5.Associative property is true. $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ is the identity element. $(M_2(z), +$ is a monoid.

5.2 Groups

If G is a non-empty set and $*$ is a binary operation, then $(G\ *)$ is called a group if the following conditions are satisfied,

1) **Closure Property,** $If \quad a, b \in G$, then $a * b \in G.$

2) **Associative Property,** $If \quad a, b, c \in G$, then $a * (b * c) = (a * b) * c$

3) Existence of Identity element
There exists an identity element $e \in$ G such that for any $a \in G,\ a * e = a = e * a$

4) Existence of Inverse element
For each $a \in G$, there exist $a^{-1} \in G$ such that $a * a^{-1} = e = a^{-1} * a$

Furthermore if $a * b = b * a$ for all $a, b \in G$, then G is called a commutative or Abelian group.

Example: The set Z of all integers with usual addition as operation is an abelian group.

Order of an element of a group

The order of an element a of a group G is the smallest positive integer n such that $a^n = e$. It is denoted by $o(a)$. If no such integer exists, we say that G is infinite order.

Let $\{1,-1,i,-i\}$ be a multiplication group with identity 1.

Then the order of the element 1 is 1 since $1^1 = 1$,

order of the element -1 is 2 since $(-1)^2 = 1$

order of the element i is 4 since $(i)^4 = 1$,

order of the element $-i$ is 4 since $(-i)^4 = 1$.

5.2.1 Sub Group

Let G be a group, $\varphi \neq H$ is a subset of G then H is a subgroup of G if H itself is a group under the same binary operation of G.

The group $(Z,+)$ is a subgroup of the group $(Q,+)$.

5.2.2 Cyclic Group

A Group $(G,*)$ is called a cyclic group if every element of G can be expressed as some power of a particular element $a \in G$. The element a is called the generator of the group G because for any $x \in G, x = a^n$ for some $x \in Z$.

For example, consider the group $G = \{1,-1,i,-i\}$ then $(G, .)$ is a cyclic group generated by i. Since $(i)^1 = i$, $(i)^2 = -1$, $(i)^3 = -i$, $(i)^4 = 1$.

$-i$ is also a generator of this group.

5.2.4 Symmetric Group

Let X be a non empty set. A permutation of X is a one-to-one function from X to X. The set G of all permutations on a nonempty set X under the binary operation $*$ of right composition of permutations, is a group called permutation group.

If $X = \{1,2,3 \dots .n\}$, the permutation group is also called symmetric group denoted by S_n. The number of elements of S_n is $n!$.

For example, let S_3 be the set all permutations on the set $S = \{1,2,3\}$ is a group under the operation of right composition of permutations.

5.2.5 Direct Produce of two groups

Let $(G, .)$ and $(H, *)$ be groups. Define a binary operation ,• on $G \times H$ by

$(g_1, h_1) \bullet (g_2, h_2) = (g_1 . g_2, h_1 * h_2)$ where $g_1, g_2 \in G$, $h_1, h_2 \in H$.Then $(G \times H, \bullet)$ is a group called direct product of G and H.

Theorem 5.2.1

For every group G prove that

a) The identity element of G is unique, b) The inverse of each element of G is unique.

Proof:

a) Assume that e_1, e_2 be the two identity elements in the group G.

Since e_1 is the identity element in G, and $e_2 \in G$, $e_1 e_2 = e_2 = e_2 e_1$ (1)

Since e_2 is the identity element in G, and $e_1 \in G$, $e_1 e_2 = e_1 = e_2 e_1$ (2)

From (1) and (2) $e_1 = e_2$. Hence the identity element in a group is unique.

b) Let $a \in G$, and suppose b and c are inverse elements of a. Since b is the inverse of a, $ab = e = ba$, Since c is the inverse of a, $ac = e = ca$ where e is the identity element of G. Then $b = eb = (ca)b = c(ab) = ce = c$. Hence the inverse element of G is unique.

Theorem 5.2.2

Let H is a nonempty subset of G. Then H is subgroup of G if and only if

a) for all $a, b \in H \Rightarrow ab \in H$ b) $a \in H \Rightarrow a^{-1} \in H$.

