Chapter 2 Basic Group Theory

■ Definitions

■ Group

A set G together with a binary operation $\cdot$ forms a group if

$\forall \quad a, b, c \in G$

1. $a \cdot b \in G$ (closure)
2. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (associativity)
3. $\exists\ e \in G \quad \ni \quad e \cdot a = a \cdot e = a$ (identity)
4. $\exists\ a^{-1} \in G \quad \ni \quad a^{-1} \cdot a = a^{-1} \cdot a = e$ (inverse)

Strictly speaking, a group should be denoted as $\{ G, \cdot \}$. However, the common practice is to call G the group.
The element e is called the **indentity** of G.
a^{-1} is called the **inverse** of a.
It is easy to show that both e & a^{-1} are unique.
The operator $\cdot$ is called the **group multiplication** & is often omitted.

A group G can be specified by enlisting the results of all pair-wise multiplication between its elements. This is often given in the form of a multiplation table of the form

G	e	a	b	…
e	e·e	e·a	e·b	⋯
a	a·e	a·a	a·b	⋯
b	b·e	b·a	b·b	⋯
⋮	⋮	⋮	⋮	⋱

A group thus defined is called an **abstract group** since no specific meaning is as yet given the elements of G.
When the elements of G are given specific meanings or mathematical forms, the result is called a **realization** of G.

■ Comment

1. Take away axiom 4 and we have a monoid.
   Eg. The natual numbers $\mathcal{N}$ (Integers ≥ 0) is an additive monoid.
   $\{ X^r, r \geq 0 \}$ is a monoid.

2. Consider the natual numbers $\mathcal{N}$, and define
   $a \cdot b \equiv a\, Q\, b$
   where the Q operator is defined as
   $a\, Q\, b = n$
   $a = n \times b + r$ ($\times$ is the ordinary multiplication between numbers)
   such that $0 \leq r < b$.

From

$$a = a \times 1 + 0$$

we have

$$a \cdot 1 = a \; Q \; 1 = a \qquad \forall \; a \in \mathcal{N}$$

From

$$1 = 0 \times a + 1$$

we have

$$1 \cdot a = 1 \; Q \; a = 0 \qquad \forall \; a \neq 0$$

This is an example of

$$a \cdot 1 = a \neq 1 \cdot a$$

- **Example C_1**

The simplest group is $G = \{ e \}$.
It is denoted as C_1 with a multiplication table

C_1	e
e	e

- **Example C_2**

$G = \{ e , \; a \}$
Now

$$a \cdot a \in G \quad \longrightarrow \quad \text{either} \quad a \cdot a = e \quad \text{or} \quad a \cdot a = a$$

However, if $a \cdot a = a$, we have

$$a^{-1} \cdot a \cdot a = a^{-1} \cdot a$$

$$e \cdot a = e$$

so that

$$a = e$$

and the group reduces to $G = \{ e \}$.
Therefore, the only choice is $a \cdot a = e$ or $a^{-1} = a$.
This group is denoted as C_2 with a multiplication table

C_2	e	a
e	e	a
a	a	e

One realization of C_2 is to assign a as a reflection about a plane.

- **Example C_3**

There's only one 3 – element group with multiplcation table

C_3	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

One realization of C_3 is to assign a & b as rotations by angles of $\frac{2\pi}{3}$ & $\frac{4\pi}{3}$, repectively.

Another is to set $\{e, a, b\} = \left\{1, e^{i\frac{2\pi}{3}}, e^{i\frac{4\pi}{3}}\right\}$

Yet another is to set e, a, & b as the cyclic permutations of 3 objects by 0, 1, & 2 times, respectively.

- **Example C_n**

A group of the general form

$$G = \left\{e, a, a^2, \ldots, a^{n-1}, a^n = e\right\}$$

is called the cyclic group of order n & is denoted by C_n.
The rows & coloumns of its multiplication table are cyclic permutations of one another; hence the name.
Obviously, a realization of C_n is the cyclic permutations of n objects.

- **Abelian Group**

G is **abelian** if

$$a\,b = b\,a \qquad \forall\ a, b \in G$$

Quite often, the group operation of an abelian group is called addition & denoted by + .
In which case, the identity is denoted by 0, the inverse, by $-a$ so that

$$a + b = b + a$$
$$a + 0 = 0 + a = a$$
$$a + (-a) = a - a = 0$$

C_n is abelian.

