1 Why Should We Study Group Theory?

Group theory can be developed, and was developed, as an abstract mathematical topic. However, we are not mathematicians. We plan to use group theory only as much as is needed for physics purpose. For this, we focus more on physics aspects than on mathematical rigour. All complicated proofs have been carefully avoided, but you should consult the reference books if you are interested.

Almost every time, we have to use some symmetry property of the system under study to get more information (like the equations of motion, or the energy eigenfunctions) about it. For example, if the potential in the Schrödinger equation is symmetric under the exchange $\mathbf{x} \to -\mathbf{x}$ (this is known as a parity transformation), even without solving, we can say that the wavefunctions are bound to have a definite parity. Group theory is nothing but a mathematical way to study such symmetries. The symmetry can be discrete (*e.g.*, reflection about some axis) or continuous (*e.g.*, rotation). Thus, we need to study both discrete and continuous groups. The former is used more in solid state physics, particularly in crystallographic studies, while the latter is used exhaustively in quantum mechanics, quantum field theory, and nuclear and particle physics.

2 What is a Group?

A *group* G is a set of discrete elements $a, b, \cdots x$ alongwith a group operator [1], which we will denote by $\odot$, with the following properties:

- *Closure*: For any two elements a, b in G, $a \odot b$ must also be in G. We will try to avoid the mathematical symbols as far as practicable, but let me tell you that in some texts this is written as $\forall a, b \in G, a \odot b \in G$. The symbol $\forall$ is a shorthand for "for all". Another commonly used symbol is $\exists$: $\exists a \in G$ means "there exists an a in G such that".

- *Associativity*: For any three elements a, b, c in G,

$$a \odot (b \odot c) = (a \odot b) \odot c, \tag{1}$$

  i.e., the order of the operation is not important. Note that the positions of a, b, and c are the same, $a \odot (b \odot c)$ need not be the same as, say, $b \odot (a \odot c)$.

- *Identity*: The set must contain an identity element e for which $a \odot e = e \odot a = a$.

- *Inverse*: For every a in G, there must be an element $b \equiv a^{-1}$ in G so that $b \odot a = a \odot b = e$ (we do not distinguish between left and right inverses). The inverse of any element a is unique; prove it [2].

These are essential properties of a group. Furthermore, if $a \odot b = b \odot a$, the group is said to be *abelian*. If not, the group is *non-abelian*. Note that no two elements of a group are

[1] In most of the texts this is called *group multiplication* or simply *multiplication* operator. Let me warn you that the operator can very well be something completely different from ordinary or matrix multiplication. For example, it can be addition for the group of all integers.

[2] Use *reductio ad absurdum*. Assume that there are two inverses of an element and show that this leads to a contradiction.

identical. If the number of group elements (this is also called the *order* of the group) is finite, it is a *finite group*; otherwise it is an *infinite group*. Elements of a finite group are necessarily discrete (finite number of elements between any two elements). An infinite group may have discrete or continuous elements.

Now some examples:

- The additive group of all integers. It is an abelian infinite group. The group operation is addition, the identity is 0, and the inverse of a is just $-a$. Note that the set of all positive integers is not a group; there is no identity or inverse.
- The multiplicative group of all real numbers excluding zero (why?).
- Z_n, the multiplicative group of n-th roots of unity (this is also called the cyclic group of order n). For example, $Z_2 = \{1, -1\}$, $Z_3 = \{1, \omega, \omega^2\}$ where $\omega = 1^{1/3}$; $Z_4 = \{1, i, -1, -i\}$. The operation is multiplication and the identity is 1 (what is the inverse?).
- The n-object permutation group S_n. Consider a 3-element permutation group $S_3 = \{a, b, c\}$. There are six elements: P_0, which is the identity and does not change the position of the elements; P_{12}, which interchanges positions 1 and 2, *i.e.*, $P_{12} \to (b, a, c)$. Similarly, there are P_{13} and P_{23}. Finally, there are P_{123} and P_{132}, with

$$P_{123}(a, b, c) \to (c, a, b)\,, \quad P_{132}(a, b, c) \to (b, c, a), \tag{2}$$