Proof:

Assume that H is a subgroup of G. Then H is a group under the same binary operation in G. Hence H satisfies all conditions of a group.

So, $a, b \in H \Rightarrow ab \in H$ (Closure property)

$a \in H \Rightarrow a^{-1} \in H$ (Existence of identity)

Conversely, assume that $\phi \neq H \subseteq G$ and H satisfying conditions $a, b \in H \Rightarrow ab \in H$, $a \in H \Rightarrow a^{-1} \in H$.

For all $a, b, c \in H \Rightarrow (ab)c = a(bc)$ in G so $(ab)c = a(bc)$ in H. So associative property is true in H.

If $a \in H \Rightarrow a^{-1} \in H$ by closure property, $aa^{-1} \in H \Rightarrow e \in H$ identity element exists in H. So H satisfies all the properties of a group. Therefore, H is a sub group of G.

Theorem 5.2.3

If G is a group and $\phi \neq H \subseteq G$with H is finite, then H is a subgroup of G if and only if H is closed under binary operation of G.

Proof:

Assume that $\phi \neq H \subseteq G$ and H is a finite subgroup of G. Prove that H is closed under binary operation of G. Since $H \subseteq G$ and H is a subgroup of G then H itself is a group under the same operation on G. Therefore, H is closed under the binary operation of G.

Conversely, assume that H is a finite subset of G and is closed under binary operation f G. ie, $a, b \in H \Rightarrow ab \in H$ for all $a, b \in H$. To prove that H is a subgroup of G.

Let $a \in H, a \in H \Rightarrow a.a \in H \Rightarrow a^2 \in H,\ a^3 \in H,\ a^4 \in H. \ldots a^n \in H. \ldots$ (by closure property). Since H is finite there must be repetitions in the collection.

That is, for some $r > s > 0,\ a^r = a^s$. By cancellation in G, $a^{r-s} \in e \in H$ is the identity element in H. So, identity element exists in H. Since $r - s - 1 \geq 0,\ a^{r-s-1} \in H \Rightarrow a^{r-s}\, a^{-1} \in H,\ \ e.a^{-1} \in H \Rightarrow a^{-1} \in H$. Hence inverse exist in H. Therefore, H is a subgroup of G.

Theorem 5.2.4

Let $(G, \cdot), (H, *)$ be groups with respective identities e_G, e_H. If $f: G \rightarrow H$ is a homomorphism, then

a) $f(e_G) = e_H$ b) $f(a^{-1}) = [f(a)]^{-1}$ for all $a \in G$

c) $f(a^n) = [f(a)]^n$ for all $a \in G$ and $n \in Z$.

d) $f(S)$ is a subgroup of H for each subgroup S of G.

Proof:

a) $e_H * f(e_G) = f(e_G)$ since e_H is the identity element in H.

$= f(e_G \cdot e_G)$ since e_G is the identity element in G.

$= f(e_G) * f(e_G)$ since f is a homomorphism.

Therefore, by right cancellation, $e_H = f(e_G)$.

b) Let $a, a^{-1} \in G$, $a \cdot a^{-1} = e_G$ is the identity in G. $f(a.a^{-1}) = f(e_G) = e_H$ is the identity in H. Since f is a homomorphism $f(a.a^{-1}) = f(a) * f(a^{-1}) = e_H$.

So the inverse of $f(a)$ is $f(a^{-1})$. So $[f(a)]^{-1} = f(a^{-1})$ for all $a \in G$

c) For all $a \in G$, by closure property, $a.a \in G$, $a.a.a \in G \ldots,$ $a^n = a.a.\ldots.a \in G$ by theorem 5.3.3.

Since f is a homomorphism, $f(a.a.\dots\dots n\ times) = f(a) * f(a) * \dots\dots n\ times$,

ie, $f(a^n) = [f(a)]^n$.

d) If S is a subgroup of $G, S \neq \emptyset,\ f(S) \neq \emptyset$. Let $x, y \in f(S)$. Then $x = f(a)$ and $y = f(b)$, for $a, b \in S$. Since S is a subgroup of G, $x * y = f(a) * f(b) = f(a \cdot b) \in f(S)$.

