity element and hence, H is group.

Theorem – (2): If G is a group and $\emptyset \neq H \subseteq G$, with H finite, then H is a subgroup of G iff H is closed under the binary operation of G.

Proof:- If H is a subgroup of G, then H is closed under the binary operation of G.

Conversely, let H is a finite nonempty set of G that is closed.

→ If $a \in H$, then $aH = \{ah \mid h \in H\} \subseteq H$ because of the closure condition.

→ By Cancellation property, $ah_1 = ah_2 \Rightarrow h_1 = h_2$, so $|aH| = |H|$, it follows that H being finite that $aH = H$.

→ As $a \in H$, there exists $b \in H$ with $ab = a$. But in G $ab = a = a.e$ $\therefore e = b$ and H contains the identity.

→ Since, $e \in H = aH$, there is an element $c \in H$ such that $ac = e$. Then $(ca)^2 = (ca)(ca) = (c(ac))a$ $= (ce)a = ca = (ca)e$, so $ca = e$ and $c = a^{-1} \in H$.

Therefore H is a subgroup of G.

Homomorphisms, Isomorphisms, and Cyclic groups.

Definition(1):- If (G, o) and $(H, *)$ are groups and $f: G \to H$, then f is called a group homomorphism if for all $a, b \in G$, $f(a o b) = f(a) * f(b)$.

Definition(2):- If $(G, o) \to (H, *)$ is a homomorphism, we call f an isomorphism if it is one-to-one and onto. In this case G and H are said to be isomorphic groups.

Definition(3):- A group G is called cyclic if there is an element $x \in G$ such that for each $a \in G$, $a = x^n$ for some $n \in \mathbb{Z}$.

Ex ①: Let $(R,+)$ and $(R^+,\times)$ are the groups. Define $f: R \to R^+$ by $f(x) = e^x$ for all $x \in R$.
Then for all $a,b \in R$, we have

$$f(a+b) = e^{a+b} = e^a \times e^b = f(a) \times f(b)$$

Therefore f is a homomorphism.
Let $c \in R^+$. Then $\log c \in R$ and $f(\log c) = e^{\log c} = c$.
Every element in R^+ has a preimage in R under f.
Hence, f is onto.

For, $a,b \in R$

$$f(a) = f(b)$$
$$\Rightarrow e^a = e^b$$
$$\Rightarrow a = b \quad \text{i.e } a \text{ \& } b \text{ can't be different.}$$

Therefore f is one-to-one. Accordingly f is an isomorphism.

Ex ②: Let G be a group with e as its identity. Consider the function $f: G \to G$ defined by $f(x) = e$ for all $x \in G$. Then, for any $a,b \in G$, we have $f(a) = e$, $f(b) = e$ and $f(ab) = e$ so that $f(ab) = e = e.e = f(a).f(b)$. Therefore f is a homomorphism. This is not isomorphism.

Ex ③: Let G be a group. Consider the function $f: G \to G$ defined by $f(x) = x^2$ for all $x \in G$. Then for any $a,b \in G$, we have $f(a) = a^2$, $f(b) = b^2$ and $f(ab) = (ab)^2$. Therefore, $f(ab) = f(a).f(b)$ holds iff $(ab)^2 = a^2b^2$. That is, f is a homomorphism iff $(ab)^2 = a^2b^2$.

Ex ④: In the group $U_4 = \{1, -1, i, -i\}$ under usual multiplication, every element is an integral power i.

$1 = i^4$, $-1 = i^2$, $i = i^1$, $-i = i^3$. Therefore this group is a cyclic group, generated by i, denoted as $\langle i \rangle$. This is also generated by $-i$ i.e $\langle -i \rangle$.

$(-i)^4 = 1$, $(-i)^2 = -1$, $(-i)^1 = -i$, $(-i)^3 = (-i)^2 \cdot (-i) = i$

Ex ⑤: P.T. every cyclic group is abelian.

⇒ Let G be a cyclic group with g as a generator. Take, any $a, b \in G$. Then $a = g^r$ & $b = g^s$ for some integers r and s.

i.e $ab = g^r g^s = g^{r+s} = g^{s+r} = g^s g^r = ba$.

Therefore, G is abelian.

Ex ⑥: $U_9 = \{1, 2, 4, 5, 7, 8\}$

$\circ$	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

Here, we find that $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 7$, $2^5 = 5$, $2^6 = 1$. Therefore $(U_9, \circ)$ is a cyclic group of order 6 and is generated by 2. i.e $U_9 = \langle 2 \rangle$. It is also true that $U_9 = \langle 5 \rangle$ because, $5^1 = 5$, $5^2 = 7$, $5^3 = 8$, $5^4 = 4$, $5^6 = 1$, $5^5 = 2$

Some important results:

Theorem (1): If f is an onto homomorphism from G_1 to G_2. Then if G_1 is abelian then G_2 is also abelian.