  i.e., P_{123} takes element of position 1 to position 2, that of position 2 to position 3 and that of position 3 to position 1. Obviously, $P_{123} = P_{231} = P_{312}$, and similarly for P_{132}. There are texts that use some other definitions of the permutation operators, but that is just like renaming the elements.
- C_{4v}, the symmetry group of a square. Consider a square in the x-y plane with corners at (a, a), $(a, -a)$, $(-a, -a)$, and $(-a, a)$. The symmetry operations are rotations about the z axis by angles $\pi/2$, π and $3\pi/2$ (generally, they are taken to be anticlockwise, but one can take clockwise rotations too), reflections about x and y axes, and about the diagonals.
- $U(n)$, the group of all $n \times n$ unitary matrices. Thus, the elements of $U(1)$ are pure phases like $\exp(i\theta)$. It is the group of phase transformations. Apart from $U(1)$, all $U(n)$s are non-abelian. When we say that an individual phase in the wave function does not have any physical significance, we mean that the Lagrangian is so constructed that it is invariant under a $U(1)$ transformation $\psi \to e^{i\theta}\psi$.
- $SU(n)$, the group of all $n \times n$ unitary matrices with determinant unity (also called unitary unimodular matrices). This is the most important group in particle physics. All SU groups are non-abelian, of which the simplest is $SU(2)$. The simplest member of $SU(2)$ is the two-dimensional rotation matrix $\begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}$, characterised by different values of θ.
- $O(n)$, the group of all $n \times n$ orthogonal matrices. It is non-abelian for $n \geq 2$.
- $SO(n)$, the group of all $n \times n$ orthogonal matrices with determinant unity. Thus, $SO(2)$ and $SO(3)$ are the familiar rotation groups in two and three dimensions respectively. The S in $SU(n)$ and $SO(n)$ stands for *special*, *viz.*, the unimodularity property.

The first group is infinite but *discrete*, *i.e.*, there are only a finite number of group elements between any two elements of the group. The second group is infinite and continuous, since there are infinite number of reals between any two real numbers, however close they might be. Z_n and S_n are obviously discrete, since they are finite. The last four groups are infinite and *continuous*, which means that there are an infinite number of group elements between two given elements of the group. We will be interested in only those continuous groups whose elements can be parametrised by a finite number of parameters. Later, we will see that this number is equal to the number of generators [3] of the group.

Q. Show that the number of independent elements of an $N \times N$ unitary matrix is N^2, and that of an $N \times N$ unimodular matrix is $N^2 - 1$. [Hint: $U^\dagger U = 1$, so det U det $U^\dagger = 1$, or $|\det U|^2 = 1$, so that the determinant must have modulus unity and a form like $\exp(i\theta)$.]
Q. Show that the determinant of a 2×2 orthogonal matrix must be either $+1$ or -1. [*Hint: Write the matrix as* $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *and construct the constraint equations. Show that this leads to* $(ad-bc)^2 = 1$.]
Q. Check whether the following are groups: (i) All integers except zero for multiplication; (ii) All 2×2 orthogonal matrices with determinant -1; (iii) All purely imaginary numbers (excluding zero) for multiplication, and the same (including zero) for addition.
Q. Check that the matrix $\begin{pmatrix} e^{i\alpha}\cos\theta & e^{i\beta}\sin\theta \\ -e^{-i\beta}\sin\theta & e^{-i\alpha}\cos\theta \end{pmatrix}$ is a member of $SU(2)$. Note that α, β, and θ are all real and independent. Later you will see that an $SU(2)$ member has at most 3 independent elements, and an $SU(N)$ member has $N^2 - 1$.

3 Discrete and Finite Groups

3.1 Multiplication Table

A multiplication table is nothing but a compact way to show the results of all possible compositions among the group elements. Obviously, this makes sense only for finite groups. For example, the multiplication tables for Z_4 and S_3 are, respectively,

	1	i	−1	−i
1	1	i	−1	−i
i	i	−1	−i	1
−1	−1	−i	1	i
−i	−i	1	i	−1

	P_0	P_{12}	P_{13}	P_{23}	P_{123}	P_{132}
P_0	P_0	P_{12}	P_{13}	P_{23}	P_{123}	P_{132}
P_{12}	P_{12}	P_0	P_{132}	P_{123}	P_{23}	P_{13}
P_{13}	P_{13}	P_{123}	P_0	P_{132}	P_{12}	P_{23}
P_{23}	P_{23}	P_{132}	P_{123}	P_0	P_{13}	P_{12}
P_{123}	P_{123}	P_{13}	P_{23}	P_{12}	P_{132}	P_0
P_{132}	P_{132}	P_{23}	P_{12}	P_{13}	P_0	P_{123}

[3]You do not yet know what a group generator is, so wait, or directly go to the Lie group section.

