Lecture Notes on Representation Theory for Quantum Information (QMATH Masterclass 2025, Copenhagen)

Antonio Anna Mele[1, *]

[1] *Dahlem Center for Complex Quantum Systems, Freie Universität Berlin, 14195 Berlin, Germany*

(Dated: August 23, 2025)

These notes provide an introduction to the basic tools of representation theory, aimed at preparing readers for their application in quantum information science. We begin with the definition of groups, develop the theory of group representations, explore character theory, and present the fundamental Schur–Weyl duality together with its complete proof. Applications in quantum information theory — including examples from quantum learning — are discussed throughout. The material is based on preparatory lectures for the QMATH Masterclass on Representation Theory in Quantum Information Science, held in Copenhagen on 15 August 2025. Further details about the event can be found at: qmath.ku.dk.

CONTENTS

* a.mele@fu-berlin.de

I. INTRODUCTION

This crash course introduces the essential tools of representation theory, with a focus on preparing you for applications in quantum information science. At its core, representation theory studies *groups*—mathematical structures that capture *symmetries*—through the lens of linear algebra [1, 2].

Why should we care about representation theory in quantum information? Much of quantum information theory and quantum computing is built on linear algebra—and representation theory can be seen as a powerful extension of linear algebra. It provides a systematic framework to uncover and exploit symmetries, turning seemingly complicated problems into ones with clear structure and elegant solutions. Once you learn to use it, it feels like a secret weapon.

In quantum information, representation theory lies at the heart of many essential ideas. It underpins fundamental subroutines in quantum algorithms, such as the quantum Fourier transform [3] and quantum Schur sampling [4, 5] for spectrum estimation [6]. It provides the mathematical machinery to understand and classify entanglement [7], and it is crucial for the efficient diagonalization of many-body Hamiltonians, where exploiting symmetries can drastically reduce complexity. Even in standard quantum mechanics, topics like determining the spectrum of the hydrogen atom or performing Clebsch–Gordan decompositions to add angular momenta are direct applications of representation theory [8].

Beyond quantum information, its reach extends throughout physics. In solid-state physics it determines crystal band structures [9], in quantum chemistry it governs the analysis of molecular vibrations and wavefunctions [10], in particle physics it forms the mathematical backbone of the Standard Model [11], and even in classical mechanics it provides systematic ways to exploit symmetries for solving problems more efficiently.

We now begin by reviewing the basic language of group theory, which forms the foundation for the entire subject.

II. GROUP THEORY

We begin with the definition of a group.

Definition II.1 (Group)**.** A *group* is a set G equipped with a binary operation $\circ : G \times G \to G$ satisfying:

1. **Closure:** For all $a, b \in G$, we have $a \circ b \in G$.
2. **Associativity:** For all $a, b, c \in G$, $(a \circ b) \circ c = a \circ (b \circ c)$.
3. **Identity:** There exists an element $e \in G$ such that $e \circ g = g \circ e = g$ for all $g \in G$.
4. **Inverses:** For every $g \in G$, there exists $g^{-1} \in G$ such that $g \circ g^{-1} = g^{-1} \circ g = e$.

For brevity, we write gh in place of $g \circ h$.

The identity element of a group is unique, as is the inverse of each element. Moreover, for any $g \in G$, the sets $\{h \mid h \in G\}$ and $\{gh \mid h \in G\}$ coincide. In particular, for any function $f : G \to \mathbb{C}$ we have

$$\sum_{h \in G} f(h) = \sum_{h \in G} f(gh), \tag{1}$$

a property that will be used repeatedly in later proofs.

Definition II.2 (Basic group-theory definitions)**.** Let G be a group.

- **Order of a group:** The *order* of G, denoted $|G|$, is the number of elements in G. If G has infinitely many elements (e.g. $(\mathbb{Z}, +)$), we say that G has infinite order.
- **Order of an element:** The *order* of an element $g \in G$ is the smallest positive integer k such that $g^k = e$. If no such k exists, g is said to have infinite order.
- **Subgroup:** A subset $H \subseteq G$ is a *subgroup* if it is itself a group under the operation of G. We write $H \leq G$. [1]
- **Generators:** A subset $S \subseteq G$ is a set of *generators* if every element of G can be written as a finite product of elements of S and their inverses. We write $G = \langle S \rangle$. If G can be generated by a single element g, we write $\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}$ and call G *cyclic*. The cardinality $|\langle g \rangle|$ equals the order of g.

---

[1] The identity of G is also the identity of H, and for every $h \in H$, the inverse h^{-1} in G lies in H.

- **Conjugacy and conjugacy classes:** Two elements $g, k \in G$ are *conjugate* if there exists $h \in G$ such that $k = hgh^{-1}$. The *conjugacy class* of g is

$$C(g) \coloneqq \{hgh^{-1} \mid h \in G\}. \tag{2}$$

Conjugacy is an equivalence relation on G: it is reflexive ($g = ege^{-1}$), symmetric (if $k = hgh^{-1}$ then $g = h^{-1}kh$), and transitive (if $k = hgh^{-1}$ and $m = uku^{-1}$ then $m = (uh)g(uh)^{-1}$).

It follows that the conjugacy classes $C(g)$ form a partition of G: each element of G lies in exactly one conjugacy class, and distinct classes are disjoint. Equivalently,

$$G = \bigsqcup_{g \in \mathcal{R}} C(g), \tag{3}$$

where $\mathcal{R}$ is any set containing one representative from each conjugacy class, and $\bigsqcup$ denotes a disjoint union.

Example II.3 (Examples of groups)**.** Examples of groups include:

- **Integers:** $(\mathbb{Z}, +)$, the set of integers with addition. Identity: 0. Inverse: $-n$ for $n \in \mathbb{Z}$. Order: infinite. Generator: 1 (or equivalently -1).

- **Cyclic group:** $(\mathbb{Z}_n, + \bmod n)$, the set $\{0, 1, \ldots, n-1\}$ with addition modulo n. Identity: 0. Inverse: $(-k) \bmod n$. Order: n. Generator: 1 (or any k coprime with n).

- **Symmetric group:** $(S_n, \circ)$, the group of all permutations of $\{1, \ldots, n\}$. Operation: composition of permutations. Order: $n!$. Generators: the adjacent transpositions $(i, i+1)$ for $i = 1, \ldots, n-1$.

- **Dihedral group:** $(D_n, \circ)$, the symmetries of a regular n-gon with composition. Elements: n rotations and n reflections, so $|D_n| = 2n$. Generators: rotation σ (by $2\pi/n$) and reflection τ, satisfying

$$\sigma^n = e, \quad \tau^2 = e, \quad \tau\sigma\tau = \sigma^{-1}.$$

- **General linear group:** $(\mathrm{GL}(n, \mathbb{C}), \cdot)$, the set of invertible $n \times n$ complex matrices. Operation: matrix multiplication. Order: infinite.

- **Unitary group:** $(\mathrm{U}(n), \cdot)$, the set of $n \times n$ matrices U with $U^\dagger U = I$. Operation: matrix multiplication. Order: infinite.

- **Special unitary group:** $(\mathrm{SU}(n), \cdot)$, the subgroup of $\mathrm{U}(n)$ with $\det(U) = 1$. Same operation, identity, and inverses as $\mathrm{U}(n)$. Order: infinite.

- **Orthogonal group:** $(\mathrm{O}(n), \cdot)$, the group of real $n \times n$ matrices O with $O^\top O = I$. Operation: matrix multiplication. Order: infinite. Its subgroup $\mathrm{SO}(n)$ consists of matrices with $\det(O) = 1$.

We now summarize several key structural properties used to classify groups.

Definition II.4 (Types of groups)**.** Let G be a group.

- **Finite group:** G is *finite* if $|G| < \infty$. Examples: $(\mathbb{Z}_n, +)$, D_n, and S_n are finite. In contrast, $(\mathbb{Z}, +)$ is infinite.

- **Infinite group:** G is *infinite* if it has infinitely many elements. Discrete example: $(\mathbb{Z}, +)$. Continuous examples: *Lie groups* such as $\mathrm{GL}(n, \mathbb{C})$ or $\mathrm{U}(n)$, which, in addition to their group structure, also carry the structure of a smooth manifold. In a Lie group, both the multiplication and inversion maps are smooth (infinitely differentiable).

- **Abelian group:** G is *Abelian* if $gh = hg$ for all $g, h \in G$. Examples: $(\mathbb{Z}, +)$ and $(\mathbb{Z}_n, +)$ are Abelian, whereas S_n and D_n are non-Abelian for $n \geq 3$.

A. Cosets, normal subgroups, and Lagrange's theorem

Definition II.5 (Left and right cosets)**.** Let G be a group and $H \leq G$ a subgroup. For any $g \in G$, the *left coset* of H with representative g is

$$gH \coloneqq \{gh \mid h \in H\}.$$

Similarly, the *right coset* of H with representative g is

$$Hg \coloneqq \{hg \mid h \in H\}.$$

Cosets are closely related to the idea of quotienting a group by a subgroup.

Definition II.6 (Quotient set)**.** Let $H \leq G$. The set of all left cosets of H in G is called the *left quotient set* and is denoted

$$G/H \coloneqq \{gH \mid g \in G\}.$$

Similarly, the set of all right cosets of H in G is called the *right quotient set* and is denoted

$$H\backslash G \coloneqq \{Hg \mid g \in G\}.$$

To define quotient groups, we first recall the notion of normality.

Definition II.7 (Normal subgroup)**.** A subgroup $H \leq G$ is *normal* if

$$ghg^{-1} \in H \quad \text{for all } g \in G,\ h \in H.$$

Equivalently, $gH = Hg$ for all $g \in G$. Normality is denoted by $H \trianglelefteq G$.

