GROUP THEORY

AN INTRODUCTION TO FINITE GROUPS & THEIR REPRESENTATIONS

Shreya Shrivastava
200260051
Undergraduate, Department of Physics
Indian Institute of Technology, Bombay
Mentor: Nehal Mittal

ABSTRACT

In this report we start with some basic definitions and theorems as an introduction to Group theory, following which we construct the finite groups of orders up to 13 and look into their possible representations. We conclude with a brief discussion on Representation theory, which serves as a more formal approach to studying group representations, and with special emphasis to finite groups. We will be following the texts *Group Theory and Its Applications in Physics*[1] and*Group Theory: A Physicist's Survey*[2] in this report.

CONTENTS

1 Groups

A group $\mathscr{G}$ is a set of distinct operators,

$$\mathscr{G} : \{G_1, G_2, \ldots, G_k, \ldots\}$$

such that for any 2 operators (also known as group elements) G_i, G_j an operation ($\circ$) called the group multiplication is defined, that satisfies the group axioms. We say that $\mathscr{G}$ is a group under $\circ$ if $(\mathscr{G}, \circ)$ is a group.

1.1 Group axioms

- **Closure** For any 2 operators G_i, G_j of the group $\mathscr{G}$ their unique product also belongs to $\mathscr{G}$.
$$G_i \circ G_j = G_k$$
- **Associativity** For any G_i, G_j, G_k belonging to $\mathscr{G}$,
$$G_i \circ (G_j \circ G_k) = (G_i \circ G_j) \circ G_k$$
- **Existence of Identity Element** There exists an element G in $\mathscr{G}$ such that,
$$G \circ G_i = G_i \circ G = G_i$$
for any $G_i \in \mathscr{G}$. This element G is called the *identity element* or *unit element* and will be represented as E[1] henceforth. Also from the above definition of E we can say that
$$E \circ E = E$$
Theorem 1. *Any group $\mathscr{G}$ has a unique identity element.*

Proof. Let E_1 and E_2 be two identities of $\mathscr{G}$. We have $E_1 \circ E_2 = E_1$ and $E_2 \circ E_1 = E_2$. Therefore
$$E_1 = E_1 \circ E_2 = E_2 \circ E_1 = E_2$$
□

[1] or as e

- **Existence of Inverse** For every element $G \in \mathscr{G}$ there exists an element G' also belonging to $\mathscr{G}$ such that,

  $$G \circ G' = G' \circ G = E$$

  We call G' as the *inverse* of G.

  Theorem 2. *Any element G in $\mathscr{G}$ has a unique inverse G'.*

  Proof. Let G'_1 and G'_2 be two inverses of G. We have $G \circ G'_1 = E$ and $G \circ G'_2 = E$ and so

  $$G'_2 \circ (G \circ G'_1) = G'_2 \implies (G'_2 \circ G) \circ G'_1 = G'_1 = G'_2$$

  □

Note that the group axioms do not require the commutative law to hold true. However there do exist some special groups that are commutative. Such groups are known as *Abelian groups* and satisfy the following property,

$$G_i \circ G_j = G_j \circ G_i$$

where $G_i, G_j \in \mathscr{G}$ and $\mathscr{G}$ is an *Abelian group.*

Groups having an infinite number of elements are known as *infinite groups* and those having a finite number of elements are known as *finite groups.* For a finite group having a total of n elements, the *order* of the group is n.

1.2 Basic Concepts

1.2.1 Subgroups

A subset $\mathscr{H}$ of the group $\mathscr{G}$ is called a *subgroup* of $\mathscr{G}$ if it satisfies the four group axioms. Observe that for $\mathscr{H}$ to be a subgroup we require only the following conditions to hold

1. For any two $H_i, H_j \in \mathscr{H}$ we have $H_i H_j \in \mathscr{H}$.
2. For every $H \in \mathscr{H}$ there exists a corresponding $H^{-1} \in \mathscr{H}$.

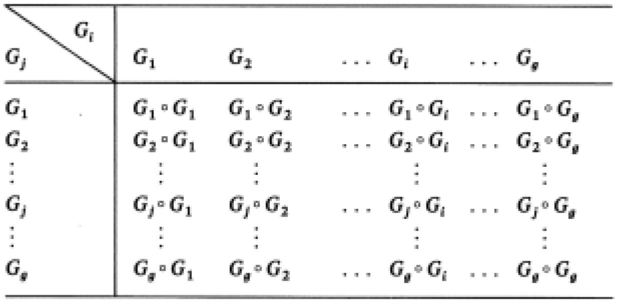
Did we reduce the four group axioms into the above two? NO! Recall that $\mathscr{H}$ is a subset of $\mathscr{G}$ and so by default associativity holds in $\mathscr{H}$. Also from conditions (1) & (2) existence of the identity element is guaranteed since $HH^{-1} = E$. The set $\{E\}$ and the group $\mathscr{G}$ itself are trivial subgroups of $\mathscr{G}$. Any other subgoups of $\mathscr{G}$ are known as *proper subgroups.*

1.2.2 Generating elements

If every element of a group $\mathscr{G}$ can be expressed as the product of a smaller subset of distinct elements, we call this set of elements as generating elements or generators. For cyclic groups there exists exactly one unique generator. Also note that the choice of generators can vary.

1.2.3 Multiplication Tables

The structure of a group can be visualized using a multiplication table. We construct this table by placing the group elements $G_1, G_2, \ldots, G_n$ in the top row and in the leftmost column, as shown in Figure 1. We then place the product $G_i \circ G_j$[2] at the intersection of the i^{th} row and j^{th} column.



G_i G_j	G_1	G_2	...	G_i	...	G_g
G_1	$G_1 \circ G_1$	$G_1 \circ G_2$	...	$G_1 \circ G_i$	...	$G_1 \circ G_g$
G_2	$G_2 \circ G_1$	$G_2 \circ G_2$	...	$G_2 \circ G_i$	...	$G_2 \circ G_g$
$\vdots$	$\vdots$	$\vdots$		$\vdots$		$\vdots$
G_j	$G_j \circ G_1$	$G_j \circ G_2$	...	$G_j \circ G_i$	...	$G_j \circ G_g$
$\vdots$	$\vdots$	$\vdots$				$\vdots$
G_g	$G_g \circ G_1$	$G_g \circ G_2$	...	$G_g \circ G_i$	...	$G_g \circ G_g$

Figure 1: Construction of a multiplication table

1.2.4 Rearrangement Theorem

Theorem 3. *Consider a group* $\mathscr{G} : \{G_1, G_2, \ldots, G_n\}$ *of order n. On multiplying* $\mathscr{G}$ *with an arbitrary element* $G \in \mathscr{G}$ *we obtain the set*

$$\mathscr{G}G = \{G_1G, G_2G, ..., G_nG\}$$

where each element appears only once and belongs to the group $\mathscr{G}$*.*

Proof. Take any element $G_i \in \mathscr{G}$, which on post multiplication with G gives G_iG that belongs to $\mathscr{G}$ as per the closure property.
Now lets consider some $G_iG, G_jG \in \mathscr{G}G$ such that

$$G_iG = G_jG$$

[2] Henceforth we shall represent the group multiplication as G_iG_j instead of $G_i \circ G_j$.

It is trivial that $G_i = G_j$ for the above to hold. However this is a contradiction as every element in a group occurs only once. Therefore every element in the set $\mathscr{G}G$ is unique. □

Observe that as a consequence of this theorem every group element appears only once in any row or column of the group multiplication table.

Aliter Let f be any function that takes group elements G_i as an argument. Then for an arbitrary element $G \in \mathscr{G}$

$$\sum_{i=1}^{g} f(GG_i) = \sum_{i=1}^{g} f(G_iG) = \sum_{i=1}^{g} f(G_i)$$

1.2.5 Direct Product

Consider two groups $\mathscr{A}$ and $\mathscr{B}$ with elements $\{a_i\}$, $i = 1,\ldots,n_a$ and $\{b_j\}$, $j = 1,\ldots,n_b$ respectively. We now define

$$\mathscr{A} \times \mathscr{B} = \{A_iB_j | \, i = 1,\ldots,n_a \,\text{and}\, j = 1,\ldots,n_b\}$$

where we follow the multiplication rule

$$(a_i, b_j)(a_k, b_l) = (a_ia_k, b_jb_l)$$

Clearly the above rule satisfies the group axioms. Therefore we have a group of order n_an_b called the *direct (Kronecker) product group* $\mathscr{A} \times \mathscr{B}$. Note that the groups $\mathscr{A}$ and $\mathscr{B}$ operate in separate spaces and so we have concluded the order of $\mathscr{A} \times \mathscr{B}$ as n_an_b. Also, since they operate in separate spaces we can safely say that the groups $\mathscr{A}$ and $\mathscr{B}$ commute i.e.

$$a_ib_j = b_ja_i$$

This construction will prove to be particularly useful in generating groups of higher order.

1.2.6 Cosets and Coset decomposition

Let's consider a group $\mathscr{G}$ of order n and one of its subgroups $\mathscr{H}$ of order h. Now we pick any element $G_i \in \mathscr{G}$ and premultiply it with the subgroup $\mathscr{H}$. We obtain

$$\mathscr{H}G_i = \{H_jG_i | j = 1,\ldots,h\}$$

This is called as a *right coset*[3]. Observe that the elements of any coset belong to the group $\mathscr{G}$ by the closure property, and every element in a coset is unique (recall the rearrangement theorem [3]). Thus the order of a coset is same as that of the subgroup considered.

Theorem 4. *Take any coset $\mathscr{H} G_1$ and pick another element say G_2 from $\mathscr{G}$ which doesn't belong to the coset $\mathscr{H} G_1$. We then have*

$$\mathscr{H} G_1 \cap \mathscr{H} G_2 = \emptyset$$

Proof. Let's assume $H_i G_1 = H_j G_2$ for some $i, j = 1, \ldots, h$. Then

$$G_2 = H_j^{-1} H_i G_1$$

but $H_j^{-1} H_i$ belongs to $\mathscr{H}$ and so G_2 is of the form HG_1. This implies that $G_2 \in \mathscr{H} G_1$ and contradicts our assumption that G_2 doesn't occur in $\mathscr{H} G_1$. Therefore the two cosets are disjoint. □

We shall now use this result to decompose the group $\mathscr{G}$ into some l disjoint cosets. We start by taking the subgroup[4] $\mathscr{H}$ itself, and pick an element G_2 from $\mathscr{G}$ which doesn't belong to $\mathscr{H}$, and make a right coset $\mathscr{H} G_2$. Now pick another element G_3 from $\mathscr{G}$ which isn't present in the cosets created so far i.e. $\mathscr{H}$, $\mathscr{H} G_1$ to make the next coset $\mathscr{H} G_3$. We follow this procedure recursively until we have exhausted all the group elements and we obtain the (right) decomposition of $\mathscr{G}$ as follows

$$\mathscr{G} = \mathscr{H} G_1 + \mathscr{H} G_2 + \cdots + \mathscr{H} G_l$$

The elements G_i are called *coset representatives.* Note that as per this decomposition the order of $\mathscr{G}$, $n = hl$ i.e. the order of the subgroup $\mathscr{H}$ is a factor of n. This is a powerful result which shall save us a good deal of work while constructing *finite groups.*

Theorem 5 (Lagrange's Theorem)**.** *If a group $\mathscr{G}$ of order n has a subgroup $\mathscr{H}$ of order h, then n is necessarily an integer multiple of h.*

The ratio $l = n/h$ is called the *index* of $\mathscr{H}$ in $\mathscr{G}$.