- **Order of a Group**

The **order** of a group is the number of its elements.

The order of C_n is n.

- **Example D_2**

The simplest non–cyclic, abelian group is of order 4.
It's usually called the $4-$ group or the **dihedral group** D_2.
Its multiplication table is

D_2	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

A realization of D_2 is the set of symmetry operations that leaves a rectangle invariant. Thus

a, b = reflections about the axes that goes through the center of the rectangle & parallel to the edges.

c = rotation of angle π about an axis that goes through the center & perpendicular to the plane of the rectangle.

■ **Example D_3**

The simplest non–abelian group is of order 6 & is called the dihedral group D_3 or the permutation group S_3 .
Its multiplication table is

S_3	e	(12)	(23)	(31)	(123)	(321)
e	e	(12)	(23)	(31)	(123)	(321)
(12)	(12)	e	(123)	(321)	(23)	(31)
(23)	(23)	(321)	e	(123)	(31)	(12)
(31)	(31)	(123)	(321)	e	(12)	(23)
(123)	(123)	(31)	(12)	(23)	(321)	e
(321)	(321)	(23)	(31)	(12)	e	(123)

where $(l\,m\,\ldots\,n)$ denotes the cyclic permutation $\begin{pmatrix} l & m & \ldots & n \\ m & n & \ldots & l \end{pmatrix}$ which replaces l with m, m with n, & so on, ending with n being replaced by l.

■ **Subgroup**

A proper subset H of G which forms a group under the group operation of G is called a **subgroup** of the group G.

Note that e must be in H. Also,
$a \in H \longrightarrow a^{-1} \in H$.

■ **Example D_2**

There're 3 subgroups of D_2 , namely,
$\{e, a\}$ $\{e, b\}$ $\{e, c\}$

■ **Example S_3**

There're 4 subgroups of S_3 , namely,
$\{e, (12)\}$ $\{e, (23)\}$ $\{e, (13)\}$ $\{e, (123), (321)\}$

■ **Infinite Groups**

A group is called **infinite** if its order is infinite.

An example is the translation group of a lattice.

■ **Continuous Groups**

A group is called **continuous** if its elements are specified by continuous parameters.
A continuous group is necessarily infinite.

An example is the rotation groups $R(n)$ in n-D.

■ Classical Groups

■ **General Linear Group GL(n)**

The set of all invertible $n \times n$ matrices forms a **general linear group** GL(n) under the usual matrix multiplication.

Unitary Group $U(n)$

The set of all unitary $n \times n$ matrices forms a **unitary group** $U(n)$ under the usual matrix multiplication.

Furthermore, if the determinants of each of these matrices are equal to 1, it is called a **special unitary group** SU(n).

- **Orthogonal Group $O(n)$**

The set of all orthogonal $n \times n$ matrices forms an **orthogonal group** $O(n)$ under the usual matrix multiplication.

Furthermore, if the determinants of each of these matrices are equal to 1, it is called a special unitary group SO(n).

The Rearrangement Lemma

If

$p , a , b \in G$

$p\, a = p\, b$

then

$a = b$

Similarly

$a\, p = b\, p \quad \longrightarrow \quad a = b$

- **proof**

$p\, a = p\, b$

$\longrightarrow$

$p^{-1}\, p\, a = p^{-1}\, p\, b$

$e\, a = e\, b$

$a = b$

Proof for the other case is similar.

- **Implications**

The rearrangement lemma implies

$b \neq c \quad \longrightarrow \quad p\, a \neq p\, b \quad \& \quad a\, p \neq b\, p$

Thus, $p\, G$ or $G\, p$ contains the same number of distinct elements as G.

ie., $p\, G$ or $G\, p$ is simply G with the elements arranged in a different order.

This means the rows or columns of the multiplication table are just permutations of each other. Thus, no 2 elements in the same row or column can be the same. These considerations can be used to construct or check on the multiplication tables of groups of small order.

Permutation Groups

- S_n

The $n!$ permutations of n objects form a **symmetric (permutation) group** S_n of degree n & order $n!$.

The group elements are written as

$$p = \begin{pmatrix} 1 & 2 & \dots & n \\ p_1 & p_2 & \dots & p_n \end{pmatrix} \equiv \begin{pmatrix} i \\ p_i \end{pmatrix}$$

Obviously, the order of the elements in the permutation symbol is immaterial, eg.:

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

- **Group Product**

There're 2 inequivalent ways to define the group product.
The active view will be adopted in this note.
In either view, 2 permutations commute if they do not involve permutations of the same index.