Proof: Take any $x, y \in G_2$. Since f is onto, there exists $a, b \in G_1$ such that $f(a) = x$, $f(b) = y$ then

$$\begin{aligned} x *_2 y &= f(a) *_2 f(b) \\ &= f(a *_1 b) \quad ; \text{ because } f \text{ is a homomorph.} \\ &= f(b *_1 a) \quad ; \ *_1 \text{ is commutative or } G_1 \text{ is abelian} \\ &= f(b) *_2 f(a) = y *_2 x. \end{aligned}$$

This shows that $*_2$ is commutative. Hence $(G_2, *_2)$ is an abelian group.

Theorem (2): If f is a homomorphism from G_1 to G_2, then if f is onto and e is the identity of G_1 and e_2 is the identity G_2, then we have $f(e_1) = e_2$.

Proof: Take any $y \in G_2$. Then, since f is onto, there exists $a \in G_1$ such that $f(a) = y$.

Since $a = a *_1 e_1 = e *_1 a$, we have

$$y = f(a) = f(a *_1 e_1) = f(a) *_2 f(e) = y *_2 f(e)$$

& $$y = f(a) = f(e *_1 a) = f(e) *_2 f(a) = f(e) *_2 y$$

Hence, for any $y \in G_2$, we have

$$y *_2 f(e) = f(e) *_2 y = y$$ i.e $f(e)$ is an identity in G_2. $\therefore f(e) = e_2$ //

Theorem -(3) :- If f is a homomorphism from a group G_1 to a group G_2, Then $f(a^{-1}) = (f(a))^{-1}$ for all $a \in G_1$.

proof :- for any $a \in G_1$, we have

$$f(a) *_2 f(a^{-1}) = f(a *_1 a^{-1}) = f(e_1) = e_2$$

$$f(a^{-1}) *_2 f(a) = f(a^{-1} *_1 a) = f(e_1) = e_2.$$

This shows that $f(a^{-1})$ is the inverse of $f(a)$ in G_2 i.e $f(a^{-1}) = (f(a))^{-1}$

Theorem -(4) :- If f is a homomorphism from a group G_1 to a group G_2, then if H_1 is a subgroup of G_1 then $H_2 = f(H_1)$ is a subgroup of G_2.

Proof :- Let $H_2 = f(H_1)$ is the image of H_1 under f. & $H_2 \subseteq G_2$. Take any $f(a), f(b) \in f(H_1)$, then $a, b \in H_1$ so that $ab^{-1} \in H_1$ because H_1 is a subgroup of G_1, also

$$f(a)(f(b))^{-1} = f(ab^{-1}) \in f(H_1)$$

$\therefore f(H_1)$ is a subgroup of G_2.

Theorem -(5) : If f is an isomorphism from G_1 onto G_2 then f^{-1} is an isomorphism from G_2 onto G_1.

Proof : Since, $f : G_1 \to G_2$ is an isomorphism, it is an One-to-one and onto homomorphism. Since, f is one-to-one and onto its inverse f^{-1} exists and is One-to-one function from G_2 to G_1 if $f^{-1} : G_2 \to G_1$

Take any $x, y \in G_2$. Then there exist $a, b \in G_1$ such that $f(a) = x$, $f(b) = y$. Then $f^{-1}(x) = a$, $f^{-1}(y) = b$.

Since $x, y \in G_2$, and G_2 is closed under $*_2$, we have

$$x *_2 y \in G_2, \text{ and}$$

$$\begin{aligned} f^{-1}(x *_2 y) &= f^{-1}(f(a) *_2 f(b)) \\ &= f^{-1}(f(a *_1 b)) \\ &= f^{-1} \circ f(a *_1 b) \\ &= a *_1 b \quad \because f^{-1} \circ f \text{ is identity fn.} \end{aligned}$$

$$\boxed{f^{-1}(x *_2 y) = f^{-1}(x) *_1 f^{-1}(y)}$$

$\therefore f^{-1}$ is a homomorphism from G_2 to G_1 and hence f^{-1} is a isomorphism from G_2 onto G_1.

Coset and Lagrange's theorem :-

COSETS :- If H is a subgroup of G, then for each $a \in G$, the set $aH = \{ah \mid h \in H\}$ is called a **left coset** of H in G. The set $Ha = \{ha \mid h \in H\}$ is a right coset of H in G. (9)

- If the binary operation in G is addition, then we write $a+H$ in place of aH, where $a+H = \{a+h \mid h \in H\}$.
- coset means it is left-coset unless otherwise specified.
- If the group is abelian, then no need to distinguish between left cosets and right cosets.