[3] Similarly we can define left and double cosets as $G_i\mathscr{H}$ and $G_i\mathscr{H}G_j$ respectively.

[4] $\mathscr{H}$ is also a coset of the from $\mathscr{H} G_1$, where $G_1 \equiv E$

1.2.7 Isomorphism

If there exists a one-to-one correspondence between the elements G of a group $\mathscr{G}$ and G' of a group $\mathscr{G}'$ i.e. for the multiplication $G_i G_j = G_k$ in $\mathscr{G}$ there is a corresponding multiplication $G'_i G'_j = G'_k$ in $\mathscr{G}'$, then $\mathscr{G}$ and $\mathscr{G}'$ are said to be *isomorphic*, and the same is represented as

$$\mathscr{G} \cong \mathscr{G}'$$

Mathematically, isomorphic groups have the same *structure* (recall the group multiplication table) and are hence termed as *identical* (not equivalent!).

1.2.8 Homomorphism

Simply put, homomorphism is similar to isomorphism except here we have an n-to-one mapping between the groups $\mathscr{G}$ and $\mathscr{G}'$ (i.e. a generalization of isomorphism). Let's consider the onto mapping $f : \mathscr{G} \to \mathscr{G}'$ and so $f(G) = G'$ [5]. If the relation

$$f(G_i G_j) = f(G_i) f(G_j)$$

holds where $G_i, G_j \in \mathscr{G}$, we call f as a *homomorphic mapping.* Two groups related by such a mapping are said to be *homomorphic* and we represent this relation as follows

$$G \sim G'$$

Some results

- $f(E_g) = E_{g'}$, where E_g and $E_{g'}$ are the identity elements of $\mathscr{G}$ and $\mathscr{G}'$ respectively.
- $f(G^{-1}) = (f(G))^{-1}$
  Explanation. $f(G^{-1}G) = f(G^{-1})f(G) \Leftrightarrow f(G^{-1}) = (f(G))^{-1}$

1.2.9 The Kernel

Consider a homomorphic mapping f that maps a group $\mathscr{G}$ onto a group $\mathscr{G}'$. The set $\mathscr{K}$ of elements that are mapped onto the *unit element* E' of $\mathscr{G}'$, is called the *kernel* of the mapping f.

$$\mathscr{K} = \{G \mid G \in \mathscr{G},\, f(G) = E'\}$$

[5] The element G' of $\mathscr{G}'$ is said to be the image of some G of $\mathscr{G}$, and G the inverse image of G'. If for every G' there exists an inverse image in $\mathscr{G}$ then f is an *onto* mapping.

1.2.10 Conjugation

Elements A and B of a group $\mathscr{G}$ are *conjugate* with respect to $\mathscr{G}$ if

$$B = GAG^{-1} \Leftrightarrow A = G^{-1}BG$$

where $G \in \mathscr{G}$. We now adopt a change of notation, where the conjugate of g_a is

$$\tilde{g}_a = gg_ag^{-1} \qquad g \in \mathscr{G}$$

Consider the elements $g_a, g_b \in \mathscr{G}$,

$$g_ag_b = g_c$$

Now taking the conjugates of g_a, g_b,

$$\tilde{g}_a\tilde{g}_b = (gg_ag^{-1})(gg_bg^{-1}) = gg_cg^{-1} = \tilde{g}_c$$

And so we conclude that the transformation maps the multiplication table into itself. Hence this mapping leaves the multiplication table invariant, and is a special example of *homomorphism* known as *automorphism.* This is because the mapping is *inner* as every element is generated by another element of the same group.

Suppose the elements g_a, g_b commute then,

$$\tilde{g}_a = g_bg_ag_b^{-1} = g_bg_b^{-1}g_a = g_a$$

Since $\tilde{g}_a = g_a$, we say that g_a is *self conjugate.*

1.2.11 Classes

A class C is defined as the set of conjugate elements of some group $\mathscr{G}$,

$$C : \tilde{g} = g_agg_a^{-1}, \forall g_a \in \mathscr{G}$$

The conjugate class[6] of a group element g is also denoted as $[g]$.

[6] The terms *conjugate class* and *class* are used interchangeably.

Theorem 6. *Consider the class*

$$[g_b] : \tilde{g}_b = g_a g_b g_a^{-1}, \forall g_a \in \mathscr{G}$$

Now we pick an element say g_c from $\mathscr{G}$ which doesn't occur in the class $[g_b]$, and construct the class,

$$[g_c] : \tilde{g}_c = g_a g_c g_a^{-1}, \forall g_a \in \mathscr{G}$$

We then have

$$[g_b] \cap [g_c] = \emptyset$$

Proof. Let's assume that $[g_b] \cap [g_c] \neq \emptyset$ i.e. there exists some group element $g \in [g_b] \cap [g_c]$. Now by the definition of conjugation we have,

$$g_c = g_1 g g_1^{-1} \; g_1 \in \mathscr{G} \tag{1}$$

and

$$g = g_2 g_b g_2^{-1} \; g_2 \in \mathscr{G} \tag{2}$$

From 1 & 2 we have

$$g_c = g_1(g_2 g_b g_2^{-1}) g_1^{-1} = (g_1 g_2) g_b (g_2^{-1} g_1^{-1}) = (g_1 g_2) g_b (g_1 g_2)^{-1}$$

This implies that g_c belongs to the class $[g_b]$, which is a contradiction. □

We follow the procedure used in the above theorem until we have exhausted all the elements of the group $\mathscr{G}$, resulting in the decomposition of the group $\mathscr{G}$ into say some $k < n$ classes, where n is the order of $\mathscr{G}$.

Any Abelian group of order n has n classes, each containing one element and the identity element is always in a class by itself, traditionally denoted as C_1.

Finding the conjugacy classes of a group $\mathscr{G}$ is quite similar to coset decomposition. However note that a group $\mathscr{G}$ can have more than one coset decomposition as the same depends on the choice of subgroup of $\mathscr{G}$. When finding the conjugacy classes of $\mathscr{G}$ our construction doesn't depend on the choice of our elements $g_b, g_c, \ldots$, and is consequently *unique*.

Theorem 7. *Any group $\mathscr{G}$ is composed of a unique set of conjugate classes.*

1.2.12 Normal Subgroups[7]

Let $\mathscr{H}$ be a subgroup of a group $\mathscr{G}$. If we transform every element of $\mathscr{H}$ with respect to some $G \in \mathscr{G}$,

$$G\mathscr{H}G^{-1}$$

we obtain another subgroup [8] of $\mathscr{G}$ and is called as a *conjugate subgroup* of $\mathscr{H}$. Now $\mathscr{H}$ is said to be *normal* if it is left invariant on conjugation i.e.

$$\mathscr{H} = G\mathscr{H}G^{-1}$$

where $G \in \mathscr{G}$ and is represented as

$$\mathscr{H} \lhd \mathscr{G}$$

Aliter If the left coset $G\mathscr{H}$ and the right coset $\mathscr{H}G$ of a group $\mathscr{G}$ w.r.t. a subgroup $\mathscr{H}$ are equal, $\mathscr{H}$ is a normal subgroup.

Remark. Like groups, normal subgroups are also composed of classes.

Note that most groups have normal subgroups however those that have only the trivial normal subgroups, $\{E\}$ and the group itself, are called *simple groups.*

1.2.13 Simple groups

We now take a little detour to look at the types of simple groups, the so called *fundamental* groups. This distinction was first made by Galois, the founder of group theory who split groups into two types: simple groups and the remaining. Classification of all simple groups has been one of the greatest triumphs modern mathematics. Following are the types of simple groups[9]

- Cyclic groups of prime order $\mathcal{Z}_p$
- Alternating groups $\mathscr{A}_n$ for $n \geq 5$

[7] a.k.a. Invariant subgroups, Normal divisor

[8] The 2 conditions for a subset of $\mathscr{G}$ to be a subgroup are satisfied as follows

$$(GH_1G^{-1})(GH_2G^{-1}) = G(H_1H_2)G^{-1}$$

and for any element GHG^{-1} we have a corresponding inverse $GH^{-1}G^{-1}$ in $G\mathscr{H}G^{-1}$

[9] of which we shall study only the first two types

- Infinite families of groups of Lie type
- Twenty-six sporadic groups

In fact, Galois related the simplicity of the alternating group $\mathscr{A}_5$, to the impossibility of finding a formula that solves the quintic[10] equation by radicals. In Section 1.2.15 we will see how simple groups are the building blocks of all finite groups (and are hence called as *fundamental*).

1.2.14 Quotient group[11]

Recall the product group that we have already constructed. We now seek to divide a group $\mathscr{G}$[12] by its subgroup $\mathscr{H}$ (the divisor). This can be achieved by dividing $\mathscr{G}$ into cosets w.r.t. the subgroup $\mathscr{H}$ i.e.

$$\mathscr{G}/\mathscr{H} = \{a\mathscr{H}, a \in \mathscr{G}\}$$[13]

We need this newly group to satisfy the group axioms, and so we (intuitively) define group multiplication as

$$(a\mathscr{H})(b\mathscr{H}) = c\mathscr{H}$$

where $a, b \in \mathscr{G}$. This can turn out to be particularly problematic as $(a\mathscr{H})(b\mathscr{H})$ need not always produce a left coset. We overcome this by making the following assumption

$$a\mathscr{H} = \mathscr{H}a$$

which happens to be precisely the condition for a subgroup $\mathscr{H}$ to be a normal subgroup.
As a consequence we see that,

$$(a\mathscr{H})(b\mathscr{H}) = a\mathscr{H}\mathscr{H}b = a\mathscr{H}b = ab\mathscr{H}$$

which gives a satisfactory (and unconventional) group structure. This group has the identity element $\mathscr{H}$[14], and any element $a\mathscr{H}$ has an inverse of the form

[10] function of the form $g(x) = ax^5 + bx^4 + cx^3 + dx^2 + ex + f$

[11] a.k.a. Factor group

[12] ...to give a group whose elements are sets themselves!

[13] *"Huhh? Why not a right coset?"* Read on!

[14] the product group $\mathscr{H} \times \mathscr{H} = \mathscr{H}$ as any internal direct product always results in elements that belong to the group itself (closure)

$a^{-1}\mathscr{H}$.
By coset decomposition we have,

$$\mathscr{G} = g_1\mathscr{H} + g_2\mathscr{H} + \cdots + g_l\mathscr{H}$$

where

$$\mathscr{G}/\mathscr{H} = \{g_i\mathscr{H} \mid i = 1,\ldots,l\}$$

Observe that the group $\mathscr{G}/\mathscr{H}$ is of the order $l = n/h$ which also happens to be the index of $\mathscr{H}$.

Alternatively, we can represent the transformation of a group $\mathscr{G}$ into its cosets in terms of a mapping $\pi : \mathscr{G} \to \mathscr{G}/\mathscr{H}$, defined as, $\pi(g) = g\mathscr{H}$. Also we have,

$$\pi(g_1)\pi(g_2) = (g_1\mathscr{H})(g_2\mathscr{H}) = g_1g_2\mathscr{H} = \pi(g_1g_2)$$

and so π is a homomorphic mapping.