- **Active Point of View**

The **active way** used by Tung (see p.18, Tung) interprets a permutation

$$p = \begin{pmatrix} 1 & 2 & \dots & n \\ p_1 & p_2 & \dots & p_n \end{pmatrix} = (\, p_i \leftarrow i \,)$$

as taking the object originally in box i to box p_i.
The product $p\,q$ of 2 permutations p & q then denotes 2 consecutive actions:

1st, take objects in box i to box q_i ,
then, take objects in box i to box p_i.

Thus, an object that is originally in box i is 1st taken to box q_i , then to box p_{q_i} .
Symbolically:

$$\begin{aligned} p\,q &= (\, p_i \leftarrow i \,)(\, q_i \leftarrow i \,) \\ &= \left(\, p_{q_i} \leftarrow q_i \,\right)(\, q_i \leftarrow i \,) \\ &= \left(\, p_{q_i} \leftarrow i \,\right) \end{aligned}$$

or

$$p\,q = \begin{pmatrix} 1 & 2 & \dots & n \\ p_1 & p_2 & \dots & p_n \end{pmatrix} \begin{pmatrix} 1 & 2 & \dots & n \\ q_1 & q_2 & \dots & q_n \end{pmatrix}$$

$$= \begin{pmatrix} q_1 & q_2 & \dots & q_n \\ p_{q_1} & p_{q_2} & \dots & p_{q_n} \end{pmatrix} \begin{pmatrix} 1 & 2 & \dots & n \\ q_1 & q_2 & \dots & q_n \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & \dots & n \\ p_{q_1} & p_{q_2} & \dots & p_{q_n} \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & \dots & n \\ (p\,q)_1 & (p\,q)_2 & \dots & (p\,q)_n \end{pmatrix}$$

where $\begin{pmatrix} q_1 & q_2 & \dots & q_n \\ p_{q_1} & p_{q_2} & \dots & p_{q_n} \end{pmatrix}$ is the rearrangement of the columns of $\begin{pmatrix} 1 & 2 & \dots & n \\ p_1 & p_2 & \dots & p_n \end{pmatrix}$ so that the 1st row ($1 \;\; 2 \;\; \dots \;\; n$) becomes ($q_1 \;\; q_2 \;\; \dots \;\; q_n$).
Thus $(\, p\,q \,)_j = p_{q_j}$.

The inverse p^{-1} of p is:

$$p^{-1} = \begin{pmatrix} 1 & 2 & \dots & n \\ \left(p^{-1}\right)_1 & \left(p^{-1}\right)_2 & \dots & \left(p^{-1}\right)_n \end{pmatrix} = \begin{pmatrix} p_1 & p_2 & \dots & p_n \\ 1 & 2 & \dots & n \end{pmatrix} = (\, i \leftarrow p_i \,) = (\, p_i \rightarrow i \,)$$

so that

$$p\, p^{-1} = (\, p_i \leftarrow i \,)(\, i \leftarrow p_i \,) = (\, p_i \leftarrow p_i \,) = e$$
$$p^{-1}\, p = (\, i \leftarrow p_i \,)(\, p_i \leftarrow i \,) = (\, i \leftarrow i \,) = e$$

$$p\, p^{-1} = \begin{pmatrix} 1 & 2 & \dots & n \\ p_1 & p_2 & \dots & p_n \end{pmatrix} \begin{pmatrix} p_1 & p_2 & \dots & p_n \\ 1 & 2 & \dots & n \end{pmatrix} = \begin{pmatrix} p_1 & p_2 & \dots & p_n \\ p_1 & p_2 & \dots & p_n \end{pmatrix} = e$$

$$p^{-1}\, p = \begin{pmatrix} p_1 & p_2 & \dots & p_n \\ 1 & 2 & \dots & n \end{pmatrix} \begin{pmatrix} 1 & 2 & \dots & n \\ p_1 & p_2 & \dots & p_n \end{pmatrix} = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix} = e$$

as expected.