One should note a few things. First, Z_4 is obviously abelian, and hence the multiplication table is symmetric, but S_3 is non-abelian (*e.g.*, $P_{13}P_{23} \neq P_{23}P_{13}$). For both of them, all elements occur *only once* in each row or column. This is a general property of the multiplication table and is easy to prove. Suppose two elements $a \odot b$ and $a \odot c$ are same. Multiply by a^{-1}, so $b = c$, contrary to our assumption of all elements being distinct. However, number of elements in each row or column is equal to the order of the group, so all elements must occur once and only once.

Second, $(1, -1)$ or Z_2 is a subgroup (a subset of a group that itself behaves like a group under the same operation) of Z_4, and (P_0, P_{123}, P_{132}) is a subgroup of S_3. In fact, there are three more subgroups of S_3, find them. We of course exclude two trivial subgroups that every group has, the identity element and the entire group itself. Can you show that the identity of the bigger group must be the identity of the subgroup too?

3.2 Isomorphism and Homomorphism

Consider the symmetry group C_3 of an equilateral triangle, with six elements (identity, three reflections about the medians, and rotations by $2\pi/3$ and $4\pi/3$). The multiplication table is identical with S_3. Only this (not just the number of elements) shows that the groups behave in an identical way. This is known as *isomorphism*: we say that these two groups are isomorphic to one another. Thus, isomorphism means a one-to-one correspondence between the elements of two groups so that if $a, b, c \in G$ and $p, q, r \in H$, and a, b, c are isomorphic to p, q, r respectively, then $a \odot b = c$ implies $p \odot q = r$, for all a, b, c and p, q, r. The operations in G and H may be completely different. Try to convince yourself that the identity of one group must be mapped on to the identity of the second group [4].

Thus, S_3 is isomorphic to C_3. If we consider only rotational symmetries, then the three-member subgroup of C_3 is isomorphic to Z_3 (and also to the (P_0, P_{123}, P_{132}) subgroup of S_3, which, because of isomorphism, we will call Z_3 from now on if there is no chance for any confusion). In fact, this is a general property: the rotational symmetry group of any symmetric n-sided polygon, having $2\pi/n$ rotation as a symmetry operation, is isomorphic to Z_n. Check this for Z_4. This cannot be a coincidence; what is the physical reason behind this?

If the mapping is not one-to-one but many-to-one, the groups are said to be homomorphic to one another. Obviously, in a many-to-one mapping, some information is lost. All groups are homomorphic to the group containing the identity; but that is a very bad mapping, since no information about the group structure is retained. A better homomorphism occurs between Z_2 and Z_4, where $(1, -1)$ of Z_4 is mapped to 1 of Z_2, and $(i, -i)$ of Z_4 is mapped to -1 of Z_2. Isomorphism is only a special case of homomorphism, but in general, the two groups which are homomorphic to one another should be of different order, and the ratio of their orders n/m should be an integer k. In this case, set of k elements of G is mapped to one element of H. The set containing identity in G must be mapped to the identity of H: prove this. Also prove that this set itself must form a group.

[4] Show that if $e_G \mapsto p \neq e_H$, this leads to a contradiction.

3.3 Conjugacy Classes

Consider a group G with elements $\{a, b, c, d, \cdots\}$. If $aba^{-1} = c$, (from now on we drop the $\odot$ symbol for group operation), then b and c are said to be conjugate elements. If b is conjugate to both c and d, then c and d are conjugate to each other. The proof goes like this: Suppose $aba^{-1} = c$ and $hbh^{-1} = d$, then $b = a^{-1}ca$ and hence $ha^{-1}cah^{-1} = d$. But ah^{-1} is a member of the group, and hence its inverse, ha^{-1}, too (why the inverse of ah^{-1} is not $a^{-1}h$?). So c and d are conjugate to each other.

It is trivial to show that the identity element in any group is conjugate only to itself, and for an abelian group all members are conjugate to themselves only.

Now, any discrete group can be separated into sets of elements (need not having the same number of elements) where all members of a set are conjugate to each other but no member of any set is conjugate to another member of a different set. In that case, the sets are called *conjugacy classes* or simply *classes*.