As examples, the special unitary group $\mathrm{SU}(n)$ is a normal subgroup of the unitary group $\mathrm{U}(n)$, and in quantum information, the Pauli group is a normal subgroup of the Clifford group. In contrast, $\mathrm{U}(n)$ is not normal in the general linear group $\mathrm{GL}(n, \mathbb{C})$.

We can now collect fundamental properties of cosets. For the last property, the notion of normality is essential.

Lemma II.8 (Basic properties of cosets)**.** *Let G be a group and $H \leq G$ a subgroup.*

- ***Disjointness:*** *Any two left cosets are either disjoint or identical.*
- ***Equal size:*** *All left cosets of H in G have the same cardinality as H, i.e. $|gH| = |H|$ for every $g \in G$.*
- ***Partition of G:*** *The left cosets of H form a partition of G, i.e.*

$$G = \bigsqcup_{gH \in G/H} gH.$$

- ***Normal subgroups and quotient groups:*** *If $H \trianglelefteq G$ (i.e. H is normal), then left and right cosets coincide, and the set of cosets G/H inherits a natural group structure with multiplication*

$$(gH) \cdot (g'H) \coloneqq (gg')H,$$

which is well defined (independent of the chosen coset representatives). This group is called the quotient group *G/H.*

Proof. We prove each property point by point:

- *Disjointness:* Assume $gH \cap g'H \neq \emptyset$. Then there exists $x \in gH \cap g'H$, so $x = gh = g'h'$ for some $h, h' \in H$. Multiplying on the right by h^{-1} yields $g = g'h'h^{-1}$. Since $h'h^{-1} \in H$, we have $g \in g'H$. For any $k \in H$, $gk = g'(h'h^{-1}k) \in g'H$, so $gH \subseteq g'H$. By symmetry, $g'H \subseteq gH$, hence $gH = g'H$. If $gH \cap g'H = \emptyset$, the cosets are disjoint.
- *Equal size:* Define $f : H \to gH$ by $f(h) = gh$. This map is bijective: if $f(h) = f(h')$, then $gh = gh' \Rightarrow h = h'$; and for any $y \in gH$, there exists $h \in H$ with $y = gh = f(h)$. Therefore, $|gH| = |H|$.

- *Partition of G:* For every $g \in G$, $g \in gH$. By disjointness, any two distinct cosets do not overlap. Thus, G is the disjoint union of all left cosets of H.
- *Normal subgroups and quotient groups:* If $H \trianglelefteq G$, then for every $g \in G$ and $h \in H$ we have $ghg^{-1} \in H$, which implies $gH = Hg$ because for any $x \in gH$ we can write $x = gh = (ghg^{-1})g$ with $ghg^{-1} \in H$, so $x \in Hg$ and $gH \subseteq Hg$ (and similarly for $Hg \subseteq gH$).

  To prove that coset multiplication is well defined, assume $gH = g_1H$ and $g'H = g'_1H$. Then there exist $h_1, h_2 \in H$ such that $g_1 = gh_1$ and $g'_1 = g'h_2$. Consider $(g_1g'_1)H = (gh_1g'h_2)H$. Since H is normal, $g'^{-1}h_1g' \in H$, so we can write $h_1g' = g'h_3$ for some $h_3 \in H$. Thus $(gh_1g'h_2)H = (gg'h_3h_2)H = (gg')H$ because $h_3h_2 \in H$ and multiplying by an element of H does not change the coset. Therefore $(g_1g'_1)H = (gg')H$, which proves that the product $(gH) \cdot (g'H) \coloneqq (gg')H$ is independent of the chosen coset representatives and G/H inherits a well-defined group structure.

□

Theorem II.9 (Lagrange's theorem)**.** *Let G be a finite group and $H \leq G$ a subgroup. Then $|H|$ divides $|G|$. Specifically, it holds*

$$|G| = |G/H| \cdot |H|.$$

Proof. By the partition property established in Lemma II.8, the left cosets of H form a disjoint partition of G, and by the equal-size property of the same lemma, each coset has cardinality $|H|$. Since there are exactly $|G/H|$ cosets, it follows that

$$|G| = |G/H| \cdot |H|.$$

□

We call $[G : H] \coloneqq |G/H|$ the *index* of H in G. Thus,

$$|G/H| = [G : H] = \frac{|G|}{|H|}.$$

If $H \trianglelefteq G$ is normal, then G/H is a group (the *quotient group*) of order $|G/H| = |G|/|H|$.

Moreover, Lagrange's theorem implies that the order of any element $g \in G$ divides $|G|$ (since $|\langle g \rangle| \mid |G|$). Thus, if $|G|$ is prime, then G is cyclic and generated by any non-identity element.

B. Group homomorphisms

Group theory is not only about studying single groups in isolation, but also about understanding how different groups relate to each other. The natural way to compare two groups is via maps that preserve their group operation.

Definition II.10 (Group homomorphisms, kernels, and images)**.** Let G and G' be groups.

- **Homomorphism:** A map $\varphi : G \to G'$ is called a *group homomorphism* if for all $g, h \in G$ we have $\varphi(gh) = \varphi(g)\varphi(h)$. Homomorphisms automatically preserve the identity and inverses, i.e. $\varphi(e_G) = e_{G'}$ and $\varphi(g^{-1}) = \varphi(g)^{-1}$ for all $g \in G$.
- **Kernel:** The *kernel* of φ is the set

$$\ker \varphi \coloneqq \{g \in G \mid \varphi(g) = e_{G'}\}.$$

- **Image:** The *image* of φ is the set

$$\operatorname{im} \varphi \coloneqq \{\varphi(g) \mid g \in G\} \subseteq G'.$$

- **Isomorphism:** A homomorphism φ is an *isomorphism* if it is bijective. In this case, G and G' are said to be *isomorphic*, written $G \cong G'$, and they have the same group structure.

- **Faithful homomorphism:** A homomorphism $\varphi : G \to G'$ is called *faithful* if it is injective. Equivalently, φ is faithful if its kernel is trivial:

$$\ker \varphi = \{e_G\}.$$

  This means that different elements of G are sent to different elements of G', so the homomorphism captures the full structure of G.

Note that a faithful homomorphism need not be surjective, so it is not necessarily an isomorphism.

Proposition II.11 (Kernel and image of a group homomorphism)**.** *Let $\varphi : G \to G'$ be a group homomorphism. Then:*

1. *The kernel* $\ker \varphi$ *is a normal subgroup of G, i.e.* $\ker \varphi \trianglelefteq G$.
2. *The image* $\operatorname{im} \varphi$ *is a subgroup of G', i.e.* $\operatorname{im} \varphi \leq G'$.

Proof. **(1)** *Kernel is normal:* The identity e_G satisfies $\varphi(e_G) = e_{G'}$, so $e_G \in \ker \varphi$. If $g, h \in \ker \varphi$, then $\varphi(gh^{-1}) = \varphi(g)\varphi(h)^{-1} = e_{G'}e_{G'}^{-1} = e_{G'}$, so $gh^{-1} \in \ker \varphi$. Thus $\ker \varphi \leq G$. For normality, for any $g \in G$ and $k \in \ker \varphi$,

$$\varphi(gkg^{-1}) = \varphi(g)\varphi(k)\varphi(g)^{-1} = \varphi(g)e_{G'}\varphi(g)^{-1} = e_{G'},$$

hence $gkg^{-1} \in \ker \varphi$.

(2) *Image is a subgroup:* If $x, y \in \operatorname{im} \varphi$, then $x = \varphi(g)$ and $y = \varphi(h)$ for some $g, h \in G$. Then $xy^{-1} = \varphi(g)\varphi(h)^{-1} = \varphi(gh^{-1}) \in \operatorname{im} \varphi$. Also, $\varphi(e_G) = e_{G'} \in \operatorname{im} \varphi$. □

Group homorphisms will play a central role later when we study group representations. Indeed, a representation of a group is simply a homomorphism from G into the group of invertible linear transformations on a vector space.

C. Actions of groups

Beyond the study of groups and homomorphisms, it is often useful to understand how groups can act on other sets. A *group action* formalises the idea of representing elements of a group as transformations of a set in a way that respects the group structure.

Definition II.12 (Group action)**.** Let G be a group and X a set. A *(left) action* of G on X is a map

$$\cdot : G \times X \to X, \qquad (g, x) \mapsto g \cdot x,$$

such that:

1. **Identity:** $e \cdot x = x$ for all $x \in X$.
2. **Compatibility:** $(gh) \cdot x = g \cdot (h \cdot x)$ for all $g, h \in G$ and $x \in X$.

If such a map exists, we say that G *acts* on X.

Remark II.13. Typical examples include:

- S_n acting on $\{1, \ldots, n\}$ by permutation.
- A matrix group acting on $\mathbb{R}^n$ or $\mathbb{C}^n$ by matrix multiplication.
- A group G acting on itself by left multiplication, $g \cdot x = gx$.
- A group G acting on itself by conjugation, $g \cdot x = gxg^{-1}$.

Definition II.14 (Orbit and stabilizer)**.** Let a group G act on a set X.

- The *orbit* of $x \in X$ is

$$\operatorname{Orb}(x) := \{g \cdot x \mid g \in G\}.$$

- The *stabilizer* of $x \in X$ is the subgroup

$$\mathrm{Stab}(x) \coloneqq \{g \in G \mid g \cdot x = x\} \leq G.$$

Theorem II.15 (Orbit–Stabilizer Theorem)**.** *Let G act on X and fix $x \in X$. Then*

$$|G| = |\mathrm{Orb}(x)| \cdot |\mathrm{Stab}(x)|.$$

Equivalently, $|\mathrm{Orb}(x)| = [G : \mathrm{Stab}(x)]$.