Obviously, $p_{\left(p^{-1}\right)_j} = \left(\, p\, p^{-1} \,\right)_j = e_j = j = \left(\, p^{-1}\, p \,\right)_j = \left(p^{-1}\right)_{p_j}$

For the sake of convenience, a set of permutations will sometimes be labelled by superscripts, eg., $\left\{\, p^i \,\right\}$. The counterparts of the above formulas are

$$p^i = \begin{pmatrix} 1 & 2 & \cdots & m & \cdots & n \\ p_1^i & p_2^i & \cdots & p_m^i & \cdots & p_n^i \end{pmatrix}$$

$$p^i\, p^j = \begin{pmatrix} 1 & 2 & \cdots & m & \cdots & n \\ p_1^i & p_2^i & \cdots & p_m^i & \cdots & p_n^i \end{pmatrix} \begin{pmatrix} 1 & 2 & \cdots & m & \cdots & n \\ p_1^j & p_2^j & \cdots & p_m^j & \cdots & p_n^j \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & \cdots & m & \cdots & n \\ p^i_{p_1^j} & p^i_{p_2^j} & \cdots & p^i_{p_m^j} & \cdots & p^i_{p_n^j} \end{pmatrix}$$

ie

$$\left(\, p^i\, p^j \,\right)_m = p^i_{p_m^j}$$

■ **Passive Point of View**

The **passive way** used by Inui is (see p.16, Inui) interprets a permutation

$$p = \begin{pmatrix} 1 & 2 & \dots & n \\ p_1 & p_2 & \dots & p_n \end{pmatrix} = (\, i \to p_i)$$

as relabeling object i as p_i .

The product $p\,q$ of 2 permutations p & q then denotes 2 consecutive re-labeling:

1st, relabeling object i as q_i ,

then, relabeling object i as p_i .

Thus, object i is finally labeled q_{p_i} .

Symbolically:

$$\begin{aligned} p\,q &= (\, i \to p_i\,)\,(\, i \to q_i\,) \\ &= (\, i \to p_i\,)\left(\, p_i \to q_{p_i}\right) \\ &= \left(\, i \to q_{p_i}\right) \end{aligned}$$

or

$$p\,q = \begin{pmatrix} 1 & 2 & \dots & n \\ p_1 & p_2 & \dots & p_n \end{pmatrix}\begin{pmatrix} 1 & 2 & \dots & n \\ q_1 & q_2 & \dots & q_n \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & \dots & n \\ p_1 & p_2 & \dots & p_n \end{pmatrix}\begin{pmatrix} p_1 & p_2 & \dots & p_n \\ q_{p_1} & q_{p_2} & \dots & q_{p_n} \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & \dots & n \\ q_{p_1} & q_{p_2} & \dots & q_{p_n} \end{pmatrix}$$

where $\begin{pmatrix} p_1 & p_2 & \dots & p_n \\ q_{p_1} & q_{p_2} & \dots & q_{p_n} \end{pmatrix}$ is the rearrangement of the columns of $\begin{pmatrix} 1 & 2 & \dots & n \\ q_1 & q_2 & \dots & q_n \end{pmatrix}$ so that the 1st row ($1 \;\; 2 \;\; \dots \;\; n$) becomes ($p_1 \;\; p_2 \;\; \dots \;\; p_n$).

Thus $(\, p\,q\,)_j = q_{p_j}$.

This means products in the passive view correspond to products in inverse order in the active view, & vice versa. ie.

passive $p\,q \dots r\,s \quad \Longleftrightarrow \quad$ active $s\,r \dots q\,p$

Since we shall adopt the active point of view in the rest of this note, further development of the passive way will be left as exercise for those interested.

■ **Example**

Let

$$p = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \qquad\qquad q = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

The active view gives

$$p\,q = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 2 & 1 \\ 3 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$q\,p = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 2 & 1 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

The passive view gives

$$p\,q = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 2 & 1 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$q\,p = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}\begin{pmatrix} 3 & 2 & 1 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

- **Example S_3**

Permutations of 3 objects form the group S_3.
There are $3! = 6$ group elements:

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad b = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$c = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \qquad d = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \qquad f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

- **S_3 & C_{3v}**

Consider the group C_{3v}, which is isomorphic to S_3.

To facilitate the correspondence between elements of the 2 groups, we identify the objects under permutation to be the vertices of the triangle & the boxes to be positions in space.
Both vertices & positions are labeled 1, 2, 3 in a counterclockwise sense.
Originally, vertex labelled i is at postion (box) i.