Let us take C_{4v}, the symmetry group of a square. The symmetry operations are 1 (identity), $r_{\pi/2}, r_\pi, r_{3\pi/2}$ (rotations, may be clockwise or anticlockwise), R_x, R_y (reflections about x and y axes, passing through the centre of the square), and R_{NE} and R_{SE}, the reflections about the NE and the SE diagonal. [In some texts you will see different notations, but these are equally good, if not more transparent.]

These eight elements form a group; that can be checked from the multiplication table. The group is non-abelian. However, the first four members form an abelian group isomorphic to Z_4. The eight elements can be divided into five classes: (1), (r_π), $(r_{\pi/2}, r_{3\pi/2})$, (R_x, R_y), (R_{NE}, R_{SE}). It is left as an exercise to check the class structure.

What is the physical significance of classes? In other words, can we guess which elements should be in a particular class? The answer is yes: note that the conjugacy operation is nothing but a similarity transformation performed with the group elements. This will be more obvious in the next section when we show how to represent the abstract group elements with matrices, in particular unitary matrices.

Identity must be a class by itself. $r_{\pi/2}$ and $r_{3\pi/2}$ belong to the same class *because* there is an element of the group which relates rotation by $\pi/2$ with rotation by $3\pi/2$: just the reflection about the x or y axis, which makes a clockwise rotation anticlockwise and vice versa. Similarly, R_x and R_y belong to the same class since there is an operation that relates them: rotation by $\pi/2$. However, R_x and R_{NE} cannot belong to the same class, since there is no symmetry operation of $r_{\pi/4}$.

4 Representation of a Group

The permutation group discussed above is an example of a *transformation group* on a physical system. In quantum mechanics, a transformation of the system is associated with a unitary operator in the Hilbert space (time reversal is the only example of antiunitary transformation that is relevant to us). Thus, a transformation group of a quantum mechanical system is associated with a mapping of the group to a set of unitary operators [5]. Thus, for each a in G there is a unitary operator $D(a)$, with identity $\mathbf{1}$ being the operator corresponding to

[5] If this mapping is one-to-one, the *representation* is called *faithful*. We will deal with faithful representations only.

the identity element of the group: $D(e) = \mathbf{1}$. This mapping must also preserve the group operation, *i.e.*,

$$D(a)D(b) = D(a \odot b) \tag{3}$$

for all a and b in G. A mapping which satisfies eq. (3) is called a *representation* of the group G. In fact, a representation can involve nonunitary operators so long as they satisfy eq. (3).

For example, the mapping

$$D(n) = \exp(in\theta) \tag{4}$$

is a representation of the additive group of integers, since

$$\exp(im\theta)\exp(in\theta) = \exp(i(n+m)\theta). \tag{5}$$

Also,

$$D(e) = 1\,, \quad D(a) = e^{2\pi i/3}\,, \quad D(b) = e^{4\pi i/3} \tag{6}$$

is a 1×1 representation of Z_3.

Check that the following mapping is a representation of the 3-element permutation group S_3:

$$\begin{aligned} D(1) &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}; \ D(12) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}; \ D(13) = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}; \\ D(23) &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}; \ D(123) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}; \ D(321) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}. \end{aligned} \tag{7}$$

Particularly, check the multiplication table.

In short, a representation is a specific realisation of the group operation law by finite or infinite dimensional matrices. For abelian groups, their representative matrices commute.

Consider a n-dimensional Hilbert space. Thus, there are n orthonormal basis vectors. Let $|i\rangle$ be a normalised basis vector. We define the ij-th element of any representation matrix $D(a)$ as

$$[D(a)]_{ij} = \langle i|D(a)|j\rangle\,, \tag{8}$$

so that

$$D(a)|j\rangle = \sum_i |i\rangle\langle i|D(a)|j\rangle = \sum_i [D(a)]_{ij}|j\rangle\,. \tag{9}$$

From now on, we will freely translate from one language (representations as abstract linear operators) to the other (representations as matrices). Anyway, it is clear that the dimension of the representation matrices is the same as that of the Hilbert space.