Theorem 8. *$\mathscr{H}$ is a normal subgroup of a group $\mathscr{G}$ iff it is the* kernel *of some isomorphism on $\mathscr{G}$.*

Proof. First we shall prove the forward implication. If $\mathscr{H}$ is the kernel of some mapping say f, we have

$$f(H) = E$$

where $H \in \mathscr{H}$. Observe that,

$$f(GHG^{-1}) = f(G)f(H)f(G^{-1}) = f(G)f(G^{-1}) = f(GG^{-1}) = E$$

and so $GHG^{-1} \in \mathscr{H}$ i.e. $G\mathscr{H}G^{-1} = \mathscr{H}$.

We now proceed to prove the backward implication. If $\mathscr{H}$ is a normal subgroup we have,

$$\mathscr{H} = G\mathscr{H}G^{-1}$$

Let's consider a homomorphic mapping $\pi : \mathscr{G} \to \mathscr{G}/\mathscr{H}$, defined as

$$\pi(g) = g\mathscr{H}$$

We know that $\mathscr{H}$ is the identity element of E' $\mathscr{G} \to \mathscr{G}/\mathscr{H}$ and $g\mathscr{H} = \mathscr{H}$ only for any $g \in \mathscr{H}$ and so,

$$\pi(H) = H\mathscr{H} = \mathscr{H} = E'$$

where $H \in \mathscr{H}$. Thus $\mathscr{H}$ is the kernel of the homomorphic mapping π. □

Theorem 9 (First Isomorphism Theorem)**.** *Let $f : \mathscr{G} \to \mathscr{G}'$ be a homomorphic mapping defined as $f(G) = G'$ and let $\mathscr{K}$ be its kernel. Let $\bar{f} : \mathscr{G}/\mathscr{K} \to \mathscr{G}'$ be another mapping defined as $\bar{f}(G\mathscr{K}) = f(G)$, then $\bar{f}$ is an isomorphic mapping,*

$$\mathscr{G}/\mathscr{K} \cong \mathscr{G}'$$

$$\begin{tikzcd}
\mathscr{G} \arrow[rr, "f"] \arrow[dr, "\pi"'] & & \mathscr{G}' \\
& \mathscr{G}/\mathscr{K} \arrow[ur, "\bar{f}"'] &
\end{tikzcd}$$

Figure 2: The first isomorphism theorem

Proof. Firstly we require $\bar{f}$ to be homomorphic. Observe that,

$$\bar{f}(G_1\mathscr{K})\bar{f}(G_2\mathscr{K}) = f(G_1)f(G_2) = f(G_1G_2) = \bar{f}(G_1G_2\mathscr{K})$$

i.e. $\bar{f}$ is indeed homomorphic. Now if $\bar{f}$ is not isomorphic, then for some $G_1, G_2 \in \mathscr{G}$ where $G_1 \neq G_2$ we have,

$$\bar{f}(G_1\mathscr{K}) = f(G_1) = f(G_2) = \bar{f}(G_2\mathscr{K})$$

and so,

$$f(G_1G_2^{-1}) = f(G_1)f(G_2^{-1}) = f(G_1)(f(G_2))^{-1} = E'$$

which means that $G_1G_2^{-1} \in \mathscr{K}$ or equivalently $G_1 \in G_2\mathscr{K}$; a contradiction as the cosets considered are disjoint. Therefore $\bar{f}$ is isomorphic. □

Theorem 10. *The quotient group $\mathscr{G}/\mathscr{H}$ is simple iff $\mathscr{H}$ is a maximal normal subgroup of $\mathscr{G}$.*

Proof. Consider a normal subgroup $\mathscr{A}$ such that,

$$\mathscr{H} \trianglelefteq \mathscr{A} \trianglelefteq \mathscr{G}$$

and so

$$\frac{\mathscr{A}}{\mathscr{H}} \trianglelefteq \frac{\mathscr{G}}{\mathscr{H}}$$

Now if $\mathscr{H}$ is a maximal normal subgroup, we have two possibilities, either $\mathscr{A} = \mathscr{H}$ or $\mathscr{A} = \mathscr{G}$ which implies that either $\mathscr{H}$ or $\mathscr{G}/\mathscr{H}$ respectively are the only normal subgroups. Hence proved that $\mathscr{G}/\mathscr{H}$ is simple.
For the reverse implication, if $\mathscr{G}/\mathscr{H}$ is simple, it is implied that $\mathscr{H}$ and $\mathscr{G}/\mathscr{H}$ are the only normal subgroups. This is possible only if $\mathscr{A} = \mathscr{H}$ or $\mathscr{A} = \mathscr{G}$ i.e. if $\mathscr{H}$ is a maximal normal subgroup. □

1.2.15 Composition series

Let $\mathscr{G}$ be a group with a maximal normal subgroup $\mathscr{H}_1$. We now split $\mathscr{G}$ using $\mathscr{H}_1$ into the quotient group $\mathscr{G}/\mathscr{H}_1$. Consider $\mathscr{H}_1$ and its maximal normal subgroup $\mathscr{H}_2$ and repeat the procedure we applied to $\mathscr{G}$. If we do so continuously we'll end up with a *simple* subgroup $\mathscr{H}_k$ whose only normal subgroup (besides itself) is the identity element of $\mathscr{G}$. This yields the *composition series*,

$$\mathscr{G} \rhd \mathscr{H}_1 \rhd \mathscr{H}_2 \rhd \cdots \rhd \mathscr{H}_k \rhd E$$

generating the quotient subgroups,

$$\mathscr{G}/\mathscr{H}_1, \mathscr{H}_1/\mathscr{H}_2, \ldots, \mathscr{H}_k$$

hence disintegrating $\mathscr{G}$ into its simple[15] constituents. We see that simple subgroups are the fundamental building blocks using which we can build all other finite groups.

Remark. A group can have more than one composition series as it depends on the maximal normal subgroup chosen[16]. However, the number of steps to the identity and the order of the quotient subgroups (called the *composition indices*) are invariant features. It is to be noted that these features are not unique to a group and hence we cannot use them to reconstruct a particular group.

In cases where all the quotient groups are cyclic with prime indices, the group is said to be *solvable* or *soluble*.

[15] since we have taken the maximal normal subgroups

[16] A maximal normal subgroup is defined as a normal subgroup which is not completely contained in any other proper normal subgroup. This doesn't mean that it is a normal subgroup of maximum possible order!

1.2.16 Commutator subgroup[17]

We define the commutator of some $a, b \in G$ as

$$[a, b] = a^{-1}b^{-1}ab$$

Observe that $[b, a] = [a, b]^{-1}$ and it can easily be seen that condition (1) is satisfied, hence the product of all possible commutators form a subgroup G'[18] called the *commutator subgroup*.
On conjugating any element of this subgroup we see that,

$$\widetilde{[a.b]} = g(a^{-1}b^{-1}ab)g^{-1} = [\tilde{a}, \tilde{b}]$$

i.e. any commutator subgroup is a normal subgroup.
Based on the characteristics of the commutator subgroup of a group, we have the following classes of groups:

- (Perfect groups) G' is the same as G.

  Remark. This doesn't mean that perfect groups are necessarily simple! However a *non-Abelian* simple group is perfect.

- (Abelian groups) $G' = e$

- $G' \triangleleft G$

1.2.17 Cauchy's theorem

Theorem 11 (Cauchy's theorem)**.** *Let $\mathscr{G}$ be a finite group and p be a prime. If p divides the order of $\mathscr{G}$ then the group must contain an element of order p.*

Sylow's first theorem is basically a generalization of Cauchy's theorem.

Theorem 12. *Let p be a prime and $\mathscr{P}$ be a p-group of order p^m then $\mathscr{P}$ has subgroups*[19] *of order p^r for any $r < m$.*

We can prove this using the fact that p-groups are solvable[20]

[17] a.k.a. Derived subgroup

[18] also denoted as $G^{(1)}$, $[G, G]$

[19] and not element!

[20] However we won't be proving this.

1.2.18 Sylow's Criteria

Let p be a prime number. We define *p-group* as a group whose order is a power of p or equivalently the order of every group element is a power of p (from Theorem 11). Let $\mathscr{G}$ be a group of order $n = p^m r$ where r is coprime to p. We have the following theorems that place very strong restrictions of the possible groups of a given order[21]

- $\mathscr{G}_p$ contains n_p *p-groups*, $\mathscr{G}_p^i$, $i = 1, \ldots, n_p$ of order p^m.
- All $\mathscr{G}_p^i$ are isomorphic to each other, and are related by $\mathscr{G}_p^j = g\mathscr{G}_p^k g^{-1}$ where $g \in \mathscr{G}$.
- n_p is a divisor of r.
- $n_p = 1 \mod p$

Consider the groups of order $n = pq$, where p, q are both prime. By Sylow's theorems we have n_p subgroups $\mathscr{G}_p$ of order p and n_q subgroups $\mathscr{G}_q$ of order q. From Theorem 14 these two subgroups must be cyclic. Also it is required that n_p is a divisor of q i.e. $n_p = 1$ or q. However $n_p = 1 \mod p$ and without loss of generality we can take $p > q$, so we must have $n_p = 1$. Similarly we say that $n_q = 1$ or p and since $n_q = 1 \mod q$, we have a possible solution $n_q = 1$. Hence we have

$$\mathscr{Z}_{pq} = \mathscr{Z}_p \times \mathscr{Z}_q$$

We have another solution $n_q = p$ *if* $p = 1 \mod q$. *p-groups* can be abelian (cyclic groups) or non-abelian (like the dihedral group $\mathscr{D}_4$).

* * *

[21] These shall prove to be extremely useful when we will construct various finite order groups1

2 Finite groups

Groups having a finite number of elements are known as *finite groups*. Any finite group $\mathscr{G}$ can be presented using the following notation

$$\mathscr{G} = \langle G | R_1, \ldots, R_n \rangle$$

and is called as a[22] *presentation* of $\mathscr{G}$, where G is the set of generators of $\mathscr{G}$ and $R_1, \ldots, R_n$ are relations from which any other relation in $\mathscr{G}$ can be deduced.

So far we have defined a group as finite on the basis of the number of elements it contains. Can we say anything regarding the *order* of the elements themselves?
Theorem 13. *The order of every element of a finite group $\mathscr{G}$ is finite.*

Proof. Let g be an element in $\mathscr{G}$, and so the set $\langle g \rangle$ of all integral powers of g must belong to $\mathscr{G}$. However since $\mathscr{G}$ is of finite order, all the elements of $\langle g \rangle$ cannot be distinct i.e. for some $a, b \in \mathscr{Z}$ where $a > b$

$$g^a = g^b \Leftrightarrow g^{a-b} = e$$

Since the above relation holds for a set of values of $(a - b)$, and by definition the order of g is $\min\{a - b\}$. □

We now look at some families of groups which we will subsequently use to generate finite groups of lower (< 13) orders.