Proof. Fix $x \in X$. Two elements $g, h \in G$ send x to the same point in the orbit, i.e. $g \cdot x = h \cdot x$, if and only if $g^{-1}h \in \mathrm{Stab}(x)$ (equivalently, $h \in g\,\mathrm{Stab}(x)$). Thus, the elements of G that map x to the same point in the orbit form exactly one left coset of $\mathrm{Stab}(x)$. Therefore, the orbit $\mathrm{Orb}(x)$ is in one-to-one correspondence with the set of left cosets $G/\mathrm{Stab}(x)$. By Lagrange's theorem we obtain

$$|\mathrm{Orb}(x)| = |G/\mathrm{Stab}(x)| = \frac{|G|}{|\mathrm{Stab}(x)|}.$$

□

Corollary II.16 (Conjugacy classes and centralizers)**.** *If G acts on itself by conjugation, i.e. $g \cdot x = gxg^{-1}$, then:*

- *The orbits under this action are precisely the* conjugacy classes

$$C(x) \coloneqq \{gxg^{-1} \mid g \in G\}.$$

- *The stabilizer of $x \in G$ is its* centralizer

$$\mathrm{Cent}(x) \coloneqq \{g \in G \mid gx = xg\} \leq G.$$

Consequently, by the Orbit–Stabilizer Theorem,

$$|C(x)| = \frac{|G|}{|\mathrm{Cent}(x)|}.$$

D. Symmetric group

Definition II.17 (Symmetric group)**.** For a positive integer n, the *symmetric group* S_n is the group of all bijections (permutations)

$$\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\},$$

with the group operation given by composition of functions.

The identity element is the identity permutation $\mathrm{id}(i) = i$, every permutation has an inverse given by its inverse function, and $|S_n| = n!$.

Definition II.18 (Transpositions and cycles)**.** A *transposition* is a permutation that swaps two elements and leaves all others fixed, denoted $(i\,j)$. A *k-cycle* is a permutation

$$(i_1\, i_2\, \ldots\, i_k),$$

which maps $i_j \mapsto i_{j+1}$ for $j < k$ and $i_k \mapsto i_1$, leaving all other elements fixed. The *length* of a cycle is the number of elements it permutes, and the *order* of a cycle is its length. Disjoint cycles commute.

Example II.19. $S_2 = \{\mathrm{id}, (12)\}$ has two elements, where (12) swaps 1 and 2. S_3 has six elements:

$$S_3 = \{\mathrm{id}, (12), (13), (23), (123), (132)\},$$

where (ij) are transpositions and (123) is a 3-cycle of order 3.

We now collect the main structural properties of S_n.

Lemma II.20 (Basic properties of S_n)**.** *The symmetric group S_n satisfies:*

- ***Cycle decomposition:*** *Every permutation in S_n can be written uniquely (up to the order of disjoint cycles) as a product of disjoint cycles.*
- ***Minimal transposition length:*** *Any k-cycle can be written as a product of $k-1$ transpositions. Consequently, any permutation in S_n can be written as a product of at most $n-1$ transpositions (not necessarily adjacent).*
- ***Generators:*** *S_n is generated by the adjacent transpositions $(1\,2), (2\,3), \ldots, (n-1\,n)$.*
- ***Conjugacy classes:*** *Two permutations $\sigma, \tau \in S_n$ are conjugate if and only if there exists $\pi \in S_n$ such that $\tau = \pi\sigma\pi^{-1}$. Conjugacy classes in S_n correspond exactly to their* cycle type *(the cycle type of a permutation is the* multiset *of the lengths of its disjoint cycles, where multiplicities are counted. For example, in S_4, $(1\,2)(3\,4)$ has cycle type $\{2,2\}$, whereas $(1\,2)(3)(4)$ has cycle type $\{2,1,1\}$).*
- ***Transposition count:*** *A permutation cannot be expressed both as a product of an even number and as a product of an odd number of transpositions.*

Proof. **Cycle decomposition:** Given $\sigma \in S_n$, pick any $i \in \{1, \ldots, n\}$ and follow its images under σ:

$$i \mapsto \sigma(i) \mapsto \sigma^2(i) \mapsto \cdots$$

until it returns to i. This process defines a cycle. Repeating the procedure for any element not yet included in a cycle yields a product of disjoint cycles.

Uniqueness holds because each element of $\{1, \ldots, n\}$ belongs to exactly one cycle: starting from any element i and iterating σ always produces the same cycle, and disjoint cycles involve disjoint sets of elements. The only freedom is the order in which the disjoint cycles are written, but this does not change the permutation since disjoint cycles commute.

Minimal transposition length: Any k-cycle $(i_1\, i_2\, \ldots\, i_k)$ can be written as a product of $k-1$ transpositions:

$$(i_1\, i_2\, \ldots\, i_k) = (i_1\, i_k)(i_1\, i_{k-1}) \cdots (i_1\, i_2).$$

Thus, if σ is a product of disjoint cycles of lengths $k_1, k_2, \ldots, k_m$ with $k_1 + \cdots + k_m = n$, it can be expressed using at most $(k_1 - 1) + \cdots + (k_m - 1) = n - m \leq n - 1$ transpositions.

Generators: Every permutation can be written as a product of cycles, and each cycle can be written as a product of transpositions as above. Furthermore, any transposition $(i\, j)$ (with $i < j$) can be expressed in terms of adjacent transpositions:

$$(i\, j) = (j-1\, j)(j-2\, j-1) \cdots (i\, i+1) \cdots (j-2\, j-1)(j-1\, j),$$

where j is moved next to i, swapped, and then moved back. Therefore, S_n is generated by the adjacent transpositions $(1\,2), (2\,3), \ldots, (n-1\,n)$.

Conjugacy classes: If $\tau = \pi\sigma\pi^{-1}$, conjugation by π simply relabels the elements of σ, so τ has the same cycle structure, and thus the same cycle type, as σ. Conversely, if two permutations have the same cycle type, a suitable relabeling of their elements (via some $\pi \in S_n$) transforms one into the other, proving that they are conjugate.

Transposition count: Suppose a permutation $\sigma \in S_n$ can be expressed in two ways:

$$\sigma = \tau_1\tau_2 \cdots \tau_r = \rho_1\rho_2 \cdots \rho_s,$$

where each τ_i and ρ_j is a transposition. Then

$$\mathrm{id} = \sigma\sigma^{-1} = \tau_1 \cdots \tau_r\, \rho_s^{-1} \cdots \rho_1^{-1}.$$

This represents the identity as a product of $r + s$ transpositions.

An *inversion* is a pair (i, j) with $i < j$ but $\sigma(i) > \sigma(j)$. Each transposition changes the inversion count by 1 mod 2, because swapping two elements reverses their relative order and thus flips the parity of the inversion count. Since the identity permutation has zero inversions, an odd number of transpositions cannot yield the identity. Therefore, $r + s$ must be even, which implies that r and s differ by an even number. ☐

The *parity* of a permutation is defined as the parity (evenness or oddness) of the number of transpositions in any of its decompositions. By the previous lemma, this notion is well defined.

Definition II.21 (Parity of a permutation)**.** A permutation $\sigma \in S_n$ is called *even* if it can be written as a product of an even number of transpositions and *odd* otherwise.

The set of even permutations forms a normal subgroup of S_n called the *alternating group* A_n.

Its order is $|A_n| = \frac{n!}{2}$. Indeed, every permutation in S_n has a well-defined parity and is either even or odd. The even permutations form a subgroup $A_n \leq S_n$, and the odd permutations form the other coset gA_n for any odd permutation g, since multiplying an even permutation by g yields an odd permutation and vice versa. Because cosets of a subgroup have the same size and partition S_n, it follows that $|S_n| = 2|A_n|$, and therefore $|A_n| = |S_n|/2 = n!/2$.

Definition II.22 (Sign of a permutation)**.** The *sign* (or signature) of a permutation $\sigma \in S_n$ is defined as

$$\operatorname{sgn}(\sigma) = \begin{cases} +1 & \text{if } \sigma \text{ is even,} \\ -1 & \text{if } \sigma \text{ is odd.} \end{cases}$$

This defines a group homomorphism $\operatorname{sgn} : S_n \to \{\pm 1\}$ whose kernel is the alternating group A_n.

III. REPRESENTATION THEORY

We now turn to representation theory, where the central idea is to study groups by mapping their elements to matrices in such a way that the group multiplication is preserved. This perspective is powerful because it allows us to translate algebraic problems about groups into questions about linear maps and their associated matrix.

A. Representations of finite groups

Definition III.1 (Representation)**.** A *representation* of a finite group G on a complex vector space V is a homomorphism

$$\rho : G \to \mathrm{GL}(V),$$

where $\mathrm{GL}(V)$ is the group of invertible linear transformations on V. The dimension of V is called the *dimension* (or *degree*) of the representation and is denoted by $\dim(\rho)$.

We will often denote a representation of G by (ρ, V), where ρ specifies the homomorphism and V is the underlying vector space. When the space is clear from context, we will simply write ρ.