Thus, the elements of a group can be represented by matrices. The dimension of the matrices has nothing to do with the order of the group. But the matrices should be all different, and there should be a one-to-one mapping between the group elements and the matrices; that's what we call a faithful representation. Obviously, the representative matrices are square, because matrix multiplication is defined both for $D(a)D(b)$ and $D(b)D(a)$. The representation of identity must be the unit matrix, and if $T(a)$ is the representation of a, then $T^{-1}(a) = T(a^{-1})$ is the representation of a^{-1}. The matrices must be non-singular; the inverse exists.

However, the matrices need not be unitary. But in quantum mechanics we will be concerned with unitary operators, and so it is better to show now that any representation of a group is *equivalent* to a representation by unitary matrices. Two representations D_1 and D_2 are *equivalent* if they are related by a *similarity transformation*

$$D_2(a) = SD_1(a)S^{-1} \tag{10}$$

with a fixed operator S for all a in the group G.

Suppose $T(a)$ is the representation of a group G. $T(a)$s need not be unitary. Define a hermitian matrix

$$H = \sum_{a\in G} T(a)T^\dagger(a). \tag{11}$$

This matrix, being hermitian, can be diagonalised by a unitary transformation. Let $U^\dagger HU = H_d$. H_d is a real diagonal matrix whose elements are the eigenvalues of H. Using the form of H,

$$H_d = U^\dagger \sum_{a\in G} T(a)T^\dagger(a)U = \sum_{a\in G} \left(U^\dagger T(a)U\right)\left(U^\dagger T^\dagger(a)U\right) = \sum_{a\in G} \mathcal{T}(a)\mathcal{T}^\dagger(a) \tag{12}$$

where $\mathcal{T}(a)$ is also a representation (remember $U^\dagger = U^{-1}$). Take the k-th diagonal element of H_d:

$$[H_d]_{kk} \equiv d_k = \sum_{a\in G}\sum_j \mathcal{T}_{kj}(a)\mathcal{T}^\dagger_{jk}(a) = \sum_{a\in G}\sum_j |\mathcal{T}_{kj}(a)|^2. \tag{13}$$

Thus $d_k \geq 0$. The case $d_k = 0$ can be ruled out since in that case a particular row in all the representative matrices is zero and the determinants are zero, so all matrices are singular. So d_k is positive for all k, and we can define a diagonal matrix $H_d^{1/2}$ whose k-th element is $\sqrt{d_k}$. Construct the matrix $V = UH_d^{1/2}$ and the representation $\Gamma(a) = V^{-1}T(a)V$. We now show that all Γ matrices are unitary, completing the proof.

We have $\Gamma(a) = V^{-1}T(a)V = H_d^{-1/2}U^{-1}T(a)UH_d^{1/2} = H_d^{-1/2}\mathcal{T}(a)H_d^{1/2}$, and

$$\begin{aligned}
\Gamma(a)\Gamma^\dagger(a) &= \left[H_d^{-1/2}\mathcal{T}(a)H_d^{1/2}\right]\left[H_d^{1/2}\mathcal{T}^\dagger(a)H_d^{-1/2}\right] \\
&= H_d^{-1/2}\mathcal{T}(a)H_d\mathcal{T}^\dagger(a)H_d^{-1/2} \\
&= H_d^{-1/2}\mathcal{T}(a)\sum_{b\in G}\mathcal{T}(b)\mathcal{T}^\dagger(b)\mathcal{T}^\dagger(a)H_d^{-1/2} \\
&= H_d^{-1/2}\sum_{b\in G}\mathcal{T}(ab)\mathcal{T}^\dagger(ab)H_d^{-1/2} \\
&= H_d^{-1/2}H_dH_d^{-1/2} = \mathbf{1}.
\end{aligned} \tag{14}$$

Here we have used the rearrangement theorem: as long as we sum over all the elements of the group, how we denote them is immaterial.

This theorem depends on the convergence of a number of sums. For an infinite group, this is not so straightforward. However, for Lie groups (to be discussed in the next section) this theorem holds.

4.1 Reducible and Irreducible Representations

A representation D is *reducible* if it is equivalent to a representation D' with *block-diagonal* form (or itself block-diagonal):

$$D'(x) = SD(x)S^{-1} = \begin{pmatrix} D_1'(x) & 0 \\ 0 & D_2'(x) \end{pmatrix}. \tag{15}$$

The vector space on which D' acts breaks up into two orthogonal subspaces, each of which is mapped into itself by all the operators $D'(x)$. The representation D' is said to be the *direct sum* of D'_1 and D'_2:

$$D' = D'_1 \oplus D'_2. \tag{16}$$

A representation is *irreducible* if it cannot be put into block-diagonal form by a similarity transformation. We will use the shorthand IR for irreducible representations.