2.1 Cyclic groups

A group is cyclic if every group element can be expressed as a power of a single element. We represent any n^{th} order cyclic group as $\mathscr{Z}_n$. A cyclic group with generator a can be presented as

$$\mathscr{Z}_n = \langle a \,|\, a^n = e \rangle$$

All cyclic groups are Abelian. (Why?)[23]

Theorem 14. *All groups of prime order are cyclic.*

[22] in general, there can be multiple presentations of a group

[23] Observe that $g^a g^b = g^{b+a}$

Proof. Let $\mathscr{G}$ be a group of prime order p and $\langle g \rangle$ be the group generated by some non identity element g in $\mathscr{G}$. By Lagrange's theorem any subgroup of $\mathscr{G}$ will either be the identity element or a group of order p i.e. $\mathscr{G}$ itself. By our assumption $\langle g \rangle$ cannot be the identity element and so we have $\mathscr{G} = \langle g \rangle$. □

Geometrically, cyclic groups can be interpreted as the set of rotational symmetries of a polygon.

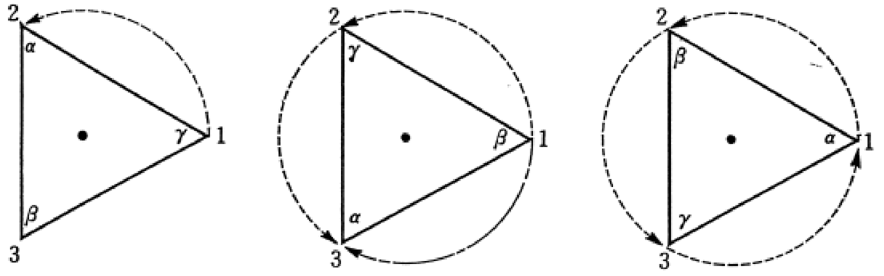
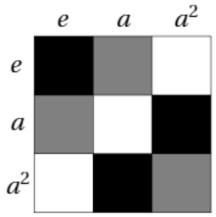


Figure 3: Geometric visualization of the cyclic group $\mathscr{Z}_3$



	e	a	a^2
e	■	▨	□
a	▨	□	■
a^2	□	■	▨

Figure 4: Multiplication table of the cyclic group $\mathscr{Z}_3$

2.2 Dihedral groups

A dihedral group is defined as the group of rotational and mirror symmetries of a polygon. The n^{th} $(n > 1)$ dihedral group $\mathscr{D}_n$ is a group order of $2n$ [24] and can be presented as

$$\mathscr{D}_n = \langle a, b | a^n = b^2 = e, (ab)^2 = e \rangle$$

[24] as it has $2n$ symmetries, n of which are the rotational symmetries and the remaining n are the reflections about the n lines of symmetry.

Geometrically, we interpret the generator a as the rotation symmetry that rotates the n-sided polygon by $2i\pi/n$ $(i = 1,\ldots,n)$ radians about its centre and interpret b as the reflection symmetry.

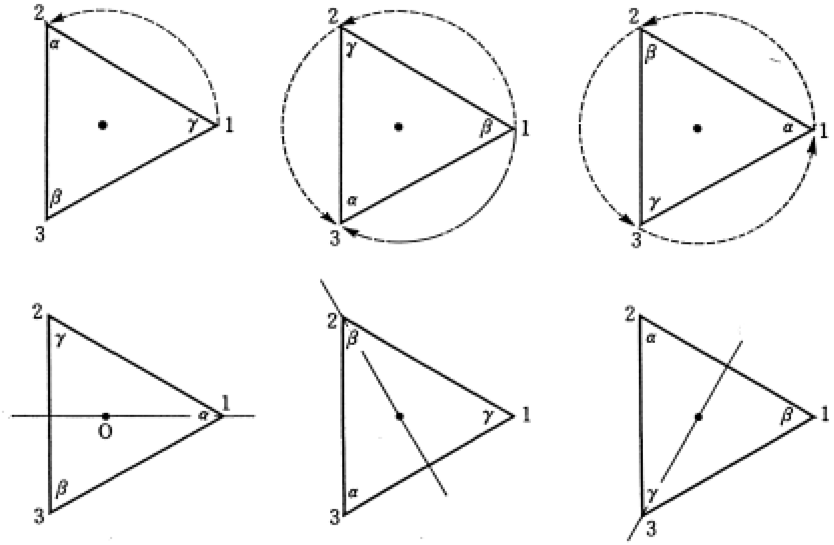


Figure 5: Geometric visualization of the dihedral group $\mathscr{D}_3$

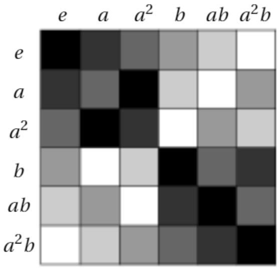


Figure 6: Multiplication table of the dihedral group $\mathscr{D}_3$

If $n \geq 3$ then $\mathscr{D}_n$ is non abelian i.e. $\mathscr{D}_2$ is the only abelian dihedral group.

2.3 Symmetric groups

The group of all possible permutations of n items[25] is called the *symmetric group* and is denoted by $\mathscr{S}_n$. Observe that the groups $\mathscr{Z}_n, \mathscr{D}_n$ can be thought of as groups of *certain* permutations of n objects. Consider a permutation on n objects $a_1, \dots, a_n$ which shuffles them to give a sequence $b_1, \dots, b_n$. We represent this permutation as

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}$$

The resultant of two permutation generates another permutation as follows

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ b_1 & b_2 & \cdots & b_n \end{pmatrix}\begin{pmatrix} b_1 & b_2 & \cdots & b_n \\ c_1 & c_2 & \cdots & c_n \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ c_1 & c_2 & \cdots & c_n \end{pmatrix}$$

However we will use the more concise *k-cycle* notation for permutations. A k-cycle is defined as a permutation that shuffles $k < n$ objects into themselves.

Examples: Consider the set of permutations on four objects. We write

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 3 & 4 \end{pmatrix}$$

Take another four-cycle element

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 4 & 2 & 3 \end{pmatrix}$$

which is read as $1 \to 4, 4 \to 2, 2 \to 3, 3 \to 1$. The following are a few other k-cycle elements.

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}\begin{pmatrix} 4 \end{pmatrix} \quad \text{[three-cycle]}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 \end{pmatrix}\begin{pmatrix} 3 \end{pmatrix}\begin{pmatrix} 4 \end{pmatrix} \quad \text{[two-cycle]}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 \end{pmatrix}\begin{pmatrix} 3 & 4 \end{pmatrix}$$

Observe that two-cycles simply swap two objects and henceforth we refer to them as *transpositions*. Also note that one-cycles leave the sequence invariant and hence can be omitted.

[25] The number of objects that a permutation acts on is called its *degree*.

Theorem 15. *Disjoint cycles commute.*

Proof. Let $a = (a_1 \cdots a_n)$ and $b = (b_1 \cdots b_m)$ be two disjoint cycles that act on a set of $n+m$ objects. Consider their product ab and any object x from the set. If x belongs to the set $\{a_1 \cdots a_n\}$ then the cycle b will leave it invariant and so ab will be nothing but a itself. Similarly for such an x, ba can be interpreted as the operation of b on any transformation of a which will essentially yield another object in the set $\{a_1 \cdots a_n\}$. Thus the action of ba will be the same as that of ab. □

2.3.1 Cycle decomposition

Theorem 16. *Every permutation can be uniquely resolved into cycles which operate on mutually exclusive sets.*

Proof. Consider a permutation on n objects and pick some object say k and folllow the chain of transformations that occur in the sequence i.e. $k \rightarrow k_1 \rightarrow \cdots \rightarrow k_{r-1} \rightarrow k$. If $r = n$ then the permutation is an n-cycle. However if $r < n$ then k goes back to into itself before we have completed one complete cycle through the n objects and so we have $n-r$ objects left unaccounted for. Now chose another element say m from the leftover objects and again trace the sequence of transformations back to m as $m \rightarrow m_1 \rightarrow \cdots \rightarrow m_{s-1} \rightarrow m$. If $s = n-r$ then we write the permutation as

$$(k\, k_1 \cdots k_{r-1})(m\, m_1 \cdots m_{n-r-1})$$

However if $s < n-r$ then we again repeat this procedure until we have covered the transformations of all n objects and arrive at the cycle decomposition

$$(k\, k_1 \cdots k_{r-1})(m\, m_1 \cdots m_{s-1}) \cdots (p\, p_1 \cdots p_{w-1})$$

where $r + s + \cdots + w = n$.

Observe that the transformation that a permutation results in is a one-to-one mapping hence the above cycles are self contained and disjoint[26] Also as any k-cycle is independent of the choice of the starting element from a particular set of objects this decomposition is unique. □

[26] Any k_i, m_j cannot be transformed into the other.

We can also decompose any permutation as a product of transpositions as follows

$$(a_1\, a_2\, a_3 \cdots a_n) = (a_1 a_2)(a_1 a_3)\cdots(a_1 a_n) = (a_1 a_2)(a_2 a_3)\cdots(a_n a_1)$$

Note that this product is not commutative (because the sets aren't mutually exclusive!). Hence we see that any cycle in $\mathscr{S}_n$ can be generated by the transpositions $(a_1 a_2), (a_2 a_3), \ldots, (a_n a_1)$ [27]. This gives us a presentation of $\mathscr{S}_n$

$$\mathscr{S}_n = \langle (a_1 a_2), (a_2 a_3), \ldots, (a_n a_1) \rangle$$

If the number of transpositions are *even* (*odd*) then the permutation is said to be *even* (*odd*). This can also be determined in terms of the *parity* of a permutation which is defined as

$$\operatorname{sgn} \sigma = (-1)^{n-c}$$

where n is the number of objects on which the permutation is done and c the number of disjoint cycles in the cycle decomposition. The parity of the permutation is 1 for even permutations and -1 for odd permutations.

Theorem 17. *All permutations are either even or odd.*

Proof. Let γ be a permutation that can be decomposed into an even and odd number of transpositions as follows

$$\gamma = (a_1 \cdots a_m) = (b_1 \cdots b_n)$$

where a_i, b_j are transpositions and m, n are odd and even respectively. It can easily be shown that

$$\gamma^{-1} = (b_n \cdots b_1)$$

and so

$$\gamma\gamma^{-1} = e = (a_1 \cdots a_m)(b_n \cdots b_1)$$

i.e. the identity element e is odd which is a contradiction as the identity element can only be obtained on performing an even number of transpositions. □

[27] Another such set could be $(a_1 a_2), (a_1 a_3), \ldots, (a_1 a_n)$. Like all sets of generators these are only some of the many possibilities!

The set of all even permutations forms a subgroup of $\mathscr{S}_n$ of order[28] $n!/2$ called the *alternating group* $\mathscr{A}_n$.

Let $\mathscr{G}$ be a group with elements g_i, $i = 1,\ldots,n$, we define the permutation of degree n

$$P_a = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ g_1 g_a & g_2 g_a & \cdots & g_n g_a \end{pmatrix}$$

where $g_a \in \mathscr{G}$. Notice the one-to-one correspondence between

$$g_a g_b = g_c \to P_a P_b = P_c$$

Also the group representation $\{P_a\}$ of $\mathscr{G}$ is a subgroup of $\mathscr{S}_n$ and so we have the following result:

Theorem 18 (Cayley's theorem)**.** *Every group of finite order n is isomorphic to a subgroup of the permutation group* $\mathscr{S}_n$.