In the **active point of view**, the permutation $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (123)$ moves the vertex 1 at position 1 to position 2, vertex 2 at position 2 to position 3, and vertex 3 at position 3 to position 1. The result is that vertices 1, 2, 3 are now at positions 2, 3, 1, respectively. Clearly, this corresponds to the C_3 rotation of the triangle if the boxes or positions are fixed in space.

In the **passive point of view**, the permutation $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (123)$ relabels the vertex 1 as vertex 2, vertex 2 as vertex 3, and vertex 3 as vertex 1. The result is that vertices 1, 2, 3 are now at positions 3, 1, 2, respectively. Clearly, this corresponds to the C_3^2 rotation of the triangle if the positions are fixed in space. Alternatively, we can also say that the boxes are rotated by C_3 while the triangle is held fixed.

Similarly, the elements of $S_3 = \{e,\ a,\ b,\ c,\ d,\ f\}$ can be identified with those of $C_{3v} = \{E,\ C_3,\ C_3^2,\ \sigma_1,\ \sigma_2,\ \sigma_3\}$, respectively, if we adopt the convention that in the active (passive) point of view, operations of C_{3v} represent rotations of the triangle (positions).
Obviously, it is also correct to identify $S_3 = \{e,\ a,\ b,\ c,\ d,\ f\}$ with $C_{3v} = \{E,\ C_3^2,\ C_3,\ \sigma_1,\ \sigma_2,\ \sigma_3\}$, respectively, if we adopt the convention that in the active (passive) point of view, operations of C_{3v} represent rotations of the positions (triangle).

This freedom of interpretation may create confusion to novices & is a major source of computational error, especially when results from different authors are quoted.
We shall henceforth adopt the active point of view for all groups, which means elements of the point groups are treated as actions on the geometric figure.
The active point of view is usually preferred by physicists while the passive one, by mathematicians.

The group multiplication table for S_3 can be obtained from that of C_{3v} (p.12, Inui) :

S_3	e	$a = C_3$	$b = C_3^2$	$c = \sigma_1$	$d = \sigma_2$	$f = \sigma_3$
e	e	a	b	c	d	f
a	a	b	e	f	c	d
b	b	e	a	d	f	c
c	c	d	f	e	a	b
d	d	f	c	b	e	a
f	f	c	d	a	b	e

This table is the same as that in p.15, Tung but the roles of a & b are interchanged in p.17, Inui.
Both authors adopt the active view on rotation operators but Tung used the active, Inui the passive view for permutations.

- **Cycles**

An $n-$ cycle $(i_1\, i_2 \ldots i_n)$ is defined by

$$(i_1\, i_2 \ldots i_n) = \begin{pmatrix} i_1 & i_2 & \ldots & i_n \\ i_2 & i_3 & \ldots & i_1 \end{pmatrix}$$

- **Examples**

1 – cycle:

$$(i) = \begin{pmatrix} i \\ i \end{pmatrix}$$

2 – cycle, also called a transposition:

$$(i,\, j) = \begin{pmatrix} i & j \\ j & i \end{pmatrix}$$

3 – cycle :

$$(i\, j\, k) = \begin{pmatrix} i & j & k \\ j & k & i \end{pmatrix}$$

The generator of a cyclic group C_n is the $n-$ cycle.

Any permutation can be written as a product of cycles with no common indices, eg.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 3 & 7 & 1 & 5 & 8 & 2 & 6 \end{pmatrix} = (14)\,(237)\,(5)\,(68)$$

- **Example S_3**

In cycle notations, elements of S_3 becomes:

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = (1)\,(2)\,(3) = ea = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (123)\, b = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (132)$$

$$c = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (1)\,(23) = (23) \qquad d = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (13) \qquad f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (12)$$

For convenience, the multiplication table is reproduced in cycle notations (cf p.15, Tung):

S_3	e	(123)	(132)	(23)	(13)	(12)
e	e	(123)	(132)	(23)	(13)	(12)
(123)	(123)	(132)	e	(12)	(23)	(13)
(132)	(132)	e	(123)	(13)	(12)	(23)
(23)	(23)	(13)	(12)	e	(123)	(132)
(13)	(13)	(12)	(23)	(132)	e	(123)
(12)	(12)	(23)	(13)	(123)	(132)	e