If we fix a basis for V, each linear map $A \in \mathrm{GL}(V)$ can be represented in such a basis by a $d \times d$ matrix, denoted by $[A]$, where $\dim V = d$. In particular, for every $g \in G$, the linear map $\rho(g)$ is represented by the matrix $[\rho(g)]$. Thus, in matrix form,

$$[\rho] : G \to \mathrm{GL}(d, \mathbb{C}), \qquad g \longmapsto [\rho(g)], \tag{4}$$

where, for all $g, h \in G$,

$$[\rho(gh)] = [\rho(g)]\,[\rho(h)], \tag{5}$$

$$[\rho(e)] = I_d, \tag{6}$$

$$[\rho(g^{-1})] = [\rho(g)]^{-1}. \tag{7}$$

Whenever it is clear from the context that we are working in a fixed basis, we will omit the brackets and simply write $\rho(g)$ for its matrix form.

Remark III.2 (Thinking in terms of unitary matrices)**.** In quantum information, most of the representations we encounter are *unitary*, meaning that

$$\rho : G \to \mathrm{U}(d),$$

where $\mathrm{U}(d)$ is the group of $d \times d$ unitary matrices.

If it helps your intuition, you may think of a representation as a map that assigns to each group element g a unitary matrix $U(g) \equiv \rho(g)$ such that, for all $g, h \in G$,

$$U(gh) = U(g)U(h) \quad \text{and} \quad U(g)U(g)^\dagger = I.$$

Later, we will see that for finite groups and finite-dimensional complex vector spaces, this viewpoint involves no loss of generality: for every representation, one can pick a suitable basis in which all the matrices $[\rho(g)]$ are unitary.

Example III.3 (Quantum information example: cyclic groups and Pauli/Weyl operators)**.** Consider the cyclic group $\mathbb{Z}_2 = \{0, 1\}$ under addition modulo 2. We can represent it on a single-qubit Hilbert space $V = \mathbb{C}^2$ in two natural ways:

- Using the Pauli-X matrix:

$$\rho(0) = I, \qquad \rho(1) = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

- Using the Pauli-Z matrix:

$$\rho(0) = I, \qquad \rho(1) = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

In both cases, ρ is a valid representation because $\rho(0+1) = \rho(1) = \rho(0)\rho(1)$ and $\rho(1+1) = \rho(0) = \rho(1)\rho(1)$. Another valid (1-dimensional) representation is $\rho(0) = 1$ and $\rho(1) = -1$.

More generally, for the cyclic group $\mathbb{Z}_d = \{0, 1, \ldots, d-1\}$ we can use the *Weyl operators* on a d-dimensional Hilbert space. The shift operator X and the phase operator Z are defined by

$$X|j\rangle = |j+1 \bmod d\rangle, \qquad Z|j\rangle = \omega^j |j\rangle,$$

where $\omega = e^{2\pi i/d}$. These define d-dimensional representations of $\mathbb{Z}_d$ via

$$\rho(k) = X^k \qquad \text{or} \qquad \rho(k) = Z^k,$$

since $\rho(k+\ell) = \rho(k)\rho(\ell)$ for all $k, \ell \in \mathbb{Z}_d$. Additionally, there are d one-dimensional representations given by

$$\rho_k(j) = \omega^{kj}, \qquad k = 0, \ldots, d-1.$$

Example III.4 (Basic examples of representations)**.** Let G be a finite group. Below are three fundamental examples of representations $\rho : G \to \mathrm{GL}(V)$, each acting on a different complex vector space V.

- **Trivial representation:** The *trivial representation* $\rho_{\text{triv}} : G \to \mathrm{GL}(\mathbb{C})$ is defined by

  $$\rho_{\text{triv}}(g) = 1 \qquad \text{for all } g \in G.$$

  It acts on the one-dimensional space $V = \mathbb{C}$, and every group element is mapped to the identity transformation.

- **Permutation representation (of S_n):** Let $G = S_n$, the symmetric group. Define $V = \mathbb{C}^n$ with standard basis $\{|1\rangle, \ldots, |n\rangle\}$. The *permutation representation* $\rho_{\text{perm}} : S_n \to \mathrm{GL}(V)$ is defined by

  $$\rho_{\text{perm}}(g)|i\rangle = |g(i)\rangle.$$

  Equivalently, the matrix form of $\rho_{\text{perm}}(g)$ is:

  $$\rho_{\text{perm}}(g) = \sum_{i=1}^{n} |g(i)\rangle\langle i|.$$

- **Regular representation:** For any finite group G, define the vector space $V = \mathbb{C}[G] = \mathrm{span}\{|g\rangle \mid g \in G\}$, which has dimension $|G|$. The *(left) regular representation* $\rho_{\text{reg}} : G \to \mathrm{GL}(V)$ is given by

  $$\rho_{\text{reg}}(g)|h\rangle = |gh\rangle.$$

  In matrix form, this becomes:

  $$\rho_{\text{reg}}(g) = \sum_{h \in G} |gh\rangle\langle h|.$$

  That is, G acts on the basis $\{|h\rangle\}$ by left multiplication.

Note that each of the constructions above satisfies the definition of a representation. In particular, we will see how the regular representation will play a fundamental role later (as it contains every irreducible representation of G as a subrepresentation, and it will be used in important proofs).

We also note that if ρ is a representation of G, then for any invertible linear operator U, the map

$$\rho'(g) \coloneqq U\rho(g)U^{-1}$$

is also a representation of G, since it satisfies

$$\rho'(gh) = U\rho(gh)U^{-1} = U\rho(g)\rho(h)U^{-1} = (U\rho(g)U^{-1})(U\rho(h)U^{-1}) = \rho'(g)\rho'(h).$$

This leads to the following definition.

Definition III.5 (Equivalent (isomorphic) representations)**.** Two representations $\rho : G \to \mathrm{GL}(V)$ and $\rho' : G \to \mathrm{GL}(W)$ are called *equivalent* (or *isomorphic*) if there exists an invertible linear map $T : V \to W$ such that

$$\rho'(g) = T\rho(g)T^{-1} \qquad \forall\, g \in G.$$

In this case, V and W necessarily have the same dimension. If ρ and ρ' are equivalent, we write $\rho \cong \rho'$; otherwise, we write $\rho \ncong \rho'$.

In quantum information, we are often mostly interested in *unitary* matrix representations, as we mentioned. In this case, the equivalence of two unitary representations can be directly defined with respect to a unitary matrix instead of a general invertible matrix. For this reason, the following fact is useful to stress.

Remark III.6 (Equivalence implies unitary equivalence for unitary representations)**.** Let $U_1, U_2 : G \to \mathrm{U}(d)$ be two unitary representations of a finite group G. If they are equivalent in the general sense, i.e. there exists an invertible matrix T such that $U_2(g) = TU_1(g)T^{-1}$ for all $g \in G$, then there also exists a *unitary* matrix V such that

$$U_2(g) = VU_1(g)V^\dagger \qquad \forall g \in G.$$

In other words, for unitary representations, equivalence can always be realized by a unitary change of basis.

The proof follows from standard linear algebra and is omitted here for conciseness

Example III.7 (Equivalence for Pauli matrices representation of the cyclic group)**.** Consider the previous example III.3. For $\mathbb{Z}_2$, the Pauli-X and Pauli-Z representations are equivalent. Indeed, if

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

is the Hadamard gate, then

$$HZ^kH^{-1} = X^k \qquad \forall\, k \in \mathbb{Z}_2,$$

so the two 2-dimensional representations are related by the change of basis $T = H$.

Now let us introduce the fundamental concepts of reducibility and irreducibility of a representation.

Definition III.8 (Subrepresentations and reducibility)**.** Let $\rho : G \to \mathrm{GL}(V)$ be a representation.

- A subspace $W \subseteq V$ is called *G-invariant* if

$$\rho(g)\,|w\rangle \in W \qquad \forall\, g \in G,\ |w\rangle \in W.$$

- If such a nontrivial subspace W exists (i.e. $W \neq \{0\}$ and $W \neq V$), then ρ is called *reducible*; otherwise, ρ is called *irreducible*. (Often, the shorthand term *irrep* is used to denote an irreducible representation.)
- If $W \subseteq V$ is G-invariant, the restriction of ρ to W defines a new representation

$$\rho|_W : G \to \mathrm{GL}(W), \qquad \rho|_W(g) = \rho(g)|_W,$$

  called the *subrepresentation* of ρ on W.

Note that the above definition of subrepresentation is well defined, i.e. the restriction is indeed a representation.

Proof. Since W is G-invariant, for every $g \in G$ we have $\rho(g)W \subseteq W$, so the map $\rho(g)|_W$ is a well-defined linear operator on W. For any $g, h \in G$ and $|w\rangle \in W$,

$$\rho|_W(g)\rho|_W(h)\,|w\rangle = \rho(g)\big(\rho(h)\,|w\rangle\big) = \rho(gh)\,|w\rangle = \rho|_W(gh)\,|w\rangle\,,$$

and $\rho|_W(e) = \rho(e)|_W = I_W$. Moreover, $\rho|_W(g)$ is invertible because for any $g \in G$, its inverse is given by $\rho|_W(g^{-1})$:

$$\rho|_W(g)\rho|_W(g^{-1}) = \rho|_W(gg^{-1}) = I_W, \qquad \rho|_W(g^{-1})\rho|_W(g) = \rho|_W(g^{-1}g) = I_W.$$

Therefore, $\rho|_W$ is a representation of G on W. □

If the representation $\rho : G \to \mathrm{GL}(V)$ of G is irreducible, we often say that V is an *irreducible subspace* (with respect to the representation ρ).