The permutations P_a form a representation called the *regular representation*, where each P_a is a $(n \times n)$ matrix acting on the n objects arranged as a column matrix. Suppose we transform a permutation P

$$P = (p_1\, p_2 \cdots p_n)$$

by g we get,

$$gPg^{-1} = (g(p_1)\, g(p_2) \cdots g(p_n))$$

i.e. conjugacy preserves the cycle decomposition of any permutation and this can be verified by operating the transformed permutation gPg^{-1} on the transformed object $g(p_i)$

$$gPg^{-1}g(p_i) = gP(p_i) = g(p_{i+1})$$

2.4 Finite groups of low order

We now construct the finite groups of order less than 13 and discuss some of their representations.

[28] The number of even permutations will be

$$\sum_{r=1}^{2[\frac{n}{2}]} \binom{n}{2r} = \frac{n!}{2}$$

2.4.1 Groups of order 2

By the group axioms any group of order 2 will look like

$$\{e, a\}$$

and a^2 is obviously equal to the identity element e, giving the multiplication table

$\mathscr{Z}_2$	e	a
e	e	a
a	a	e

Hence the cyclic group $\mathscr{Z}_2$ is the only group of order two. However doing this was unnecessary. (Recall Theorem 14)

2.4.2 Groups of order 3

From Theorem 14 the cyclic group $\mathscr{Z}_3$ is the only possible group of order 3.

$\mathscr{Z}_3$	e	a	a^2
e	e	a	a^2
a	a	a^2	e
a^2	a^2	e	a

Since constructing groups of prime order is quite straightforward we shall skip the same for orders 5, 7, 11, 13.

2.4.3 Groups of order 4

One obvious possibility is the cyclic group $\mathscr{Z}_4$. Any order 4 group will be of the form

$$\{e, a_1, a_2, a_3\}$$

Suppose a_1, a_2 are the generators of such a group. Then we must have $a_3 = a_1 a_2 = a_1 a_2$ and $a_1^2 = a_2^2 = e$. A presentation of this group would be

$$\langle a_1, a_2 | a_1^2 = a_2^2 = e \rangle$$

which also happens to be a presentation of the dihedral group $\mathscr{D}_2$. Observe that the direct product of the commuting (cyclic) groups (e, a_1) and (e, a_2) also gives $\mathscr{D}_2$. Thus we have

$$\mathscr{D}_2 = \mathscr{Z}_2 \times \mathscr{Z}_2$$

with the multiplication table

$\mathscr{D}_{\mathbf{2}}$	e	a_1	a_2	a_1a_2
e	e	a_1	a_2	a_1a_2
a_1	a_1	e	a_1a_2	a_2
a_2	a_2	a_1a_2	e	a_1
a_1a_2	a_1a_2	a_1	a_2	e

Since the multiplication table is symmetric about its diagonal the dihedral group $\mathscr{D}_2$ is abelian and is also called as V, *Vierergruppe* or *Klein's four-group*.

A possible representation of the dihedral group $\mathscr{D}_2$ are the following set of (2×2) matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

Another representation involving functional dependence is as follows

$$f_1(x) = x \qquad f_2(x) = -x \qquad f_3(x) = \frac{1}{x} \qquad f_4(x) = -\frac{1}{x}$$

where f_1, f_2, f_3, f_4 are like operators, similar to the action of group elements on a space.

2.4.4 Groups of order 6

The cyclic group $\mathscr{Z}_6$ and the direct product group $\mathscr{Z}_2 \times \mathscr{Z}_3$ are the two possible abelian groups of order 6. Let a, b be the generators of the direct product group i.e.

$$\mathscr{Z}_2 \times \mathscr{Z}_3 = \{e, a, a^2, b, ab, a^2b\}$$

such that $a^3 = b^2 = e$ and $ab = ba$. Observe that $(ab)^3 = b$ and so ab is of order 6, implying that the direct product group has a single generator, hence it is cyclic.

$$\mathscr{Z}_2 \times \mathscr{Z}_3 = \mathscr{Z}_6$$

The direct product group needn't always be cyclic.

Theorem 19. *A direct product group $\mathscr{Z}_m \times \mathscr{Z}_n$ is cyclic iff m, n are coprime.*

Proof. Let a, b be the generators of the cyclic groups $\mathscr{Z}_n, \mathscr{Z}_m$ respectively. Consider the direct product (a, b) then

$$(ab)^k = e = e_a e_b$$

where k is the order of ab and e_a, e_b are the identity elements of the cyclic groups $\mathscr{Z}_n, \mathscr{Z}_m$. Since the two cyclic groups operate on independent spaces we must have

$$a^k = e_a \quad b^k = e_b$$

i.e. $k = \text{lcm}(m, n)$. We have $k = mn$ iff m, n are coprimes. Since mn also happens to be the order of the direct product group $\mathscr{Z}_m \times \mathscr{Z}_n$, we have ab as its generator. Hence $\mathscr{Z}_m \times \mathscr{Z}_n$ is cyclic. □

Corollary 20. *A direct product group $\mathscr{Z}_m \times \mathscr{Z}_n \times \cdots \times \mathscr{Z}_s$ is cyclic iff $m, n, \ldots, s$ are coprime.*

Any group of order 6 by Lagrange's theorem must contain an order 3 element say a and so $\{e, a, a^2\}$ will be a subgroup of the order 6 group. If this group contains another element say b we get the following 6 elements

$$\{e, a, a^2, b, ba, ba^2\}$$

The element b will either be of order 2 or 3. If $b^3 = e$ then b^2 must be equal to ba or ba^2 implies $b = a$ or a^2. However this is a contradiction as group elements must be distinct. If $b^2 = e$ then $ab = ba$ or ba^2. If $ab = ba$ then we get the cyclic group $\mathscr{Z}_6$ again. Thus any other group must be non-abelian and must have $ab = ba^2$, giving us the dihedral group $\mathscr{D}_3$ with the following group presentation

$$\mathscr{D}_3 = \langle a, b | a^3 = b^2 = e, \; ba = a^2 b \rangle$$

Also observe that the permutation group $\mathscr{S}_3$ is another group of order 6. By definition the dihedral group $\mathscr{D}_3$ is the set of 6 rotational and mirror symmetries of an equilateral triangle, which also happens to be the set of all possible permutations of 3 objects.

$$\mathscr{D}_3 = \mathscr{S}_3$$

We now look at a representation of the dihedral group $\mathscr{D}_3$ interms of (3×3) matrices. Consider a triangle with vertices *A, B, C*. Since b is of order 2 and a of order 3 we draw the following relation

$$b = (A\,B) \rightarrow \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad a = (A\,B\,C) \rightarrow \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

where the group action is simply matrix multiplication.

2.4.5 Groups of order 8

We have the obvious possibilities

$$\mathscr{Z}_8 \qquad \mathscr{Z}_2 \times \mathscr{Z}_4 \qquad \mathscr{D}_2 \times \mathscr{Z}_2 \qquad \mathscr{D}_4$$

however we shall systematically construct these groups inorder to avoid missing out on any possibilities.[29] Suppose such a group has an element of order 8, the only such group is the cyclic group $\mathscr{Z}_8$. Any other group of order 8 (which doesn't have an order 8 element) must have an element of order 2 (Theorem 11) and *can* have an order 4 element. Suppose the group has an order 4 element, say a then $\{e, a, a^2, a^3\}$ will be its subgroup. If we consider another element b that doesn't belong to this subgroup we obtain the following 8 group elements

$$\{e, a, a^2, a^3, b, ba, ba^2, ba^3\}$$

Observe that any order 8 group is a Sylow's two-group and so b can either be of order 2 or 4. If $b^4 = e$ then $b^2 = e$ or a^2. If $b^2 = e$ then $ab = ba, ba^2$ or ba^3. For $ab = ba$ we get the direct product group $\mathscr{Z}_2 \times \mathscr{Z}_4$. If $ab = ba^2$ then

$$\begin{aligned} bab &= a^2 \\ (bab)^2 &= e \\ ba^2b &= e \\ a^2 &= e \qquad\qquad \textit{(Contradiction.)} \end{aligned}$$

If $ab = ba^3$ we get $(ab)^2 = e$, generating the dihedral group $\mathscr{D}_4$.

If $b^2 = a^2$ then $ab = ba, ba^2$ or ba^3. Again if $ab = ba$ we get the direct product group $\mathscr{Z}_2 \times \mathscr{Z}_4$, and if $ab = ba^2$ we run into a contradiction. Finally if $ab = ba^3$ we get a new group, $\mathscr{Q}$ called the quaternion group and its presentation is

$$\mathscr{Q} = \langle a, b \,|\, a^4 = e,\ a^2 = b^2,\ aba = b\rangle$$

The last possibility is of a group that has neither an order 8 nor an order 4 element and the only such group is the the direct product group $\mathscr{Z}_2 \times \mathscr{Z}_2 \times \mathscr{Z}_2$.[30]

[29] This will payoff!

[30] $= \mathscr{D}_2 \times \mathscr{Z}_2$

2.4.6 Groups of order 9

Ofcourse following the procedure that we have used to construct groups so far will be quite tedious. However the following theorem makes our job fairly simple.

Theorem 21. *Any group of order p^2 where p is a prime is abelian.*

Hence we narrow down to two possibilities, the cyclic group and the direct product group i.e. $\mathscr{Z}_9$ and $\mathscr{Z}_3 \times \mathscr{Z}_3$ respectively.

2.4.7 Groups of order 10

Observe that the order of this group is of the form $n = pq$ where p, q are primes and so we can use the result we had discussed under Sylow's theorem. As $5 = 1 \mod 2$ there can be at most two order 10 groups, one of which is obviously be the cyclic group $\mathscr{Z}_{10}$. Since the order is even the second possibility is the dihedral group $\mathscr{D}_5$.

2.4.8 Groups of order 12

Again we list the obvious possibilities

$$\mathscr{Z}_{12} \quad \mathscr{Z}_3 \times \mathscr{Z}_4 \quad \mathscr{Z}_2 \times \mathscr{Z}_6 \quad \mathscr{D}_6 \quad \mathscr{D}_3 \times \mathscr{Z}_2 \quad \mathscr{D}_2 \times \mathscr{Z}_3 \quad \mathscr{A}_4$$

However we have the following isomorphisms

$$\mathscr{Z}_2 \times \mathscr{Z}_6 = \mathscr{Z}_2 \times \mathscr{Z}_2 \times \mathscr{Z}_6 = \mathscr{D}_2 \times \mathscr{Z}_3$$

$$\mathscr{Z}_{12} = \mathscr{Z}_4 \times \mathscr{Z}_3$$

Another not so obvious isomorphism is

$$\mathscr{D}_6 = \mathscr{D}_3 \times \mathscr{Z}_2$$

We know that $\mathscr{D}_3$ is the set of rotational and mirror symmetries of an equilateral triangle, $\mathscr{D}_6$ is the same but for a regular hexagon and $\mathscr{Z}_2$ is essentially reflection. In order to derive this homomorphism we consider some group $D = \{e, s, r^2, sr^2, r^4, sr^4\}$ and $Z_2 = \{e, r^3\}$ and where r is a rotation of 60° about the centre of a hexagon and s is the reflection about the rotational axes of symmetry of a hexagon. Since

$$D_3 \times Z_2 = \{e, s, r, sr, r^2, sr^2, r^4, sr^4, r^3, sr^3, r^5, sr^5\}$$

we get the required isomorphism.