For comparison purposes, the following table may be more useful:

S_3 C_{3v}	e	a = (123) = C_3	b = (132) = C_3^2	c = (23) = σ_1	d = (13) = σ_2	f = (12) = σ_3
e	e	a = (123) = C_3	b = (132) = C_3^2	c = (23) = σ_1	d = (13) = σ_2	f = (12) = σ_3
a = (123) = C_3	a = (123) = C_3	b = (132) = C_3^2	e	f = (12) = σ_3	c = (23) = σ_1	d = (13) = σ_2
b = (132) = C_3^2	b = (132) = C_3^2	e	a = (123) = C_3	d = (13) = σ_2	f = (12) = σ_3	c = (23) = σ_1
c = (23) = σ_1	c = (23) = σ_1	d = (13) = σ_2	f = (12) = σ_3	e	a = (123) = C_3	b = (132) = C_3^2
d = (13) = σ_2	d = (13) = σ_2	f = (12) = σ_3	c = (23) = σ_1	b = (132) = C_3^2	e	a = (123) = C_3
f = (12) = σ_3	f = (12) = σ_3	c = (23) = σ_1	d = (13) = σ_2	a = (123) = C_3	b = (132) = C_3^2	e

■ Isomorphism

■ Definition (Isomorphism)

2 groups G & G' are **isomorphic**, ie., $G \simeq G'$, if

$\exists$ a 1–1 onto mapping

$f: \quad G \longrightarrow G'$

$\quad g_i \mapsto g_i'$

$\ni \quad g_i \cdot g_j = g_k \quad \longleftrightarrow \quad g_i' \cdot g_j' = g_k'$

■ Cayley's Theorem

Every group of finite order n is isomorphic to a subgroup of S_n.

■ **Proof:**

Consider the multiplication table

	g^1	…	g^j	…	g^n
g^1	$g^1 g^1$	…	$g^1 g^j$	…	$g^1 g^n$
⋮	⋮	⋱	⋮	⋱	⋱
g^i	$g^i g^1$	…	$g^i g^j$	…	$g^i g^n$
⋮	⋮	⋱	⋮	⋱	⋱
g^n	$g^n g^1$	…	$g^n g^j$	…	$g^n g^n$

In particular, the *i*th row is simply a rearrangement of

$$\{ g^1, \ldots, g^m, \ldots, g^n \}$$

into

$$\{ g^i g^1, \ldots, g^i g^m, \ldots, g^i g^n \}$$
$$= \{ g^i, \ldots, g^k, \ldots, g^l \} \qquad \text{where } g^1 = e,\ g^i g^m = g^k$$

This is simply a permutation of the indices:

$$p^i = \begin{pmatrix} 1 & \ldots & m & \ldots & n \\ p^i_1 & \ldots & p^i_m & \ldots & p^i_n \end{pmatrix}$$
$$= \begin{pmatrix} 1 & \ldots & m & \ldots \\ i & \ldots & k & \ldots \end{pmatrix}$$

ie

$$p^i_m = k \qquad \text{where } g^i g^m = g^k$$

It is easy to show that the mapping

$$g^i \rightarrow p^i$$

is a rep of G.

Thus

$$g^i g^m = g^k$$

should be mapped into

$$p^i p^m = p^k$$

By definition,

$$\left(p^i p^m\right)_l = p^i_{p^m_l}$$
$$= p^i_j \qquad \text{provided } g^m g^l = g^j$$
$$= h \qquad \text{provided } g^i g^j = g^h$$
$$p^k_l = h' \qquad \text{provided } g^k g^l = g^{h'}$$

We therefore need to show $h = h'$.

This is done by manipulating the 4 equations relating the g's,

$$g^h = g^i g^j = g^k (g^m)^{-1} g^m g^l = g^k g^l = g^{h'} \qquad \text{QED [} p^i \text{ is a rep of } G \text{].}$$

Now, p^i are permutations of n objects.

Since they form a rep of G, they form a group.

Therefore, $\{ p^i \}$ is a subgroup of S_n.

■ **Corollary**

If the order of a group is prime, it must be isomorphic to C_n.