Finally, $x^{-1} = [f(a)]^{-1} = f(a^{-1}) \in f(S)$ since $a^{-1} \in S$. By theorem 5.2.2 $f(S)$ is a subgroup of H.

Proof $a, b \in f(H) \Rightarrow a = f(h_1),\ b = f(h_2)$

Theorem 5.2.5 $a, b \in f(H) \Rightarrow ab^{-1} \in f(H)$

$ab^{-1} = f(h_1)[f(h_2)]^{-1}$

Prove that every subgroup of a cyclic group is cyclic.

$= f(h_1 h_2^{-1}) = f(h)$

$f(h) \in f(H)$

Proof:

Let G be a cyclic group and a be the generator of G. Let H be the subgroup of G. Then each element of H has the form a^k for some $k \in Z$.

For $H \neq \{e\}$, let t be the smallest positive integer such that $a^t \in H$.

Let $b \in H \Rightarrow b = a^s$ for some $s \in H$. By division algorithm, $s = qt + r$ where $q, r \in Z$, $0 \leq r < t$.

So $a^s = a^{qt+r} = a^{qt}\ a^r$. Consequently, $a^r = a^s.a^{-qt} = b.(a^t)^{-q}$. Since H is a subgroup of G, $a^t \in H \Rightarrow (a^t)^{-q} \in H$,

That is, $(a^t)^{-q}, b \in H \Rightarrow (a^t)^{-q} a^s \in H \Rightarrow a^{s-qt} \in H \Rightarrow a^r \in H$ which is a contradiction since $0 \leq r < t$ and a^t is the smallest integer such that $a^t \in H$. There fore the only possibility is $r = 0$.Thus, we have $s = qt \Rightarrow a^s = a^{qt} = (a^t)^q$. So, every element in H is generated by a^t.Thus H is cyclic.

Worked Example. 5.2

Example 5.2.1

Show that $(A,*)$ be an abelian group where $A = \{a \in Q | a \neq -1\}$ and for any $a, b \in A$, $a * b = a + b + ab$

Solution:

1. For any $a, b \in A$, $a * b = a + b + ab \in A$ $\therefore$ Closure property is satisfied
2. For any $a, b, c \in A$, $(a * b) * c = (a + b + ab) * c$

$$= a + b + ab + c + (a + b + ab)c$$
$$= a + b + c + ab + ac + bc + abc$$

$a * (b * c) = a * (b + c + bc) = a + b + bc + c + (b + c + bc)a$
$= a + b + c + ab + ac + bc + abc = (a * b) * c$

Associative property is true

3. For all $a \in A$ there exist $e \in A$ such that $a * e = a$. So $a * e = a + e + ae = a$. Then $e(1 + a) = 0$. Since a is arbitrary and $a \neq -1, 1 + a \neq 0$. Therefore $e = 0$ is the identity element. So, identity element exists.
4. For any $a \in A$ there exist $b \in A$ such that $a * b = 0$. ie. $a + b + ab = 0$. Thus $b = \frac{-a}{1+a}$ is the inverse of a. So inverse exist.
5. $a * b = a + b + ab = b + a + ba = b * a$. So $*$ is commutative.$\therefore$ $(A,*)$ is an abelian group.

Example 5.2.2

Show that Q^+ of all positive rational numbers from an abelian group under the operation $*$ defined by $a * b = \frac{1}{2} ab,\ a, b \in Q^+$.

Solution:

1. For any $a, b \in Q^+$, $a * b = \frac{1}{2} ab \in Q^+$, Closure property is satisfied.
2. For any $a, b, c \in A$, $(a * b) * c = \left(\frac{1}{2} ab\right) * c = \frac{1}{4} (ab)c = \frac{1}{4} a(bc) = a * (b * c)$

   Associative property is true

3. For all $a \in A$ there exist $e \in A$ such that $a * e = \frac{1}{2} ae$. So $a * e = \frac{1}{2} ae = a$.

   So $e = 2 \in Q^+$ is the identity element.