One can add up several IRs to construct a bigger reducible representation. There is another way to construct a bigger representation out of several IRs. Condider two IRs D_1 and D_2, where D_1 is m-dimensional, acting on a vector space $|i\rangle$ where $i = 1, \cdots m$ and D_2 is n-dimensional, acting on another vector space $|p\rangle$ where $p = 1, \cdots n$. We can make a mn dimensional space by taking basis vectors labeled by $|i\rangle$ and $|p\rangle$ in an ordered pair $|i, p\rangle$, which can have mn possible values. The representation $D_1 \otimes D_2$ is called a *tensor product representation*, which can be obtained by direct multiplication of two smaller representations:

$$\langle i, p|D_1(g) \otimes D_2(g)|j, q\rangle \equiv \langle i|D_1(g)|j\rangle\langle p|D_2(g)|q\rangle\,. \tag{17}$$

Q. Show that the 3-dimensional representation of Z_3, given by $D(1)$, $D(123)$ and $D(321)$ of (7), is completely reducible with a similarity transformation by

$$S = \frac{1}{3}\begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega^2 & \omega \\ 1 & \omega & \omega^2 \end{pmatrix} \tag{18}$$

where $\omega = \exp(2\pi i/3)$.

4.2 Schur's Lemma and the Great Orthogonality Theorem

Before closing the section on discrete groups, we will prove a very important theorem on the orthogonality of different representations of a group. This theorem tells you that if you have two different representations of a group which are both irreducible but inequivalent to each other, then the 'dot product' of these two representations is zero. What is a 'dot product'? Each of these representations form a g-dimensional vector space, where g is the order of the group. The 'dot product' is something like taking a matrix from one space, taking its corresponding matrix from the other space, taking any two elements of these matrices, and then sum over all elements of the group. A more mathematical definition will soon follow, but before that we need to prove two lemmas by Schur.

Schur's Lemma 1. If a matrix P commutes with all representative matrices of an irreducible representation, then $P = c\mathbf{1}$, a multiple of the unit matrix.

Proof. Given, $PT(a) = T(a)P$ for all $a \in G$, where we take $T(a)$s to be a unitary representation without loss of generality. Suppose the dimension of $T(a)$ is $n \times n$; evidently, that should be the dimension of P. $T(a)$s possess a complete set of n eigenvectors. So does P, since $[P, T(a)] = 0$. Let ψ_j be some eigenvector of P with eigenvalue c_j: $P\psi_j = c_j\psi_j$. Then $PT(a)\psi_j = c_jT(a)\psi_j$. So both $\psi_j = T(1)\psi_j$ and $T(a)\psi_j$, two independent eigenvectors, have same eigenvalue. How many such degenerate states exist? Obviously n, since if the number of such degenerate states be $m < n$, we have an m-dimensional invariant subspace in the whole n-dimensional vector space, so the original space is not irreducible. Thus, all c_js are equal, and $P = c\mathbf{1}$.

Schur's Lemma 2. Suppose you have two irreducible representations $T^i(a)$ and $T^j(a)$ of dimension l_i and l_j respectively. If a matrix M satisfies $T^i(a)M = MT^j(a)$ for all $a \in G$, then either (i) $M = 0$, a null matrix, or (ii) $det\ M \neq 0$, in which case T^i and T^j are equivalent representations.

Proof. The dimension of M is $l_i \times l_j$. If $l_i = l_j$, M is a square matrix. If its determinant is not zero, T^i and T^j are obviously equivalent representations.

First, we show, with the help of the first lemma, that $M^\dagger M$ is a multiple of the unit matrix. Take the hermitian conjugate of both sides of the defining equation:

$$\begin{aligned} M^\dagger {T^i}^\dagger(a) = {T^j}^\dagger(a) M^\dagger \quad &\Rightarrow \quad M^\dagger T^i(a^{-1}) = T^j(a^{-1})M^\dagger, \\ M^\dagger T^i(a^{-1})M = T^j(a^{-1})M^\dagger M \quad &\Rightarrow \quad M^\dagger M T^j(a^{-1}) = T^j(a^{-1})M^\dagger M. \end{aligned} \tag{19}$$

This is true for all the elements of G, so $M^\dagger M = c\mathbf{1}$. If M is a square matrix and $c \neq 0$, then the representations are equivalent. If $c = 0$, then

$$(M^\dagger M)_{ii} = \sum_k |M_{ki}|^2 = 0. \tag{20}$$

This is true only if $M_{ki} = 0$ for all k. But i is arbitrary and can run from 1 to n. So $M = 0$.