Classes & Invariant Subgroups

- **Definition (Conjugate Elements)**

Let $a, b \in G$.
b is **conjugate** to a, or $a \sim b$, if
$\exists\ p \in G \quad \ni \quad b = p\, a\, p^{-1}$

- **Equivalence Relation**

Now
$a = e\, a\, e^{-1}$
so that
$a \sim a$ (**reflexive**)

Since
$b = p\, a\, p^{-1} \longrightarrow a = p^{-1}\, b\, p = q\, b\, q^{-1}$ where $q = p^{-1}$
we see that
$a \sim b \longrightarrow b \sim a$ (**symmetric**)

Let
$a \sim b \quad b \sim c$
then
$\exists\ p, q \in G$
$\ni \quad b = p\, a\, p^{-1} \quad c = q\, b\, q^{-1}$
Thus
$c = q\, p\, a\, p^{-1}\, q^{-1}$
$= \ r\, a\, r^{-1}$ where $r = q\, p \in G$
$\longrightarrow$
$a \sim c$ (**transitive**)

Therefore, the conjugation is an **equivalent relation**.

- **Definition (Conjugate Class)**

Since conjugation is an equivalent relation, it can be used to separate the elements of a group into mutually exclusive equivalent classes called the **conjugate classes**, or more simply, **classes**.

Specifically, let $a \in G$.
The class of a is the set $\{ g \mid g = p\, a\, p^{-1} \ \forall \ p \in G \}$.

Since
$e = p\, e\, p^{-1} \quad \forall \ p \in G$
the identity e of any group is a class by itself.

For an abelian group,
$p\, a\, p^{-1} = p\, p^{-1}\, a = a \quad \forall \ p \in G$
Thus, each element of an abelian group is a class by itself.

Conjugate Subgroup

Let H be a subgroup of G.
For a given $p \in G$.
The set

$$H' = \{ h' \mid h' = p\, h\, p^{-1} \ \forall \ h \in H \}$$

is also a subgroup of G. It is called a **conjugate subgroup** to H.

Proof

The **associativity** of H' follows immediately from that of H.

Its **closure** is as follows:

$$\forall \ h_i \in H$$
$$h_i' \, h_j' = p\, h_i\, p^{-1}\, p\, h_j\, p^{-1} = p\, h_i\, h_j\, p^{-1} \in H' \qquad \text{since} \quad h_i\, h_j \in H$$

Its **identity** is simply

$$e' = p\, e\, p^{-1} = e \in H'$$

since

$$e'\, h_i' = p\, e\, p^{-1}\, p\, h_i\, p^{-1} = p\, e\, h_i\, p^{-1} = p\, h_i\, p^{-1} = h_i'$$

The **inverse** of h_i' is

$$h_i'^{-1} = p\, h_i^{-1}\, p^{-1}$$

since

$$h_i'^{-1}\, h_i' = p\, h_i^{-1}\, p^{-1}\, p\, h_i\, p^{-1} = p\, e\, p^{-1} = e'$$

Invariant Subgroup

An **invariant subgroup** is a subgroup that is identical to all its conjugate subgroups.

Simple & Semi–Simple Groups

A group is **simple** if it has no non–trivial invariant subgroup.
(Trivial subgroups are the identity group & the group itself.)
A group is **semi– simple** if it has no abelian invariant subgroup.

Cosets & Factor (Quotient) Groups

Definition (Cosets)

Let

H be a subgroup of G.
$p \in G$

then

$p\, H = \{ p\, h \ \ \forall \ h \in H \}$ is a **left coset** of H
$H\, p = \{ h\, p \ \ \forall \ h \in H \}$ is a **right coset** of H

All subsequent discussions will be based on the left cosets with the understanding that they're applicable to the right cosets with suitable modifications.

1st of all

$p H = H$ if $p \in H$

Also

For $p \notin H$, $p H$ is not a group since $e \notin p H$

■ **Lemma**

2 cosets of a subgroup are either identical or completely distinct.

■ **Proof**

Let $p H$ & $q H$ be 2 left cosets of H.

If they have a common element, say,

$p h_i = q h_j$

then

$h_i h_j^{-1} = p^{-1} q \in H$

Thus

$p^{-1} q H = H$

or

$q H = p H$

■ **Lagrange Theorem**

The order of a finite group must be an integral multiple of the order of everyone of its subgroups.

■ **Proof**

This is simply the consequence of the previous lemma, which implies that the left cosets partition the group into disjoint sets each of the order of the subgroup.

■ **Theorem (Factor Group)**

Let H be an invariant subgroup of G.