Adding on to these there are two[31] new non abelian groups of order 12. First is the tetrahedral group $\mathscr{T}$[32] which is isomorphic to the alternating group $\mathscr{A}_4$ and its presentation is

$$\mathscr{T} = \langle a, b \,|\, s^2 = r^3 = (sr)^3 = e \rangle$$

having the multiplication table

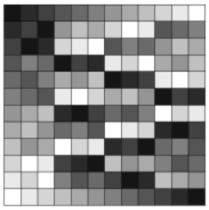


Figure 7: Multiplication table of the tetrahedral group $\mathscr{T}$

The alternating group $\mathscr{A}_4$ is generated by the even permutations of 4 objects. Similarly the tetrahedral group $\mathscr{T}$ can be visualized as the set of rotational symmetries of a tetrahedron.

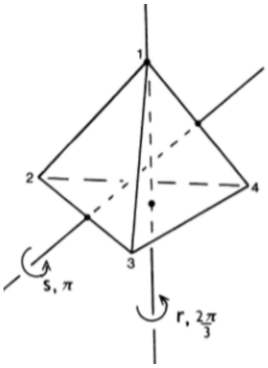


Figure 8: Geometric visualization of the tetrahedral group $\mathscr{T}$

[31] technically only one as the other group is isomorphic to one of our *obvious* groups

[32] Actually this the pure rotational subgroup of the tetrahedral group $\mathscr{T}_d$ which is the set of all possible symmetries of a tetrahedron.

This group can be generated by the (4×4) matrices

$$s = (12)(34) \to \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad r = (123) \to \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

hence generating the four-dimensional matrix representation of $\mathscr{T}$.

The second one is the group Γ which belongs to the family of dicyclic groups $\mathscr{Q}_{2n}$ and it has the presentation

$$\Gamma = \langle a, b \,|\, a^6 = e,\, b^2 = a^3, bab^{-1} = a^{-1} \rangle$$

* * *

Order	$N\,[N_{Abel}]$	Order	$N\,[N_{Abel}]$	Order	$N\,[N_{Abel}]$	Order	$N\,[N_{Abel}]$	Order	$N\,[N_{Abel}]$
1	1[1]	41	1[1]	81	15[5]	121	2[2]	161	1[1]
2	1[1]	42	6[1]	82	2[1]	122	2[1]	162	55[5]
3	1[1]	43	1[1]	83	1[1]	123	1[1]	163	1[1]
4	2[2]	44	4[2]	84	15[2]	124	4[2]	164	5[2]
5	1[1]	45	2[2]	85	1[1]	125	5[3]	165	2[1]
6	2[1]	46	2[1]	86	2[1]	126	16[2]	166	2[1]
7	1[1]	47	1[1]	87	1[1]	127	1[1]	167	1[1]
8	5[3]	48	52[5]	88	12[3]	128	2328[15]	168	57[3]
9	2[2]	49	2[2]	89	1[1]	129	2[1]	169	2[2]
10	2[1]	50	2[2]	90	10[2]	130	4[1]	170	4[1]
11	1[1]	51	1[1]	91	1[1]	131	1[1]	171	5[2]
12	5[2]	52	5[2]	92	4[2]	132	10[2]	172	4[2]
13	1[1]	53	1[1]	93	2[1]	133	1[1]	173	1[1]
14	2[1]	54	15[3]	94	2[1]	134	2[1]	174	4[1]
15	1[1]	55	2[1]	95	1[1]	135	5[3]	175	2[2]
16	14[5]	56	13[3]	96	230[7]	136	15[3]	176	42[5]
17	1[1]	57	2[1]	97	1[1]	137	1[1]	177	1[1]
18	5[2]	58	2[1]	98	5[2]	138	4[1]	178	2[1]
19	1[1]	59	1[1]	99	2[2]	139	1[1]	179	1[1]
20	5[2]	60	13[2]	100	16[4]	140	11[2]	180	37[4]
21	2[1]	61	1[1]	101	1[1]	141	1[1]	181	1[1]
22	2[1]	62	2[1]	102	4[1]	142	2[1]	182	4[1]
23	1[1]	63	4[2]	103	1[1]	143	1[1]	183	2[1]
24	15[3]	64	267[11]	104	14[3]	144	197[10]	184	12[3]
25	2[2]	65	1[1]	105	2[1]	145	1[1]	185	1[1]
26	2[1]	66	4[1]	106	2[1]	146	2[1]	186	6[1]
27	5[3]	67	1[1]	107	1[1]	147	6[2]	187	1[1]
28	4[2]	68	5[2]	108	45[6]	148	5[2]	188	4[2]
29	1[1]	69	1[1]	109	1[1]	149	1[1]	189	13[3]
30	4[1]	70	4[1]	110	6[1]	150	13[2]	190	4[1]
31	1[1]	71	1[1]	111	2[1]	151	1[1]	191	1[1]
32	51[7]	72	50[6]	112	43[5]	152	12[3]	192	1543[11]
33	1[1]	73	1[1]	113	1[1]	153	2[2]	193	1[1]
34	2[1]	74	2[1]	114	6[1]	154	4[1]	194	2[1]
35	1[1]	75	3[2]	115	1[1]	155	2[1]	195	2[1]
36	14[4]	76	4[2]	116	5[2]	156	18[2]	196	17[4]
37	1[1]	77	1[1]	117	4[2]	157	1[1]	197	1[1]
38	2[1]	78	6[1]	118	2[1]	158	2[1]	198	10[2]
39	2[1]	79	1[1]	119	1[1]	159	1[1]	199	1[1]
40	14[3]	80	52[5]	120	47[3]	160	238[7]	200	52[6]

Table 1: Number of groups of orders up to 200

3 Representation theory of finite groups

Representations are realisation of groups on linear vector spaces. So far we have seen that group action of any finite group of order n can be represented in terms of $(n \times n)$ matrices (Section 2.3.1) and that group elements are nothing but operators. Simply put the representation theory of finite groups involves representing group operations in terms of matrices acting on some vector space. However the regular representation for practical purposes (relatively larger values of n) can be difficult to manage. We now see how we can reduce them down to smaller *irreducible* matrices.

3.1 Hilbert Spaces

Owing to their physical relevance we shall specifically work in *Hilbert spaces.*

Hilbert spaces are complex vector spaces with an inner product.

What does this mean? Consider a complex vector space V on which we define the inner product $\langle a, b\rangle$ which gives rise to a norm as follows

$$\|x\| = \sqrt{\langle x, x\rangle}$$

A sequence of vectors x_n, $n = 1, \ldots, \infty$ in V is said to converge to a vector x in V if

$$\lim_{n\to\infty} \|x_n - x\| = 0$$

and we call $\|x_n - x\|$ as the norm of differences. If the norm of differences approaches zero we say that the vector space V is complete with respect to this norm and hence V is a *Hilbert space.*

3.1.1 Bra-ket notation

While dealing with Hilbert spaces we shall use the *bra-ket* notation. In this notation we denote the inner product $\langle u, v\rangle$ as

$$\langle u|v\rangle$$

Here $|v\rangle$ is called a *ket* and $\langle u|$ is called a *bra.* Essentially kets are just another way to represent vectors and so belong to the space V. Bras on the other hand belong to the space V^*. Consider a vector $v \in V$ and a linear function $\phi \in V^*$, then $\phi(v)$ denotes the action of the function ϕ on the vector v and gives a number. In the *bra-ket* notation we denote this as

$$\begin{aligned} v &\to |v\rangle \\ u &\to \langle u| \\ \phi &\to \langle u|v\rangle \end{aligned}$$

Bras and kets can also be viewed as row and column vectors respectively. Consider two vectors a, b which can be written in terms of matrices as

$$a = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \quad b = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$$

and so $\langle a|$ and $|b\rangle$ can be thought of as

$$\Big\langle a \Big| = \big(a_1^*, a_2^* \ldots, a_n^*\big) \quad \Big| b \Big\rangle = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$$

and we define the outer product as

$$|b\rangle\langle a|$$

which results in an $(n \times n)$ matrix i.e. an operator.

Let V be an N-dimensional having the basis $\{e_i\}$, $i = 1, \ldots, N$. We write $|e_i\rangle$ as $|i\rangle$ and hence say that V is spanned by the orthonormal set of kets $|i\rangle$. Then we have

$$\langle i|j\rangle = \delta_{ij} \qquad \sum_{i=1}^{N} |i\rangle\langle i| = \mathbf{1}$$

where **1** is the $(n \times n)$ unitary matrix or identity operator.

3.2 Reducible & Irreducible representations

Consider a finite N-dimensional vector space V and let $\mathscr{G}$ be an order n group. We represent the action of $g \in \mathscr{G}$ on this vector space by $(N \times N)$ non-singular matrices which act as

$$|i\rangle \to |i(g)\rangle = \mathscr{M}_{ij}|j\rangle$$

with

$$\mathcal{M}_{ij}(g^{-1}) = \mathcal{M}_{ij}^{-1}(g)$$

hence forming an N-dimensional representation $\mathcal{R}$ of $\mathcal{G}$. Now if $n = N$ then we get the regular representation. If the representation $\mathcal{R}$ can be broken down into the smallest possible non-trivial[33] representations, we say that $\mathcal{R}$ is *reducible.*

Now suppose the representation $\mathcal{R}$ is reducible and can be reduced to an irreducible representation $\mathcal{R}_1$ of $\mathcal{G}$ of dimension $N_1 < N$ that acts on a subspace V_1 of V spanned by $|a\rangle$, $a = 1, \dots, N_1$. The space spanned by the remaining $|m\rangle$, $m = 1, \dots, N - N_1$ is the orthogonal complement V_1' of V. Hence the representation matrices of $\mathcal{R}$ will be of the form

$$\mathcal{M}(g) = \begin{pmatrix} \mathcal{M}_1(g) & \mathcal{N}(g) \\ 0 & \mathcal{M}_1'(g) \end{pmatrix}$$

where $\mathcal{M}_1(g)$, $\mathcal{N}(g)$ and $\mathcal{M}(g)$ are $N_1 \times N_1, N_1 \times (N - N_1)$ and $(N - N_1) \times (N - N_1)$ matrices.

<u>*Justification*</u> Since $\mathcal{M}(g)$ is a group representation we have

$$\mathcal{M}(g_1 g_2) = \mathcal{M}(g_1)\mathcal{M}(g_2)$$

then we see that this form is preserved under matrix multiplication as

$$\mathcal{M}(g_1 g_2) = \begin{pmatrix} \mathcal{M}_1(g_1)\mathcal{M}_1(g_2) & \mathcal{M}_1(g_1)\mathcal{N}(g_2) + \mathcal{N}(g_1)\mathcal{M}_1(g_2) \\ 0 & \mathcal{M}_1'(g_1)\mathcal{M}_1'(g_2) \end{pmatrix}$$

and we get an N_1 dimensional representation $\mathcal{R}_1$ as $\mathcal{M}_1(g_1 g_2) = \mathcal{M}_1(g_1)\mathcal{M}_1(g_2)$ and an $(N - N_1)$ dimensional representation $\mathcal{R}_1'$ as $\mathcal{M}_1'(g_1 g_2) = \mathcal{M}_1'(g_1)\mathcal{M}_1'(g_2)$.