Example III.9 (Reducibility of the regular representation)**.** The regular representation of a finite group G on the space $V = \mathrm{span}\{|g\rangle \mid g \in G\}$ is always reducible. Indeed, consider the vector

$$|\psi\rangle = \sum_{g \in G} |g\rangle\,.$$

For every $h \in G$,

$$\rho(h)\,|\psi\rangle = \sum_{g \in G} |hg\rangle = \sum_{g' \in G} |g'\rangle = |\psi\rangle\,,$$

where we relabeled $g' = hg$. Thus, the span of $\{|\psi\rangle\}$ is a G-invariant subspace. The restriction of ρ to this one-dimensional space is irreducible, as every one-dimensional representation is irreducible.

Before defining the direct sum of representations, let us briefly recall the notion of the direct sum of vector spaces. If V_1 and V_2 are vector subspaces of the same vector space, then their sum is defined as

$$V_1 + V_2 \coloneqq \{v_1 + v_2 \mid v_1 \in V_1,\ v_2 \in V_2\}.$$

If, in addition, $V_1 \cap V_2 = \{0\}$, we say that the sum is *direct*, and we write

$$V_1 \oplus V_2 \coloneqq \{v_1 + v_2 \mid v_1 \in V_1,\ v_2 \in V_2\}.$$

In this case, every element of $V_1 \oplus V_2$ can be written uniquely as a sum of a vector from V_1 and a vector from V_2.

Definition III.10 (Direct sum of representations)**.** Let $\rho_1 : G \to \mathrm{GL}(V_1)$ and $\rho_2 : G \to \mathrm{GL}(V_2)$ be two representations of a finite group G. The *direct sum* of ρ_1 and ρ_2 is the representation

$$\rho_1 \oplus \rho_2 : G \longrightarrow \mathrm{GL}(V_1 \oplus V_2),$$

defined by

$$(\rho_1 \oplus \rho_2)(g) \coloneqq \rho_1(g) \oplus \rho_2(g), \qquad \forall\, g \in G,$$

where the right-hand side is the linear map on $V_1 \oplus V_2$ that acts as $\rho_1(g)$ on V_1 and as $\rho_2(g)$ on V_2.

In matrix form, after choosing a basis of $V_1 \oplus V_2$ obtained by concatenating bases of V_1 and V_2, we have

$$(\rho_1 \oplus \rho_2)(g) = \begin{pmatrix} \rho_1(g) & 0 \\ 0 & \rho_2(g) \end{pmatrix} = \sum_{i=1}^{2} |i\rangle\langle i| \otimes \rho_i(g).$$

We now prove that every G-invariant subspace admits an invariant complement.

Proposition III.11 (Existence of invariant complements)**.** *Let $\rho : G \to \mathrm{GL}(V)$ be a representation of a finite group, and let $W \subseteq V$ be a G-invariant subspace. Then there exists a G-invariant subspace $W^\perp \subseteq V$ such that*

$$V = W \oplus W^\perp.$$

Proof. **Special case: unitary representations.** Suppose that ρ is unitary, i.e. there exists a basis in which $\rho(g) \equiv U(g) \in \mathrm{U}(d)$ for all $g \in G$. Let $W^\perp$ be the orthogonal complement of W with respect to the standard inner product. Take any $|v\rangle \in W^\perp$ and $|w\rangle \in W$. For any $g \in G$,

$$\langle \rho(g)v|w\rangle = \langle v|\rho(g)^\dagger|w\rangle = \langle v|\rho(g^{-1})|w\rangle = 0,$$

because $\rho(g^{-1})\,|w\rangle \in W$ by G-invariance of W and $|v\rangle$ is orthogonal to W. Therefore, $\rho(g)\,|v\rangle \in W^\perp$ for all g, showing that $W^\perp$ is G-invariant. The orthogonal decomposition then gives $V = W \oplus W^\perp$.

General case. In general, the representation $\rho(g)$ may not be unitary transformations for all $g \in G$. However, we can define a G-invariant inner product by averaging over the group:

$$\langle v, w\rangle_G \coloneqq \frac{1}{|G|} \sum_{g\in G} \langle \rho(g)v, \rho(g)w\rangle.$$

This inner product satisfies

$$\langle \rho(h)v, \rho(h)w\rangle_G = \langle v, w\rangle_G \qquad \forall h \in G,$$

which can be shown as follows:

$$\langle \rho(h)v, \rho(h)w\rangle_G = \frac{1}{|G|} \sum_{g\in G} \langle \rho(g)\rho(h)v, \rho(g)\rho(h)w\rangle \tag{8}$$

$$= \frac{1}{|G|} \sum_{g\in G} \langle \rho(gh)v, \rho(gh)w\rangle \tag{9}$$

$$= \frac{1}{|G|} \sum_{g'\in G} \langle \rho(g')v, \rho(g')w\rangle \tag{10}$$

$$= \langle v, w\rangle_G, \tag{11}$$

where in the third step we relabeled $g' = gh$; the sum is unchanged because $g \mapsto gh$ is a bijection of G. That is, for each $g \in G$, $\rho(G)$ is a unitary transformation. Now define $W^\perp$ as the orthogonal complement of W with respect to $\langle \cdot, \cdot \rangle_G$. For $v \in W^\perp$ and $w \in W$,

$$\langle \rho(h)v, w \rangle_G = \langle v, \rho(h^{-1})w \rangle_G = 0,$$

because $\rho(h^{-1})w \in W$ and $v \perp W$. Thus, $\rho(h)v \in W^\perp$, so $W^\perp$ is G-invariant. Finally, the orthogonal decomposition theorem yields $V = W \oplus W^\perp$. □

This leads to a fundamental result in the representation theory of finite groups:

Theorem III.12 (Maschke's theorem: complete reducibility)**.** *Every finite-dimensional representation of a finite group G over $\mathbb{C}$ is completely reducible, i.e. it can be written as a direct sum of irreducible representations.*

Proof. We prove this by induction on $\dim V$. If ρ is irreducible, there is nothing to prove. If ρ is reducible, let $W_1 \subset V$ be a nontrivial G-invariant subspace. By Proposition III.11, there exists an invariant complement W_2 such that

$$V = W_1 \oplus W_2. \tag{12}$$

The restrictions $\rho|_{W_1}$ and $\rho|_{W_2}$ are representations of smaller dimension, so by induction they decompose as direct sums of irreducible representations. Combining these decompositions yields the desired result. □

Corollary III.13 (Block-diagonal form of representations)**.** *By Maschke's theorem, every finite-dimensional complex representation $\rho : G \to \mathrm{GL}(V)$ of a finite group G decomposes as a direct sum of irreducible representations. That is,*

$$\rho(g) \;=\; \bigoplus_{i=1}^{k} \rho_{V_i}(g), \qquad V \;=\; \bigoplus_{i=1}^{k} V_i, \tag{13}$$

where each ρ_{V_i} is an irreducible representation of G acting on the subspace $V_i \subseteq V$.

Choosing a basis of V obtained by concatenating bases of the V_i yields a block-diagonal matrix form for $\rho(g)$:

$$[\rho(g)] = \begin{pmatrix} [\rho_{V_1}(g)] & 0 & \cdots & 0 \\ 0 & [\rho_{V_2}(g)] & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & [\rho_{V_k}(g)] \end{pmatrix} \tag{14}$$

$$= \sum_{i=1}^{k} |i\rangle\langle i| \otimes [\rho_{V_i}(g)], \tag{15}$$

where $[\rho_{V_i}(g)]$ is the matrix of $\rho_{V_i}(g)$ in a chosen basis of V_i.

If some of the irreducible subrepresentations ρ_{V_i} are equivalent (i.e. according to Definition III.5), we can reorganize our vector space to group all equivalent copies together. Let $\rho_1, \ldots, \rho_r$ be a set of pairwise non-isomorphic irreducible representations, and let m_i be the multiplicity of ρ_i in ρ, i.e., the number of times ρ_i appears in the decomposition. Then we can write

$$\rho(g) = \bigoplus_{i=1}^{r} \Big(\underbrace{\rho_i(g) \oplus \cdots \oplus \rho_i(g)}_{m_i \text{ times}} \Big) \tag{16}$$

$$= \bigoplus_{i=1}^{r} \big(I_{m_i} \otimes \rho_i(g) \big), \tag{17}$$

and similarly for the underlying vector space:

$$V = \bigoplus_{i=1}^{r} \big(\underbrace{V_i \oplus \cdots \oplus V_i}_{m_i \text{ times}} \big) \tag{18}$$

$$= \bigoplus_{i=1}^{r} \big(\mathbb{C}^{m_i} \otimes V_i \big) \tag{19}$$

$$= \mathrm{span}\big\{ \, |i, a\rangle \otimes |v\rangle \;\big|\; 1 \le i \le r,\; 1 \le a \le m_i,\; |v\rangle \in V_i \big\}. \tag{20}$$

Here:

- ρ_i are pairwise non-isomorphic irreducible representations acting on V_i,
- $m_i \in \mathbb{N}$ is the *multiplicity* of ρ_i in ρ, i.e. the number of times ρ_i appears in the decomposition,
- $\mathbb{C}^{m_i}$ is a multiplicity space on which $\rho(g)$ acts trivially,
- $\{|i,a\rangle\}_{a=1}^{m_i}$ is an orthonormal basis of the multiplicity space $\mathbb{C}^{m_i}$, and $\{|v\rangle\}$ a basis of V_i.

In matrix form, after choosing a basis adapted to this decomposition, we obtain

$$[\rho(g)] = \bigoplus_{i=1}^{r} \underbrace{\begin{pmatrix} [\rho_i(g)] & & 0 \\ & \ddots & \\ 0 & & [\rho_i(g)] \end{pmatrix}}_{m_i \text{ times}} \tag{21}$$

$$= \bigoplus_{i=1}^{r} \left(I_{m_i} \otimes [\rho_i(g)]\right) \tag{22}$$

$$= \sum_{i=1}^{r} |i\rangle\langle i| \otimes I_{m_i} \otimes [\rho_i(g)] \tag{23}$$

$$= \sum_{i=1}^{r} \sum_{a=1}^{m_i} |i,a\rangle\langle i,a| \otimes [\rho_i(g)]. \tag{24}$$

Here $I_{m_i} = \sum_{a=1}^{m_i} |a\rangle\langle a|$ is the identity on the multiplicity space.