4. For any $a \in A$ there exist $b \in A$ such that $a * b = 2$. ie. $\frac{1}{2} ab = 2$. Thus $b = \frac{4}{a} \in Q^+$ is the inverse element of a. So inverse exist.
5. $a * b = \frac{1}{2} ab = \frac{1}{2} ba = b * a$. So $*$ is commutative. $\therefore$ $(Q^+,*)$ is an abelian group.

Example 5.2.3

Show that $(A,*)$ be a non abelian group where $A = R \times R$ and for any $a, b \in A$,

$(a, b).(c, d) = (ac, bc + d)$

Solution:

1. $(a, b).(c, d) = (ac, bc + d) \in A$ Closure property is satisfied
2. $[(a, b).(c, d)].(e, f) = (ac, bc + d).(e, f) = (ace, (bc + d)e + f)$

   $= (ace, bce + de + f)$

$(a,b).[(c,d).\ (e,f)] = \ (a,b).(ce, de+f) = (ace, bce+de+f)$
$= [(a,b).(c,d)].(e,f).$

Associative property is true

3.For all $(a,b) \in A$ there exist $(e_1,e_2) \in A$ such that $(a,b).(e_1,e_2) = (ae_1, be_1 + e_2)$
$= (a,b)$

So $ae_1 = a,\quad be_1 + e_2 = b.$ ie, $e_1 = 1$ and $e_2 = 0.$

Thus $(1,0))\in A$ is the identity element. So, identity exist in A.

4.For any $(a,b) \in A$ there exist $(c,d) \in A$ such that $(a,b).(c,d) = (1,0)$

$\Rightarrow (ac, bc+d) = (1,0)$. Thus $ac = 1,, bc + d = 0\ \ ie, c = a^{-1} and\ d = -ba^{-1}$

So the inverse of (a,b) is $(a^{-1}, -ba^{-1}) \in A$. Inverse exists.

5. $(a,b).(c,d) = (ac, bc+d) \neq (ca, ad+b) = (c,d).(a,b)$

$\therefore (A,*)$ is a non abelian group.

Example 5.2.4

Let $*$ be a binery operation on N with $m * n = m + n + k$ where k is a constant and $m,n \in N$. Show that $*$ is commutative and associative.

Solution:

For any $m,n \in N$, $m * n = m + n + k = n + m + k = n * m$. Therefore $*$ satisfies commutative property.

For any $m,n,p \in N$,

$$(m * n) * p = (m + n + k) * p = m + n + k + p + k = m + n + 2k + p$$
$$m * (n * p) = m * (n + p + k) = m + n + p + k + k = m + n + 2k + p$$

Therefore $*$ satisfies the associative property.

Example 5.2.5

Show that any group G is abelian if and only if $(ab)^2 = a^2\ b^2$ for all $a,b \in G$.

Solution:

Suppose G is abelian

Now $(ab)^2 = \ (ab)(ab)$

$= a(ba)b$ by associative property

$= a(ab)b$ since G is abelian

$= (aa)\ (bb)$ by associative property

$= a^2\ b^2$

Suppose $(ab)^2 = a^2\ b^2$

$(ab)(ab) = (aa)\ (bb)$

$$a(ba)b = a(ab)b \text{ by associative property}$$
$$(ba)b = (ba)b \text{ by cancellation property}$$
$$(ba) = (ab) \text{ by cancellation property}$$

Therefore, G is abelian.

Example 5.2.6

Prove that commutative property is invariant under homomorphism.

Solution:

Let $f: A \to B$ be a group homomorphism.

Suppose A is abelian

Then for any $a_1, a_2 \in A$ there exist $b_1, b_2 \in B$ such that $f(a_1) = b_1$ and $f(a_2) = b_2$.

Now $b_1 b_2 = f(a_1)\, f(a_2)$

$= f(a_1 a_2)$ since f is a homomorphism

$= f(a_2 a_1)$ since G is abelian

$= f(a_2) f(a_1)$ since f is a homomorphism

$= b_2 b_1$.