The set of cosets $G/H = \{ p H \ \forall \ p \in G \}$ is a group under the multiplication

$p H \cdot q H = (p q) H \qquad \forall \ p, q \in G$

It is called the **factor (quotient) group** of G with respect to H.

Its order is $n_{G/H} = n_G / n_H$.

■ **Proof**

Closure & associativity follow directly from those of H, G & the partition of G into distinct closets.

Identity is H since $\forall \ p, q \in H$

$p H \cdot q H = H \cdot H = H$

$(p q) H = H$ since $p q \in H$

Inverse of $p H$ is $p^{-1} H$ since

$p H \cdot p^{-1} H = \left(p \, p^{-1} \right) H = H \qquad (e \in H)$

■ Homomorphism

■ Definition (Homomorphism)

G is **homomorphic** to G' if

$$\exists\ f:\ G \longrightarrow G'$$

$$\ni\quad g_i \cdot g_j = g_k \quad\mapsto\quad f(g_i)\circ f\left(g_j\right) = g_i'\circ g_j' = g_k' = f(g_k)$$

Note that isomorphism is a special case of homomorphism when the mapping is 1–1 onto.

Furthermore

$$e\cdot g = g \qquad \forall\ g \quad\longrightarrow\quad f(e)\circ f(g) = f(g)$$

implies

$$f(e) = e'$$

■ Theorem

Let G be homomorphic to G' under the mapping

$$f:\quad G \longrightarrow G'$$

& $K = \{\, g \in G \mid f(a) = e' \,\}$

then

K is an invariant subgroup of G.

$G/K \simeq G'$ (isomorphic)

■ Proof

Since f is a homomorphism, $f(e) = e'$ so that $e \in K$. (identity)

Let $p, q, r \in K$

then

$$f(p) = f(q) = e'$$

$$f(pq) = f(p)\circ f(q) = e'\circ e' = e' \longrightarrow pq \in K \quad \text{(closure)}$$

$$f\left(p\,p^{-1}\right) = f(e) = e' \longrightarrow p^{-1} \in K \quad \text{(inverse)}$$

Associativity is inherited from G.

Thus, K is a subgroup of G.

Let $g \in G$ but $g \notin K$

$$f\left(g\,p\,g^{-1}\right) = f(g)\circ f(p)\circ f\left(g^{-1}\right)$$

$$= \text{f(g)}\circ \text{e '}\circ \text{f}\left(\text{g}^{-1}\right)$$

$$= \text{f(g)}\circ \text{f}\left(\text{g}^{-1}\right)$$

$$= \text{f}\left(\text{ g g}^{-1}\right)$$

$$= \text{f(e)}$$

$$= \text{e'}$$

$\longrightarrow\quad g\,p\,g^{-1} \in K$

Hence, K is an invariant subgroup of G.

Let G be partitioned as

$$G = \sum_{j=0}^{m} p_j K$$

with $p_0 \in K$.

We have

$$G/K = \{ K,\ p_1 K,\ \ldots,\ p_m K \}$$

Cosider the mapping

$$h: \quad G/K \longrightarrow G'$$
$$p_j K \mapsto h(p_j K) \equiv f(p_j) = p_j'$$

If $p_j' = p_k'$

then $f(p_j) = f(p_k)$

& $h(p_j K) = h(p_k K)$

Therefore

$$h(p_k^{-1} p_j K) = h(K) = f(e) = e'$$

Thus

$$p_k^{-1} p_j \in K$$

ie

$$p_j \in p_k K$$

&

$$p_j K = p_k K$$

Thus h is 1–1.

Since f is by definition onto, so is h, & we have $G/K \simeq G'$.

■ Direct Product

■ Definition (Direct Product Group)

Let H_1 & H_2 be subgroups of G.

$[h_1, h_2] = 0 \qquad \forall\ h_1 \in H_1,\ h_2 \in H_2$

$\forall\ g \in G, \qquad \exists\ h_1 \in H_1 \ \& \ h_2 \in H_2 \qquad \ni \qquad g = h_1 h_2 = h_2 h_1$

then

G is said to be a **direct product** of H_1 & H_2 and we write

$G = H_1 \otimes H_2$

■ Properties

Let $G = H_1 \otimes H_2$

then

H_1 & H_2 must be invariant subgroups of G.

$H_1 = G/H_2$

$H_2 = G/H_1$