Consider a vector $|a\rangle \in V_1$ then we have

$$\begin{pmatrix} \mathcal{M}_1(g) & \mathcal{N}(g) \\ 0 & \mathcal{M}_1'(g) \end{pmatrix} \begin{pmatrix} a \\ 0 \end{pmatrix} = \begin{pmatrix} \mathcal{M}_1(g)a \\ 0 \end{pmatrix}$$

and so any transformation by $\mathcal{M}_1$ leaves the subspace V_1 invariant. However, if we do the same for a vector $|m\rangle \in V_1'$ we get

$$\begin{pmatrix} \mathcal{M}_1(g) & \mathcal{N}(g) \\ 0 & \mathcal{M}_1'(g) \end{pmatrix} \begin{pmatrix} 0 \\ m \end{pmatrix} = \begin{pmatrix} \mathcal{N}(g)m \\ \mathcal{M}_1'(g)m \end{pmatrix}$$

[33] The trivial representation being the one dimensional representation where every group action is multiplication by 1 i.e. the action of the identity element, which every group has.

the transformation results in a vector that belongs to V and so under this transformation the complementary $(N-N_1)$ dimension subspace is not invariant.

If suppose $\mathscr{N}(g)=0$ then the complementary $(N-N_1)$ dimension subspace is also left invariant under all transformations of the group. This would mean that the basis vectors $|a\rangle$, $a=1,\dots,N_1$ transform among themselves and so do the basis vectors $|m\rangle$, $m=1,\dots,N_1$, hence the transformations don't couple two subspaces. In other words the vector space V is decomposed into the direct sum of the independent subspaces V_1 and V_2 as

$$V = V_1 \oplus V_1'$$

and the representation $\mathscr{R}$ is decomposed as

$$\mathscr{R} = \mathscr{R}_1 \oplus \mathscr{R}_1'$$

and $\mathscr{R}$ is said to be fully reducible. In such a situation the representation matrices will assume the block diagonal form

$$\mathscr{M}(g) = \begin{pmatrix} \mathscr{M}_1(g) & 0 \\ 0 & \mathscr{M}_1'(g) \end{pmatrix}$$

We obtain this from by doing a change of basis which can be brought about by multiplying $\mathscr{M}(g)$ by

$$\begin{pmatrix} 1 & 0 \\ \mathscr{N}' & 1 \end{pmatrix}$$

where $\mathscr{N}' = \frac{1}{n}\sum_g \mathscr{M}_1'(g^{-1})\mathscr{N}$. We continue this process if $\mathscr{R}_1'$ itself is reducible and we end up with the decomposition

$$V = V_1 \oplus \cdots \oplus V_k$$

and

$$\mathscr{R} = \mathscr{R}_1 \oplus \cdots \oplus \mathscr{R}_k$$

3.3 Schur's Lemmas

Lemma 1 (Schur's First Lemma). *For two given irreducible representations $\mathscr{R}_1$ and $\mathscr{R}_2$ of dimensions N_1 and N_2 respectively, a rectangular matrix $\mathscr{S}$ that satisfies*

$$\mathscr{S}\mathscr{M}_1 = \mathscr{M}_2\mathscr{S}$$

for any group element $g \in \mathscr{G}$ must be either

1. *the zero matrix*

2. *a square matrix* $(N_1 = N_2)$ *and* $\det \mathscr{S} \neq 0$

Proof. Let the basis of the irreducible representations $\mathscr{R}_1$ and $\mathscr{R}_2$ be $\{|a_1\rangle\}$ and $\{|a_2\rangle\}$ respectively with $N_1 > N_2$. Let $\mathscr{S}$ be the matrix of transformation of $\{|a_1\rangle\}$ to $\{|a_2\rangle\}$. We have

$$g|a_1\rangle = \mathscr{M}_1(g)|b_1\rangle$$

where $g \in \mathscr{G}$ and

$$|a_2\rangle = \mathscr{S}|a_1\rangle \quad |b_2\rangle = \mathscr{S}|b_1\rangle$$

then

$$g|a_2\rangle = \mathscr{S}g|a_1\rangle = (\mathscr{S}\mathscr{M}_1(g))|b_1\rangle = \mathscr{M}_2(g)(\mathscr{S}|b_1\rangle) = \mathscr{M}_2(g)|b_2\rangle$$

which means that the representation $\mathscr{R}_1$ is reducible if $\mathscr{S} \neq 0$ which is a contradiction. Hence, $\mathscr{S} = 0$ if $N_1 \neq N_2$.
Now if $N_1 = N_2$ and if $|a_1\rangle$ and $|a_2\rangle$ span the same Hilbert space then $\mathscr{S} \neq 0$ and $\mathscr{R}_1$ and $\mathscr{R}_2$ are said to be equivalent i.e.

$$\mathscr{M}_1 = \mathscr{S}^{-1}\mathscr{M}_2\mathscr{S}$$

However if if $|a_1\rangle$ and $|a_2\rangle$ span different Hilbert spaces then $\mathscr{S} = 0$. □

Lemma 2 (Schur's Second Lemma)**.** *A matrix $\mathscr{S}$ that commutes with all the representation matrices $\mathscr{M}$ of a representation $\mathscr{R}$ of the group $\mathscr{G}$ i.e.*

$$\mathscr{S}\mathscr{M}(g) = \mathscr{M}(g)\mathscr{S}$$

where $g \in \mathscr{G}$, must be a multiple of the identity matrix I

$$\mathscr{S} = cI$$

if $\mathscr{R}$ is irreducible.

Proof. Let $\lambda \in \mathbb{C}$ be the eigenvalue of $\mathscr{S}$ such that

$$\mathscr{S}v = \lambda v$$

then

$$\mathscr{M}(g)\mathscr{S}v = \lambda\mathscr{M}(g)v \Leftrightarrow \mathscr{S}\mathscr{M}(g) = \lambda\mathscr{M}v$$

i.e. $\mathscr{M}v$ is also an eigenvector. This would mean that the subspace of eigenvectors of $\mathscr{S}$ is invariant under all transformations of the group $\mathscr{G}$ and so $\mathscr{R}$ is reducible unless the subspace of eigenvectors spans the whole space. If they span the entire space then $\mathscr{S} = \lambda I$. □

3.4 The great orthogonality theorem

Theorem 22 (The Great Orthogonality Theorem)**.** *Matrices $\mathscr{M}$ in V of an N dimensional irreducible unitary*[34] *representation $\mathscr{R}$ satisfy the following orthogonality relations*[35]

$$\frac{1}{n}\sum_g M_{ij}(g)M^*_{qp}(g) = \frac{1}{N}\delta_{iq}\delta_{jp}$$

where n is the order of the group $\mathscr{G}$ and $g \in \mathscr{G}$. If $\mathscr{R}_A$ and $\mathscr{R}_B$ are inequivalent irreducible representations of dimensions N_A and N_B $(N_A \neq N_B)$ and representation matrices $\mathscr{A}$ and $\mathscr{B}$ respectively

$$\frac{1}{n}\sum_g A_{ij}(g)B^*_{qp}(g) = 0$$

The two orthogonality relations combined together give

$$\frac{1}{n}\sum_g A_{ij}(g)B^*_{qp}(g) = \frac{1}{N_A}\delta_{AB}\delta_{iq}\delta_{jp}$$

Proof. Let $\mathscr{N}$ be an arbitrary $(N_A \times N_B)$ matrix. We construct a matrix $\mathscr{S}$ as

$$\mathscr{S} = \sum_g \mathscr{A}(g)\mathscr{N}\mathscr{B}(g^{-1})$$

then observe that for some $g' \in \mathscr{G}$

$$\mathscr{A}(g')\mathscr{S} = \sum_g \mathscr{A}(g')\mathscr{A}(g)\mathscr{N}\mathscr{B}(g^{-1}) = \sum_g \mathscr{A}(g'g)\mathscr{N}\mathscr{B}(g^{-1})$$

let $g" = g'g$

$$\mathscr{A}(g')\mathscr{S} = \sum_g \mathscr{A}(g')\mathscr{A}(g)\mathscr{N}\mathscr{B}((g"(g')^{-1})^{-1}) = \left(\sum_{g"} \mathscr{A}(g")\mathscr{N}\mathscr{B}((g")^{-1})\right)\mathscr{B}(g') = \mathscr{S}\mathscr{B}(g')$$

and so $\mathscr{S}$ satisfies

$$\mathscr{A}(g)\mathscr{S} = \mathscr{S}\mathscr{B}(g)$$

for all $g \in \mathscr{G}$. Let $\mathscr{N}$ have $N_{jp} = 1$ and all other entries as 0. If the two representations are inequivalent then $\mathscr{S} = 0$ and by *Schur's first lemma* we get

$$\sum_g A_{ij}(g)B_{qp}(g^{-1}) = 0 \tag{3}$$

[34] $\mathscr{M}^*(g) = \mathscr{M}^{-1}(g) = \mathscr{M}(g^{-1})$ and $(\mathscr{M}^*)_{qp} = (\mathscr{M}^{-1})_{pq}$

[35] M_{ab} is the entry in the a^{th} row and b^{th} column of the representation matrices $\mathscr{M}$.

Now if $\mathscr{R}_A = \mathscr{R}_B = \mathscr{R}$ by *Schur's second lemma* we have

$$\mathscr{S} = \sum_g \mathscr{M}(g)\mathscr{N}\mathscr{M}(g^{-1}) = cI$$

again let $\mathscr{N}$ be an $(N \times N)$ having $N_{jp} = 1$ and all other entries as 0, then

$$\sum_g M_{ij}(g)M_{pq}(g^{-1}) = c\delta_{iq}$$

Now to determine c we let $i = q$ and sum over i

$$\sum_{i=1}^{N}\sum_g M_{ij}(g)M_{pi}(g^{-1}) = \sum_g M_{pj}(gg^{-1}) = \sum_g \delta_{jp} = n\delta_{jp} = c$$

thus

$$\frac{1}{n}\sum_g M_{ij}(g)M_{pq}(g^{-1}) = \frac{1}{N}\delta_{iq}\delta_{jp} \tag{4}$$

From (3) and (4) we get

$$\frac{1}{n}\sum_g A_{ij}(g)B_{pq}(g^{-1}) = \frac{1}{N_A}\delta_{AB}\delta_{iq}\delta_{jp}$$

and if the representations are unitary,

$$\frac{1}{n}\sum_g A_{ij}(g)B^*_{qp}(g) = \frac{1}{N_A}\delta_{AB}\delta_{iq}\delta_{jp}$$

□

* * *

4 Representations of finite groups

4.1 Character theory of finite groups

The *character* of an element g in a representation $\mathscr{R}$ is defined as the trace of its representation matrix

$$\chi(g) = \mathrm{Tr}\,\mathscr{M}(g)$$

Note that the character of g is not a unique function of g, because

$$\chi(g_1 g g_1^{-1}) = \mathrm{Tr}(\mathscr{M}(g_1)\mathscr{M}(g)\mathscr{M}(g_1^{-1})) = \mathrm{Tr}\,\mathscr{M}(g)$$

i.e. all group elements of a class have the same character.