$\therefore$ B is commutative.

Example 5.2.7

If G is a group, prove that for all a) $(a^{-1})^{-1} = a$, b) $(ab)^{-1} = b^{-1}a^{-1}$.

Solution:

For any $a \in G$, $aa^{-1} = e$, the identity element in G. Which means the inverse of a^{-1} is a ie, $(a^{-1})^{-1} = a$.

Consider $(ab)\,(b^{-1}a^{-1}) = a(bb^{-1})a^{-1}$ by associative property

$= (ae)a^{-1}$ Inverse exist in G

$= aa^{-1}$ Identity exists in G

$= e$ Inverse exists in G

Therefore, the inverse of ab is $b^{-1}a^{-1}$. So $(ab)^{-1} = b^{-1}a^{-1}$

Example 5.2.8

Prove that if H and K are subgroup of G then $H \cap K$ is a subgroup of G.

Solution:

Since H and K are subgroups of G, $e \in H, e \in K \Rightarrow e \in H \cap K$. The identity element exists.

Let $x, y \in H \cap K \Rightarrow x, y \in H$ and $x, y \in K$

$\Rightarrow xy \in H$ and $xy \in K$ by closure property of H and K.

$\Rightarrow xy \in H \cap K$

Closure property is satisfied.

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

$\Rightarrow a^{-1} \in H \ \ and\ a^{-1} \in K$ since H and K are subgroups

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

Therefore, the inverse element exists in $H \cap K$. $\therefore H \cap K$ is a subgroup of G.

Example 5.2.9

Prove that every cyclic group is abelian.

Solution:

Let $(G,*)$ be a cyclic group with $a \in G$ as generator. Let $x, y \in G$. Then $x = a^m$ and $y = a^n$ where m and n are integers.

Now, $x * y = a^m * a^n = a^{m+n} = a^{n+m} = a^n * a^m = y * x$. $\therefore G$ is abelian.

Example 5.2.10

In the group S_4, let $\propto = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ and $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$

Determine $\propto \beta,\ \ \beta \propto,\ \ \propto^2,\ \ \propto^{-1},\ \ \beta^{-1},\ \ (\propto \beta)^{-1}$

Solution:

$$\propto \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

$$\beta \propto = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

$$\propto^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

$$\propto^{-1} = \begin{pmatrix} 2 & 3 & 4 & 1 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

$$\beta^{-1} = \begin{pmatrix} 4 & 3 & 2 & 1 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

$$(\propto \beta)^{-1} = \begin{pmatrix} 3 & 2 & 1 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

Example 5.2.11

... where the

Solution:

Consider $(S_3,\circ)$ where $X = \{1,2,3\}$ is a group under the operation of composition of permutation.

$S_3 = (f_1, f_2, f_3, f_4, f_5, f_6)$ where $f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

$f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ $f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ $f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ $f_6 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

$f_2 \circ f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = f_6$

$f_3 \circ f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = f_5$

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_3	f_1	f_6	f_4	f_5
f_3	f_3	f_1	f_2	f_5	f_6	f_4
f_4	f_4	f_5	f_6	f_1	f_2	f_3
f_5	f_5	f_6	f_4	f_3	f_1	f_2
f_6	f_6	f_4	f_5	f_2	f_3	f_1

From the table closure property, Associative property are true . For example

$(f_3 \circ f_4) \circ f_5 = f_5 \circ f_5 = f_1 = \; f_3 \circ (f_4 \circ f_5)$

$f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ is the identity element.

Also $f_1^{-1} = f_1$, $f_2^{-1} = f_3$, $f_3^{-1} = f_2$, $f_4^{-1} = f_4$, $f_5^{-1} = f_5$, $f_6^{-1} = f_6$.

Thus the inverse element for each element exist. So $(S_3,\circ)$ is a group.

The symmetric group $(S_3\ \circ)$ is not abelian since $f_2 \circ f_3 = f_1 \neq \; f_3 \circ f_4 = f_5$.