Now suppose $l_i \neq l_j$. Let $l_i < l_j$. Add $l_j - l_i$ rows of zero to M to get a square matrix $\mathcal{M}$, whose determinant is obviously zero. But $\mathcal{M}^\dagger \mathcal{M} = M^\dagger M$, and since the first one is zero, so is the second one. Again take the (i,i)-th element of $M^\dagger M$ to get $M = 0$.

The Great Orthogonality Theorem says that if T^i and T^j are two inequivalent irreducible representations of a group G, then

$$\sum_{a \in G} T^i_{km}(a) T^j_{ns}(a^{-1}) = \frac{g}{l_i} \delta_{ij} \delta_{ks} \delta_{mn}, \tag{21}$$

where l_i and l_j are the dimensions of the representations T^i and T^j respectively, and g is the order of the group.

Proof. Consider a matrix M constructed as

$$M = \sum_{a \in G} T^i(a) X T^j(a^{-1}) \tag{22}$$

where X is an arbitrary matrix, independent of the group elements. Note that if the representations are unitary then $T^j(a^{-1}) = T^{j\dagger}(a)$. Let T^i and T^j be two inequivalent irreducible representations of dimensions l_i and l_j respectively. Multiplying both sides of eq. (22) by $T^i(b)$, where $b \in G$, we get

$$\begin{aligned} T^i(b)M &= \sum_{a \in G} T^i(ba) X T^j(a^{-1}) = \sum_{c \in G} T^i(c) X T^j(c^{-1}b) \\ &= \sum_{c \in G} T^i(c) X T^j(c^{-1}) T^j(b) = M T^j(b), \end{aligned} \tag{23}$$

and so, by the second lemma, $M = 0$. But this is true for any X; let $X_{pq} = \delta_{pm}\delta_{qn}$, *i.e.*, only the mn-th element is 1 and rest 0. Take the ks-th element of M:

$$M_{ks} = \sum_{a \in G} \sum_{p,q} T^i_{kp}(a) X_{pq} T^j_{qs}(a^{-1}) = 0. \tag{24}$$

But this reduces to

$$\sum_{a\in G} T^i_{km}(a)T^j_{ns}(a^{-1}) = 0. \tag{25}$$

Next, construct a matrix $N = \sum_{a\in G} T^i(a)XT^i(a^{-1})$. By an argument similar to eq. (23), we get $NT^i(a) = T^i(a)N$ for all $a \in G$, so N is a multiple of the unit matrix: $N = c\mathbf{1}$. Taking the ks-th element of N, and the same form of X, we find

$$\sum_{a\in G} = T^i_{km}(a)T^i_{ns}(a^{-1}) = c\delta_{ks}. \tag{26}$$

To get c, take the trace of N, which is a multiple of an $l_i \times l_i$ dimensional unit matrix:

$$\begin{aligned} Tr(N) = cl_i &= \sum_{a\in G}\sum_{k,p,q} T^i_{kp}(a)X_{pq}T^i_{qk}(a^{-1}) \\ &= \sum_{p,q} X_{pq}\sum_{a\in G}\sum_{k} T^i_{qk}(a^{-1})T^i_{kp}(a) \\ &= \sum_{p,q} X_{pq}\sum_{a\in G} T^i_{qp}(1) = g\sum_{p,q} X_{pq}\delta_{pq} = g\ Tr(X), \end{aligned} \tag{27}$$

so that $c = g\ Tr(X)/l_i$. But $Tr(X) = 0$ if $m \neq n$, or $Tr(X) = \delta_{mn}$. Combining this with eq. (25), we get

$$\sum_{a\in G} T^i_{km}(a)T^j_{ns}(a^{-1}) = \frac{g}{l_i}\delta_{ij}\delta_{ks}\delta_{mn}. \tag{28}$$