Theorem 23 (First Orthogonality of Characters)**.** *Characters of irreducible representations satisfy the following orthogonality relation*

$$\frac{1}{n}\sum_g \chi_A(g)\overline{\chi}_B(g) = \delta_{AB}$$

where χ_A and χ_B stand for the characters of irreducible representations $\mathscr{R}_A$ and $\mathscr{R}_B$, and the summation runs over all g group elements.

Proof. We substitute $j = i$ and $q = p$ in equation (4)

$$\sum_g \mathscr{A}_{ii}(g)\mathscr{B}_{pp}(g^{-1}) = \frac{n}{N_A}\delta_{AB}\delta_{ip}$$

and sum over all i, p

$$\sum \chi_A(g)\chi(g^{-1}) = n\delta_{AB}$$

and if the representations are unitary then

$$\sum \chi_A(g)\chi(g^{-1}) = \sum \chi_A(g)\chi_B^*(g) = \sum \chi_A(g)\overline{\chi}_B = n\delta_{AB}$$

□

Suppose the number of classes in a group are n_C where n_i number of elements in the i^{th} class C_i with character χ_i then we define the scalar product $\{\chi_A, \chi_B\}$ as

$$\{\chi_A, \chi_B\} \equiv \frac{1}{n}\sum_g \chi_A(g)\overline{\chi}_B(g) = \frac{1}{n}\sum_{i=1}^{n_C} n_i \chi_A^{(i)}\overline{\chi}_B^{(i)} = \delta_{AB} \tag{5}$$

If there were n_R different irreducible representations such that the equation (5), where $A, B = 1, \ldots, n_R$ implies that the n_R vectors χ_A form an orthonormal set in an n_C dimensional vector space and so we must have

$$n_R \leq n_C \tag{6}$$

Consider a reducible representation $\mathscr{R}$ that is the sum of r_A irreducible representations $\mathscr{R}_A$, with characters

$$\chi = \sum_A r_A \chi_A$$

where the multiplicity of $\mathscr{R}_A$ is $r_A = \{\chi, \chi_A\}$.

Test for irreducibility Consider the scalar product

$$\{\chi, \chi\} = \sum_{A,B} r_A r_B \{\chi_A, \chi_B\} = \sum_A r_A^2$$

If the scalar product of the characters of a representation $\mathscr{R}$ is equal to 1 then it is irreducible.

We now apply these formulæto the N dimensional regular representation[36] $\mathscr{R}_{\text{reg}}$ to decompose it as follows

$$\mathscr{R}_{\text{reg}} = \sum_{A=1}^{n_R} r_A \mathscr{R}$$

where

$$n = \sum_{A=1}^{n_R} r_A N_A \tag{7}$$

with its characters expressed as

$$\chi_{\text{reg}}^{(i)} = \sum_{A=1}^{n_R} r_A \chi_A^{(i)}$$

In Section 2.3 we had seen how in the regular representation group action essentially shuffles the N objects that are being dealt with (here the objects are

[36] Recall that the representation of *all* possible permutations of n objects is the regular representation i.e. $\mathscr{R}_{\text{reg}}$ contains all irreducible representations $\mathscr{R}_A$.

vectors). Observe that besides the identity matrix all other representation matrices have all diagonal entries as 0, i.e. $\chi^{(1)}_{\text{reg}} = N(= n)$ and $\chi^{(i)}_{\text{reg}} = 0$ for $i \neq 1$. Hence the multiplicity r_A can be determined as

$$r_A = \{\chi_{\text{reg}}, \chi_A\} = \frac{1}{n}\sum_{i=1}^{n_C} n_i \chi^{(i)}_{\text{reg}} \overline{\chi}^{(i)}_A$$

as $\chi^{(i)}_{\text{reg}} = 0$ for $i \neq 1$, we take $i = 1$ and we know that $n_1 = 1$

$$\frac{1}{n}\sum_{i=1}^{n_C} n_i \chi^{(i)}_{\text{reg}} \overline{\chi}^{(i)}_A = \delta_{AB} = \frac{1}{n} n_1 \chi^{(i)}_A \overline{\chi}^{(i)}_A = \frac{1}{n} n \overline{\chi}^{(i)}_A = \overline{\chi}_A(e)$$

but the character of the unit element of a representation is the dimension of the representation

$$\chi_A = N_A$$

thus $r_A = N_A$ and so have the following result

Corollary 24. *The multiplicity of any irreducible representation in the regular representation is equal to its dimension.*

As a consequence the equation (7) can now be written as

$$n = \sum_{A=1}^{n_R} N_A^2$$

Theorem 25 (Second Orthogonality of Characters)**.** *Characters of irreducible representations satisfy the following orthogonality relation as well*

$$\frac{1}{n}\sum_{A=1}^{n_R} \chi^{(i)}_A \overline{\chi}^{(j)}_A = \frac{1}{n_i}\delta_{ij}$$

Proof. We define

$$G_i \equiv \frac{1}{n_i}\sum_{l=1}^{n_i} g_l$$

where $g_1, \ldots, g_{n_i}$ are elements of a class C_i. Observe that

$$\widetilde{G}_i = G_i$$

$\{G_i\}$ also forms a class. Also

$$G_i G_j = \sum_k c_{ijk} G_k \tag{8}$$

where the c_{ijk} are called as *class coefficients*. We also define

$$\mathscr{N}_A^{(i)} \equiv \frac{1}{n_i}\mathscr{A}(G_i) = \frac{1}{n_i}\sum_{g\in C_i}\mathscr{A}(g)$$

and

$$\mathrm{Tr}(\mathscr{N}_A^{(i)}) = \chi_A^{(i)} \tag{9}$$

then we have

$$\mathscr{A}(g)\mathscr{N}_A^{(i)} = \mathscr{N}_A^{(i)}\mathscr{A}(g)$$

where $g \in C_i$ and since $\mathscr{R}_A$ is irreducible, by *Schur's second lemma*

$$\mathscr{N}_A^{(i)} = cI$$

Now taking the trace of both sides,

$$\mathrm{Tr}\left(\frac{1}{n_i}\sum_{g\in C_i}\mathscr{A}(g)\right) = \chi_A^{(i)} = c\,\mathrm{Tr}(I) = c\chi_A^{(1)}$$

we get,

$$\mathscr{N}_A^{(i)} = \frac{\chi_A^{(i)}}{\chi_A^{(1)}}I \tag{10}$$

From equation (8)

$$\mathscr{N}_A^{(i)}\mathscr{N}_A^{(j)} = \sum_k c_{ijk}\mathscr{N}_A^{(k)}$$

and from equation (10)

$$\chi_A^{(i)}\chi_A^{(j)} = \chi_A^{(1)}\sum_k c_{ijk}\chi_A^{(k)}$$

also we know that

$$\chi_{reg}^{(i)} = \sum_{A=1}^{n_R} r_A\chi_A^{(i)} = \sum_{A=1}^{n_R} d_A\chi_A^{(i)} = \sum_{A=1}^{n_R}\chi_A^{(1)}\chi_A^{(i)}$$

so

$$\sum_{A=1}^{n_R}\chi_A^{(i)}\chi_A^{(j)} = \sum_{A=1}^{n_R}\chi_A^{(1)}\sum_k c_{ijk}\chi_A^{(k)} = \sum_k c_{ijk}\sum_{A=1}^{n_R}\chi_A^{(1)}\chi_A^{(i)} = \sum_k c_{ijk}\chi_{reg}^{(k)}$$

however $\chi_{reg}^{(k)}$ vanishes for all $k \neq 1$ and so

$$\sum_{A=1}^{n_R}\chi_A^{(i)}\chi_A^{(j)} = c_{ij1}n \tag{11}$$

Now in order to determine c_{ij1} we substitute $k = 1$ in equation (8)

$$G_i G_j = c_{ij1} G_1 = c_{ij1}$$

and G_1 is the unit element which can only be obtained if C_j contains the inverse of at least one element of the class C_i. However this is only possible if every element in C_i has a corresponding inverse in C_j i.e. ($n_i = n_j$ and $j = \bar{i}$).

$$G_i G_j = \frac{1}{n_i^2} \sum_{l=1}^{n_i} g_l \sum_{l=1}^{n_i} \overline{g}_l = \frac{1}{n_i} e + \ldots$$

and

$$\chi_A^{(\bar{i})} = \overline{\chi}_A^{(i)}$$

Thus combining the above equations with equation (11) we get

$$\frac{1}{n} \sum_{A=1}^{n_R} \chi_A^{(i)} \overline{\chi}_A^{(j)} = \frac{1}{n_i} \delta_{ij} \tag{12}$$

□

If there were n_R different irreducible representations such that the equation (12), where $i, j = 1, \ldots, n_C$ implies that the n_C vectors $\chi_A^{(i)}$ form an orthonormal set in an n_R dimensional vector space and so we must have

$$n_C \leq n_R$$

However from (6) we have

$$n_C = n_R$$

Corollary 26. *The number of irreducible representations of a finite group is equal to its number of classes.*

4.2 Character Table

Hence we can deduce a groups representations once we know its classes. The information is usually displayed in a *character table*, which lists the values of the characters for the different representations.

4.2.1 $\mathcal{Z}_n$ character table

Since $\mathcal{Z}_n$ is *abelian*, it has n one dimensional classes C_i, $i = 1,\ldots,n$ (Section 1.2.11). Hence all its elements can be represented by (1×1) matrices i.e. complex numbers. As the presentation

$$\mathcal{Z}_n = \langle a \,|\, a^n = e \rangle$$

requires a to be an n^{th} root of unity ω_n, we have

$$a = 1,\, e^{2i\pi i/n},\ldots,\, e^{(n-1)2\pi i/n}$$

and we assign $a_k = e^{k2\pi i/n}$. Now suppose the first irreducible representation matrix say $\mathscr{A} = 1$, similarly $\mathscr{B} = x$ and so on up till x^{n-1}, giving us the n representation matrices with characters $\chi_0,\ldots,\chi_{n-1}$, hence we get the character table

k	0	1	2	$\ldots$	$n-1$
$\lvert C_i \rvert$	1	1	1	$\ldots$	1
χ_0	1	1	1	$\ldots$	1
χ_1	1	ω_n	ω_n^2	$\ldots$	ω_n^{n-1}
χ_2	1	ω_n^2	ω_n^4	$\ldots$	$\omega_n^{2(n-1)}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$
χ_{n-1}	1	ω_n^{n-1}	$\omega_n^{2(n-1)}$	$\ldots$	$\omega_n^{(n-1)(n-1)}$

* * *

Picture Acknowledgements

- Page 6: Figure [1]*Group Theory and Its Applications in Physics*[1]
- Page 20: Figure [3]*Group Theory and Its Applications in Physics*[1]
- Page 21: Figure [5]*Group Theory and Its Applications in Physics*[1]

Bibliography

[1] Teturo Inui, Yukito Tanabe, and Yositaka Onodera. *Group Theory and Its Applications in Physics*. Springer, 1990.

[2] Pierre Ramond. *Group Theory: A Physicist's Survey*. Cambridge University Press, 2010.

I would also like to thank OJ & KK for proofreading this report.