5.3 Cosets

If H is a subgroup of G, then for each $a \in G$ the set $aH = \{ah: h \in H\}$ is called the left coset of H in G. The set $Ha = \{ha: h \in H\}$ is the right cosets of H in G.

If the operation in G is addition then aH is $a + H$. Then the cosets are

$a + H = \{a + h: h \in H\}$ and $H + a = \{h + a: h \in H\}$

Theorem: 5.3.1

If H is a subgroup of a finite group G , then for all $a, b \in G$ a) $|aH| = |H|$

a) Either $aH = bH$ or $aH \cap bH = \varphi$.

Proof:

a) Since $aH = \{ah: h \in H\}$ then $|aH| \leq |H|$. If $|aH| < |H|$ we have $ah_i = ah_j$ where h_i and h_j are distinct elements of H. By left cancellation $h_i = h_j$. So $|aH| = |H|$.

b) If $aH \cap bH \neq \emptyset$. Let $c \in aH \cap bH$ then $c \in aH$ and $c \in bH$.

Let $c = ah_1 = bh_2$, for some $h_1, h_2 \in H$. Then $a = h_1^{-1} b\, h_2$ and $b = h_2^{-1}ah_1$

If $x \in aH$ then $x = ah$ for some $h \in H$. So $x = ah = (bh_2h_1^{-1})h = b(h_2h_1^{-1}h) \in bH$

Then $aH \subseteq bH$

If $y \in bH$ then $y = bh$ for some $h \in H$. So $y = bh = (h_2^{-1}ah_1)h = (ah_2^{-1}h_1)h \in aH$

Then $aH \subseteq bH$. There fore aH and bH are either identical or disjoint.

Theorem 5.3.2

Lagrange's Theorem

Statement

If G is a finite group of order n with H is a subgroup of G of order m, then m divides n.

Proof

If $H = G$ the result follows. If $m < n$ there exist an element $a \in G - H$. Since $a \notin H, aH \neq H$ so that $aH \cap H = \phi$.

If $G = aH \cup H$, $|G| = |aH| + |H|$, $n = m + m = 2m$ Then m divides n and the theorem follows.

$G \neq aH \cup H$ there exist an element $b \in G - \{aH \cup H\}$ with $bH \cap H = \varphi = bH \cap aH$

$|G| = |aH| + |bH| + |H| = m + m + m$. That *is* $n = 3m$. Then m divides n and the theorem follows

Otherwise there exist $c \in G - \{aH \cup bH \cup H\}$

Since the group is finite, this process terminates and $G = a_1H \cup a_2H \cup \dots\dots \cup a_kH$.

So $n = m + m + m + \cdots..k$ times $= km$.Therefore m divides n. Thus, the theorem follows in all cases.

Deductions from Lagrange's Theorem

a) The order of any element of a finite group is a divisor of the order of the group.

Proof

Let G be the finite group and $a \in G$. Let the order of a is m. Then $a^m = e$
Let H be a cyclic subgroup of G generated by a. Then $H = \{a, a^2, a^3, \ldots\ldots a^m = e\}.\therefore$ $O(H) = m$.

By Lagrange's Theorem, $O(H)$ is a divisor of $O(G)$. ie, m is a divisor of $O(G)$

ie, $o(a)$ is a divisor of $O(G)$

b) If G is a finite group of order n, then $a^n = e$ for any $a \in G$.

If m is the order of a, then $a^m = e$. Then m is a divisor of n. ie, $n = km$.

Now, $a^n = a^{km} = (a^m)^k = e^k = e$.

c) Every group of prime order is cyclic.

Let G be a group with $o(G) = p$ where p is prime. Let $a \neq e \in G$. H is a cyclic sub group of G generated by a. By Lagrange's theorem $O(H) \mid p$. So $O(H) = 1$ *or* p since p is prime. If $O(H) = 1$, then $a = e$ which is not possible since $a \neq e$. Hence $o(H) = p$

Therefore $G = H$ and H is cyclic. Hence G is cyclic.