Definition III.14 (Isotypic component)**.** Let $\rho : G \to \mathrm{GL}(V)$ be a finite-dimensional complex representation of a finite group G, and suppose

$$V \cong \bigoplus_{i=1}^{r} \left(\mathbb{C}^{m_i} \otimes V_i\right), \qquad \rho(g) = \bigoplus_{i=1}^{r} \left(I_{m_i} \otimes \rho_i(g)\right),$$

where the V_i are pairwise inequivalent irreducible representations. The *isotypic component* corresponding to ρ_i are defined as the G-invariant subspace

$$V^{(i)} := \mathbb{C}^{m_i} \otimes V_i.$$

B. Unitary representations

We now show that for finite groups any representation is equivalent to a unitary one, i.e. we can always pick an orthonormal basis in which the matrices of the representation are unitary for all group elements.

Definition III.15 (Unitary representation)**.** Let G be a group and let $(V, \langle\cdot,\cdot\rangle)$ be a complex inner product space. A representation $\rho : G \to \mathrm{GL}(V)$ is said to be *unitary* (with respect to $\langle\cdot,\cdot\rangle$) if

$$\langle \rho(g)v, \rho(g)w\rangle = \langle v, w\rangle \qquad \forall\, v, w \in V,\ g \in G.$$

Theorem III.16 (Every representation is unitary with respect to a suitable inner product)**.** *Let $\rho : G \to \mathrm{GL}(V)$ be a finite-dimensional complex representation of a finite group G. Then there exists a Hermitian inner product $\langle\cdot,\cdot\rangle_G$ on V with respect to which ρ is unitary.*

Proof. Start with any Hermitian inner product $\langle\cdot,\cdot\rangle$ on V. Define a new inner product by averaging over the group (as in the proof of Proposition III.11 that we used in Maschke's theorem):

$$\langle v, w\rangle_G := \frac{1}{|G|} \sum_{g \in G} \langle \rho(g)v, \rho(g)w\rangle.$$

This is a Hermitian, positive-definite inner product. Moreover, it is G-invariant: for all $h \in G$,

$$\langle \rho(h)v, \rho(h)w \rangle_G = \langle v, w \rangle_G.$$

Therefore, $\rho(g)$ is unitary with respect to $\langle \cdot, \cdot \rangle_G$ for all $g \in G$. □

The existence of such an inner product implies that one can always pick an orthonormal basis (with respect to this inner product) in which, for every $g \in G$, the matrix of $\rho(g)$ is unitary.

This follows from the following standard fact: given any Hermitian inner product $\langle \cdot, \cdot \rangle$ on a complex vector space V, there exists an orthonormal basis with respect to this inner product (by the Gram–Schmidt process). Moreover, a linear operator $U : V \to V$ is unitary (with respect to $\langle \cdot, \cdot \rangle$) if and only if, in such an orthonormal basis, its matrix representation $[U]$ satisfies

$$[U]^\dagger [U] = I,$$

that is, it is a unitary matrix in the usual sense.

Combining this fact with Theorem III.16, which shows that there exists an inner product with respect to which the representation is unitary, we obtain:

Corollary III.17 (Any representation can be associated with unitary matrices)**.** *Let G be a finite group, and let $\rho : G \to \mathrm{GL}(V)$ be a representation on a finite-dimensional complex vector space V. Then there exists a basis of V such that, for every $g \in G$, the matrix of $\rho(g)$ expressed in this basis is unitary, i.e.,*

$$[\rho(g)]^\dagger [\rho(g)] = I.$$

In particular, any matrix representation of a finite group can be expressed in a basis in which all the representation matrices are unitary. This observation will be fundamental in the development of *character theory.*

More generally, one may also be interested in finding a linear transformation that makes a representation unitary with respect to a given inner product. We recall this standard linear algebra fact: If $\langle \cdot, \cdot \rangle_G$ and $\langle \cdot, \cdot \rangle$ are two Hermitian inner products on V, then there exists an operator $T \in \mathrm{GL}(V)$ such that

$$\langle v, w \rangle = \langle Tv, Tw \rangle_G \qquad \forall\, v, w \in V.$$

Combining this fact with Theorem III.16, we obtain:

Corollary III.18 (Every representation is equivalent to a unitary one for any inner product)**.** *For any Hermitian inner product $\langle \cdot, \cdot \rangle$ on V, every finite-dimensional complex representation $\rho : G \to \mathrm{GL}(V)$ is equivalent to a representation that is unitary with respect to $\langle \cdot, \cdot \rangle$. In other words, there exists an invertible linear map $T \in \mathrm{GL}(V)$ such that*

$$\rho'(g) \coloneqq T^{-1} \rho(g) T$$

is unitary with respect to $\langle \cdot, \cdot \rangle$ for all $g \in G$.

Proof. By Theorem III.16, there exists an inner product $\langle \cdot, \cdot \rangle_G$ with respect to which ρ is unitary. Now, let $\langle \cdot, \cdot \rangle$ be any other Hermitian inner product on V. By the standard fact stated above, there exists an invertible operator T such that $\langle v, w \rangle = \langle Tv, Tw \rangle_G$ for all $v, w \in V$. Define the new representation $\rho'(g) \coloneqq T^{-1} \rho(g) T$. For any $v, w \in V$ and any $g \in G$, we compute:

$$\begin{aligned}
\langle \rho'(g)v, \rho'(g)w \rangle &= \langle T\rho'(g)v, T\rho'(g)w \rangle_G \\
&= \langle \rho(g)Tv, \rho(g)Tw \rangle_G \quad \text{(by definition of } \rho'\text{)} \\
&= \langle Tv, Tw \rangle_G \quad \text{(since } \rho \text{ is unitary w.r.t. } \langle \cdot, \cdot \rangle_G\text{)} \\
&= \langle v, w \rangle.
\end{aligned}$$

Thus, $\rho'(g)$ is unitary with respect to $\langle \cdot, \cdot \rangle$ for every $g \in G$. □

C. Schur's lemmas

One of the most important tools in representation theory is provided by *Schur's lemmas.* To motivate these results, let us consider the following physical scenario.

Suppose we have a Hamiltonian H that is *invariant* under a symmetry group G. Formally, this means that there exists a unitary representation $U : G \to \mathrm{U}(V)$ such that

$$U(g)HU(g)^\dagger \;=\; H \qquad \Longleftrightarrow \qquad [U(g), H] \;=\; 0, \qquad \forall g \in G. \tag{25}$$

We have already seen that any representation U admits a particularly convenient block-diagonal form: there exists a change of basis W such that, for every $g \in G$,

$$WU(g)W^\dagger \;=\; \bigoplus_{i=1}^{r} \big(I_{m_i} \otimes \rho_i(g)\big), \tag{26}$$

where ρ_i are pairwise non-isomorphic irreducible representations of G, m_i are their multiplicities, and $\dim(V_i) = \dim \rho_i$ is the dimension of the carrier space of ρ_i.

Because H commutes with *all* such block-diagonal matrices $U(g)$ simultaneously, this imposes a strong constraint on H. As we shall see, this constraint is precisely characterized by *Schur's lemma*: in the same basis W that block-diagonalizes the representation U, the Hamiltonian H is transformed into $H' = WHW^\dagger$ of the form

$$H' \;=\; \bigoplus_{i=1}^{r} \big(A_i \otimes I_{\dim(V_i)}\big) \;=\; \sum_{i=1}^{r} |i\rangle\langle i| \otimes A_i \otimes I_{\dim(V_i)} \;=\; \sum_{i=1}^{r} |i\rangle\langle i| \otimes A_i \otimes \left(\sum_{b=1}^{\dim(V_i)} |b\rangle\langle b|\right),$$

where A_i is a Hermitian matrix acting on the multiplicity space of dimension m_i, and $I_{\dim(V_i)} = \sum_{b=1}^{\dim(V_i)} |b\rangle\langle b|$ is the identity on the carrier space of the irrep ρ_i.

This result has two immediate consequences. First, if $\{E_j^{(i)}\}_{j=1}^{m_i}$ are the eigenvalues of the Hermitian matrix $A_i \in \mathbb{C}^{m_i \times m_i}$, each $E_j^{(i)}$ gives rise to a $\dim(V_i)$-fold degenerate eigenvalue of H', with corresponding eigenvectors

$$\Big\{\, |i\rangle \otimes \Big|E_j^{(i)}\Big\rangle \otimes |b\rangle \;\Big|\; 1 \le j \le m_i,\; 1 \le b \le \dim(V_i)\Big\},$$

where $|i\rangle$ labels the irrep (symmetry) sector, $\{\Big|E_j^{(i)}\Big\rangle\}_{j=1}^{m_i}$ are eigenvectors of A_i, and $\{|b\rangle\}_{b=1}^{\dim(V_i)}$ is an orthonormal basis of the carrier space V_i of the irrep ρ_i.

Second, the diagonalization of H is greatly simplified: instead of diagonalizing the full Hamiltonian at once, one only needs to diagonalize the smaller Hermitian matrices A_i, gaining significant computational efficiency by working independently within each symmetry sector.