Ex: For $G = (Z_{12}, +)$ and $H = \{[0], [4], [8]\}$, then we have

$[0]+H = \{[0],[4],[8]\}$
$[1]+H = \{[1],[5],[9]\}$
$[2]+H = \{[2],[6],[10]\}$
$[3]+H = \{[3],[7],[11]\}$
$[4]+H = \{[4],[8],[0]\} = [8]+H$
$[5]+H = \{[1],[5],[9]\} = [9]+H$
$[6]+H = \{[6],[10],[2]\} = [10]+H$
$[7]+H = \{[7],[11],[3]\} = [11]+H.$

$\therefore ([0]+H) \cup ([1]+H) \cup ([2]+H) \cup ([3]+H)$ is a partition of G.

$(G_{12}, +)$

+	0	1	2	3	4	5	6	7	8	9	10	11
0	0	1	2	3	4	5	6	7	8	9	10	11
1	1	2	3	4	5	6	7	8	9	10	11	0
2	2	3	4	5	6	7	8	9	10	11	0	1
3	3	4	5	6	7	8	9	10	11	0	1	2
4	H	5	6	7	8	9	10	11	0	1	2	3
5	5	6	7	8	9	10	11	0	1	2	3	4
6	6	7	8	9	10	11	0	1	2	3	4	5
7	7	8	9	10	11	0	1	2	3	4	5	6
8	8	9	10	11	0	1	2	3	4	5	6	7
9	9	10	11	0	1	2	3	4	5	6	7	8
10												

If G is the group as in $(S_{12}, +)$, and $H = \{\pi_0, \pi_1, \pi_2\}$, the coset $r_1 H = \{r_1\pi_0, r_1\pi_1, r_1\pi_2\} = \{r_1, r_2, r_3\}$. Likewise we have $r_2 H = r_3 H = \{r_1, r_2, r_3\}$, whereas $\pi_0 H = \pi_1 H = \pi_2 H = H$. We see that $|aH| = |H|$ for each $a \in G$ and that $G = H \cup r_1 H$ is a partition of G.

Lemma ①: If H is a subgroup of the finite group G, then for all $a, b \in G$, a) $|aH| = |H|$ &
b) either $aH = bH$ or $aH \cap bH = \emptyset$.

Proof: Since $aH = \{ah \mid h \in H\}$, it follows that $|aH| \leq |H|$.

a) If $|aH| < |H|$, we have $ah_i = ah_j$ with h_i & h_j are distinct elements of H. By left cancellation property of G we then get the contradiction $h_i = h_j$, so $|aH| = |H|$.

b) If $aH \cap bH = \emptyset$, let $c = ah_1 = bh_2$ for some $h_1, h_2 \in H$. If $x \in aH$, then $x = ah$ for some $h \in H$, and so $x = (bh_2h_1^{-1})h = b(h_2h_1^{-1}h) \in bH$, and $aH \subseteq bH$.
Similarly, $y \in bH$ then $y = bh_3$, for some $h_3 \in H$,
$\therefore y = (ah_1h_2^{-1})h_3 = a(h_1h_2^{-1}h_3) \in aH$, so $bH \subseteq aH$.
Therefore aH and bH are disjoint or identical.

Theorem ①: Lagrange's theorem:
If G is a group of finite order n with H is a subgroup of G of order m. Then m divides n.

Proof:

If $H = G$ the result follows.

Otherwise if $|H| < |G|$ i.e $m < n$, and there exists an element $a \in G - H$. Since $a \notin H$, it follows that $aH \neq H$, and $aH \cap H = \phi$. If $aH \cup H = G$, then $|aH| + |H| = |G|$ $= 2|H|$ and the theorem follows.

If $aH \cup H \neq G$, there is an element $b \in G - (H \cup aH)$ such that $bH \cap H = \phi = bH \cap aH$ and $|bH| = |H|$. If $G = bH \cup aH \cup H$, so we have $|G| = 3|H|$, otherwise we are back to an element $c \in G$ with $c \notin bH \cup aH \cup H$. Since, the group is finite, this process terminates and we find that $G = a_1H \cup a_2H \cup a_3H \cup \cdots \cup a_kH$. Therefore, $|G| = k|H|$ and hence m divides n.

The following is the alternative way to prove Lagrange's theorem.

Let G be a group of order n, and let H be a subgroup of G of order m.

(i) Define the relation R on G as follows: If $a, b \in G$, then aRb if $a^{-1}b \in H$. Prove that R is an equivalence relation.

(ii) For $a, b \in G$, prove that aRb iff $aH = bH$.

(iii) If $a \in G$, prove that $[a]$ satisfies $[a] = aH$.

(iv) For each $a \in G$, prove that $|aH| = |H|$.

(v) Now establish the conclusion of Lagrange's theorem, namely that $|H|$ divides $|G|$.