Finally, the eigenvalues of H coincide with those of $H' = WHW^\dagger$, while the eigenvectors of the original Hamiltonian H are obtained by applying the inverse change of basis:

$$|\psi_{i,j,b}\rangle \;=\; W^\dagger\big(\,|i\rangle \otimes \Big|E_j^{(i)}\Big\rangle \otimes |b\rangle\,\big).$$

To formalize and prove this structure, we now introduce the notion of *intertwiners*—linear maps that commute with a group action—after which we will state and prove Schur's lemmas and then we will prove what we have claimed above, i.e., the structure of an operator commuting with a representation.

To express this result in the most general way, we first introduce the notion of *intertwiners*. Schur's lemmas will then characterize the structure of all such intertwiners.

Definition III.19 (Intertwiner)**.** Let $\rho : G \to \mathrm{GL}(V)$ and $\rho' : G \to \mathrm{GL}(W)$ be two representations of a group G. A linear map $T : V \to W$ is called an *intertwiner* (or a *G-equivariant map*) if

$$T\rho(g) = \rho'(g)T, \qquad \forall g \in G. \tag{27}$$

We denote the space of all such intertwiners by

$$\mathrm{Hom}_G(V, W) \coloneqq \{T : V \to W \,|\, T\rho(g) = \rho'(g)T \text{ for all } g \in G\}\,. \tag{28}$$

Before introducing Schur's lemma, here is a small but useful lemma for Schur's lemma.

Lemma III.20 (Image and kernel of an intertwiner are G-invariant)**.** *Let $\rho : G \to \mathrm{GL}(V)$ and $\rho' : G \to \mathrm{GL}(W)$ be two representations of a group G, and let $T \in \mathrm{Hom}_G(V, W)$ be an intertwiner. Then both the kernel and image of T are G-invariant subspaces:*

1. $\ker T \subseteq V$ *is* G*-invariant, i.e.*

$$\rho(g)\ker T \subseteq \ker T, \quad \forall g \in G.$$

2. $\mathrm{Im}(T) \subseteq W$ *is* G*-invariant, i.e.*

$$\rho'(g)\,\mathrm{Im}(T) \subseteq \mathrm{Im}(T), \quad \forall g \in G.$$

Proof. We have:

- Let $|v\rangle \in \ker T$. Then $T|v\rangle = 0$, and for any $g \in G$,

$$T\rho(g)|v\rangle = \rho'(g)T|v\rangle = \rho'(g)\cdot 0 = 0,$$

  so $\rho(g)|v\rangle \in \ker T$.

- Let $|w\rangle \in \mathrm{Im}(T)$. Then $|w\rangle = T|v\rangle$ for some $|v\rangle \in V$. For any $g \in G$,

$$\rho'(g)|w\rangle = \rho'(g)T|v\rangle = T\rho(g)|v\rangle \in \mathrm{Im}(T).$$

□

We begin with a fundamental special case of Schur's lemma.

Lemma III.21 (Schur's Lemma — intertwiner from an irrep to itself)**.** *Let* $\rho : G \to \mathrm{GL}(V)$ *be an irreducible representation over a finite-dimensional complex vector space* V*. Then any linear operator* $T : V \to V$ *that commutes with all* $\rho(g)$*,*

$$T\rho(g) = \rho(g)T \qquad \forall g \in G,$$

must be a scalar multiple of the identity:

$$T = \lambda I_V, \qquad \lambda \in \mathbb{C}.$$

Proof. Since V is finite-dimensional over $\mathbb{C}$, the operator T has at least one eigenvalue $\lambda \in \mathbb{C}$ and an associated eigenvector (this follows because the characteristic polynomial $\det(T - \lambda I)$ has at least one root $\lambda \in \mathbb{C}$ by the fundamental theorem of algebra). Let $V_\lambda := \{|v\rangle \in V \mid T|v\rangle = \lambda|v\rangle\}$ be the eigenspace corresponding to λ, which is nonzero by definition.

Note that $V_\lambda = \ker(T - \lambda I_V)$. Since T commutes with every $\rho(g)$, the operator $T - \lambda I_V$ also commutes with every $\rho(g)$, hence is itself an intertwiner. So, by Lemma III.20 (Image and kernel of an intertwiner are G-invariant), the space $V_\lambda = \ker(T - \lambda I_V)$ is a G-invariant subspace of V. By irreducibility of ρ, the only nonzero G-invariant subspace is V itself, so $V_\lambda = V$. Therefore $T = \lambda I_V$. □

Lemma III.22 (Schur's Lemma — intertwiner from an irrep to another one)**.** *Let* $\rho : G \to \mathrm{GL}(V)$ *and* $\rho' : G \to \mathrm{GL}(W)$ *be irreducible representations over finite-dimensional complex vector spaces* V *and* W*.*

We write $\rho \cong \rho'$ *to denote that* ρ *and* ρ' *are* equivalent representations*, meaning there exists an invertible linear map* $T_0 : V \to W$ *such that*

$$\rho(g) = T_0^{-1}\rho'(g)T_0, \qquad \forall g \in G.$$

We write $\rho \ncong \rho'$ *to mean that they are* inequivalent*. Then:*

- *If* $\rho \ncong \rho'$*, then*

$$\mathrm{Hom}_G(V, W) = \{0\}.$$

- *If* $\rho \cong \rho'$*, then*

$$\mathrm{Hom}_G(V, W) = \{\lambda \cdot T_0 \mid \lambda \in \mathbb{C}\},$$

  where T_0 *is the intertwiner from the definition of equivalence.*

Proof. Let $T \in \mathrm{Hom}_G(V, W)$, i.e. $T\rho(g) = \rho'(g)T$ for all $g \in G$. We consider two cases.

- Case $\rho \ncong \rho'$: T is an intertwiner so $\ker T \subseteq V$ and $\mathrm{Im}(T) \subseteq W$ are G-invariant subspaces by lemma III.20. Since ρ and ρ' are irreducible, $\ker T$ is either $\{0\}$ or V, and $\mathrm{Im}(T)$ is either $\{0\}$ or W. If $\ker T = V$, then $T = 0$. If $\ker T = \{0\}$ and $\mathrm{Im}(T) = \{0\}$, then $T = 0$. If $\ker T = \{0\}$ and $\mathrm{Im}(T) = W$, then T is a linear isomorphism from V to W, contradicting $\rho \ncong \rho'$. Thus in all cases $T = 0$.

- Case $\rho \cong \rho'$: Let $T_0 : V \to W$ be any fixed nonzero intertwiner (which exists by equivalence). For any $T \in \mathrm{Hom}_G(V, W)$, define $S := T_0^{-1}T : V \to V$. Then S is an intertwiner from V to itself:

$$S\rho(g) = T_0^{-1}T\rho(g) = T_0^{-1}\rho'(g)T = \rho(g)T_0^{-1}T = \rho(g)S.$$

  By Lemma III.22 (Schur's lemma for an irrep to itself), $S = \lambda I_V$ for some $\lambda \in \mathbb{C}$. Hence $T = T_0S = \lambda T_0$.

□

Schur's lemma reveals a remarkable rigidity of intertwiners: if two representations are irreducible, then any intertwiner between them is either zero (if they are inequivalent) or uniquely determined up to a scalar (if they are equivalent).

An immediate consequence of Schur's lemma is the following:

Corollary III.23 (Irreps of abelian groups are 1-dimensional)**.** *Let G be a finite abelian group, and $\rho : G \to \mathrm{GL}(V)$ an irreducible representation. Then $\dim V = 1$. In other words, every irreducible representation of an abelian group is one-dimensional.*

Proof. Since G is abelian, all $\rho(g)$ commute with each other. In particular, for each $g \in G$, the map $\rho(g)$ commutes with all $\rho(h)$, so $\rho(g)$ is an intertwiner for the irrep ρ.

By Schur's lemma, this means $\rho(g) = \lambda_g I_V$ for some $\lambda_g \in \mathbb{C}$. So for all $|v\rangle \in V$ and all $g \in G$,

$$\rho(g)\,|v\rangle = \lambda_g\,|v\rangle\,.$$

So for any $|v\rangle \in V$, the subspace $\mathrm{span}\{|v\rangle\}$ is G-invariant. But since ρ is irreducible, the only G-invariant subspaces are $\{0\}$ and V, so this is only possible if $\dim V = 1$. □

1. *The commutant structure: what are the operators commuting with a representation?*

As a consequence of Schur's Lemma, we are now ready to prove the result mentioned at the beginning of the previous subsection: namely, that any operator commuting with a group representation must have a very specific block structure.

Proposition III.24 (Structure of operators commuting with a symmetry group representation)**.** *Let $U : G \to \mathrm{U}(V)$ be a unitary representation of a finite group G on a Hilbert space V, and let $H : V \to V$ be a linear operator such that*

$$[U(g), H] = 0 \qquad \text{for all } g \in G. \tag{29}$$

Let W be a unitary matrix that puts $U(g)$ into its canonical block-diagonal form:

$$WU(g)W^\dagger = \bigoplus_{i=1}^{r} \left(I_{m_i} \otimes \rho_i(g)\right),$$

where $\rho_i : G \to \mathrm{U}(V_i)$ are pairwise non-isomorphic irreps, and m_i is the multiplicity of ρ_i in U.

Then H is simultaneously block-diagonalized by the same change of basis:

$$WHW^\dagger = \bigoplus_{i=1}^{r} \left(A_i \otimes I_{\dim V_i}\right),$$

where:

- *$A_i \in \mathbb{C}^{m_i \times m_i}$ acts on the multiplicity space $\mathbb{C}^{m_i}$,*
- *$I_{\dim V_i}$ is the identity operator on the irrep space V_i.*

If H is Hermitian, then each A_i is Hermitian as well.

Proof. Let W be the unitary that brings U to its canonical block-diagonal form. In bra–ket notation,

$$WU(g)W^{\dagger} \;=\; \sum_{i=1}^{r} |i\rangle\langle i| \otimes I_{m_i} \otimes \rho_i(g), \qquad \forall g \in G, \tag{30}$$

where $|i\rangle$ labels the irrep sector, the second register is the multiplicity space of dimension m_i, and the third register is the carrier space V_i of ρ_i. Define $H' = WHW^{\dagger}$. Since H commutes with $U(g)$ for all g, we have

$$(WU(g)W^{\dagger})H' \;=\; H'(WU(g)W^{\dagger}), \qquad \forall g \in G. \tag{31}$$

We now write H' in this basis as

$$H' \;=\; \sum_{i,j=1}^{r} |i\rangle\langle j| \otimes H'_{ij}, \tag{32}$$

where H'_{ij} act on the multiplicity and carrier spaces. Projecting the commutation relation onto sectors i, j by applying $\langle i|$ and $|j\rangle$ on the first register gives

$$(I_{m_i} \otimes \rho_i(g))H'_{ij} \;=\; H'_{ij}(I_{m_j} \otimes \rho_j(g)), \qquad \forall g \in G. \tag{33}$$

Expand H'_{ij} on the multiplicity indices:

$$H'_{ij} \;=\; \sum_{a=1}^{m_i}\sum_{b=1}^{m_j} |a\rangle\langle b| \otimes H'^{(a,b)}_{ij}, \tag{34}$$

where each $H'^{(a,b)}_{ij}$ is an operator mapping $V_j \to V_i$. Substitute this into the commutation relation. For the left-hand side:

$$(I_{m_i} \otimes \rho_i(g))H'_{ij} \;=\; \sum_{a,b} |a\rangle\langle b| \otimes \rho_i(g)H'^{(a,b)}_{ij}. \tag{35}$$

For the right-hand side:

$$H'_{ij}(I_{m_j} \otimes \rho_j(g)) \;=\; \sum_{a,b} |a\rangle\langle b| \otimes H'^{(a,b)}_{ij}\rho_j(g). \tag{36}$$

Equating both sides and comparing the coefficients of $|a\rangle\langle b|$ yields

$$\rho_i(g)H'^{(a,b)}_{ij} \;=\; H'^{(a,b)}_{ij}\rho_j(g), \qquad \forall g \in G,\ \forall a, b. \tag{37}$$

Now we get:

- If $i \neq j$, the irreps ρ_i and ρ_j are inequivalent. By Schur's lemma, there is no nonzero intertwiner between them, so

$$H'^{(a,b)}_{ij} \;=\; 0, \qquad \forall a, b, \tag{38}$$

  and hence $H'_{ij} = 0$ for $i \neq j$.

- If $i = j$, then $\rho_i = \rho_j$, and by Schur's lemma any operator commuting with all $\rho_i(g)$ must be proportional to the identity on V_i. Therefore,

$$H'^{(a,b)}_{ii} \;=\; (A_i)_{a,b}\, I_{\dim(V_i)}, \tag{39}$$

  for some matrix $A_i \in \mathbb{C}^{m_i \times m_i}$. This gives

$$H'_{ii} = \sum_{a,b=1}^{m_i} |a\rangle\langle b| \otimes H'^{(a,b)}_{ii} = A_i \otimes I_{\dim(V_i)}. \tag{40}$$

Combining all blocks,

$$H' = \sum_{i=1}^{r} |i\rangle\langle i| \otimes A_i \otimes I_{\dim(V_i)}. \tag{41}$$

If H is Hermitian, then $H' = WHW^\dagger$ is Hermitian, which implies each A_i is Hermitian. Finally, transforming back with $W^\dagger$ gives

$$H = W^\dagger \Big(\sum_{i=1}^{r} |i\rangle\langle i| \otimes A_i \otimes I_{\dim(V_i)} \Big) W, \tag{42}$$

as claimed. □

Corollary III.25 (Multiplicity-free case). *In the setting of Proposition III.24, if every irreducible representation appears with multiplicity $m_i = 1$, then each A_i reduces to a scalar $\lambda_i \in \mathbb{C}$ (or $\lambda_i \in \mathbb{R}$ if H is Hermitian), and hence*

$$H = W \left(\bigoplus_{i=1}^{r} \lambda_i I_{\dim(V_i)} \right) W^\dagger = \sum_{i=1}^{r} \lambda_i P_i, \tag{43}$$

where

$$P_i = W \left(|i\rangle\langle i| \otimes \sum_{j=1}^{\dim(V_i)} |j\rangle\langle j| \right) W^\dagger = \sum_{j=1}^{\dim(V_i)} W\, |i,j\rangle\langle i,j|\, W^\dagger \tag{44}$$

is the orthogonal projector onto the carrier space of the i-th irrep.

In this case, the symmetry completely determines the structure of H: the only free parameters are the scalars $\{\lambda_i\}_{i=1}^{r}$, and each λ_i corresponds to a $\dim(V_i)$-fold degenerate eigenvalue of H.

Remark III.26. Proposition III.24 was stated for unitary representations (in order to provide more familiarity with the symmetries one meet in quantum mechanics), but the same structural result holds more generally for any representation $\rho : G \to \mathrm{GL}(V)$. That is, if $\rho : G \to \mathrm{GL}(V)$ can be block-diagonalized as

$$\rho(g) = T^{-1} \left(\bigoplus_{i=1}^{r} I_{m_i} \otimes \rho_i(g) \right) T$$

for some invertible transformation T, then any operator $H \in \mathrm{End}(V)$ that commutes with all $\rho(g)$ must also decompose as

$$H = T \left(\bigoplus_{i=1}^{r} A_i \otimes I_{\dim V_i} \right) T^{-1},$$

where each $A_i \in \mathrm{End}(\mathbb{C}^{m_i})$ is an arbitrary linear operator acting on the multiplicity space. The proof is exactly the same, relying only on Schur's lemma and the block structure.

Definition III.27 (Commutant). Given a representation $\rho : G \to \mathrm{GL}(V)$, we define the *commutant* (or *centralizer algebra*) as

$$\mathrm{Comm}(\rho) := \{ H : V \to V \mid [\rho(g), H] = 0 \text{ for all } g \in G \}.$$

That is, the set of all linear maps that commute with the group representation.

Corollary III.28 (Dimension of the commutant). *Let $\rho : G \to \mathrm{GL}(V)$ be a representation of a finite group G, and suppose it decomposes as*

$$\rho \cong \bigoplus_{i=1}^{r} \rho_i^{\oplus m_i},$$

where the ρ_i are pairwise inequivalent irreducible representations, m_i is the multiplicity of ρ_i, and r is the number of inequivalent irreps appearing in the decomposition. Then the commutant has dimension

$$\dim(\mathrm{Comm}(\rho)) = \sum_{i=1}^{r} m_i^2.$$

Proof. Let $T \in \mathrm{GL}(V)$ be a change of basis that brings $\rho(g)$ into block-diagonal form:

$$T\rho(g)T^{-1} = \bigoplus_{i=1}^{r} (I_{m_i} \otimes \rho_i(g)),$$

where the ρ_i are pairwise inequivalent irreducible representations, and m_i is the multiplicity of ρ_i in ρ. Since $[\rho(g), H] = 0$ if and only if $[T\rho(g)T^{-1}, THT^{-1}] = 0$, we may assume from the start that

$$\rho(g) = \bigoplus_{i=1}^{r} (I_{m_i} \otimes \rho_i(g)).$$

Let $H : V \to V$ be any linear map commuting with all $\rho(g)$. Then H must preserve this block structure, i.e. $H = \bigoplus_i H_i$, with each H_i acting on the i-th block. By Schur's lemma (as seen in Proposition III.24), each H_i must be of the form

$$H_i = A_i \otimes I_{\dim V_i},$$

where A_i is a linear map on a vector space of dimension m_i. The space of such operators has complex dimension m_i^2. Summing over i, we get that the total dimension of the commutant is $\sum_{i=1}^{r} m_i^2$. □

2. *Averaging an operator over irreducible representations*

We now introduce an important consequence of Schur's lemma that we will use often in the next section. It uses the idea of averaging over the group that we have already encountered. This idea — symmetrizing a map by group averaging — is one of the core tricks in representation theory.

Proposition III.29 (Twirling over irreps)**.** *Let $\rho_1 : G \to \mathrm{GL}(V_1)$, $\rho_2 : G \to \mathrm{GL}(V_2)$ be two irreducible representations of a finite group G, and let $h : V_1 \to V_2$ be a linear map. Define the averaged map:*

$$h^0 := \frac{1}{|G|} \sum_{g \in G} \rho_2(g)^{-1} h \rho_1(g). \tag{45}$$

Then:

1. *If $\rho_1 \ncong \rho_2$, then $h^0 = 0$.*
2. *If $\rho_1 = \rho_2$ and $V := V_1 = V_2$, then h^0 is a scalar multiple of the identity:*

$$h^0 = \lambda I_V, \qquad \text{with } \lambda = \frac{1}{\dim V} \mathrm{Tr}(h). \tag{46}$$

Proof. We first observe that h^0 satisfies the intertwining relation:

$$\rho_2(s) h^0 = h^0 \rho_1(s), \qquad \forall s \in G. \tag{47}$$

Indeed,

$$\begin{aligned} \rho_2(s) h^0 &= \frac{1}{|G|} \sum_{g \in G} \rho_2(s)\rho_2(g)^{-1} h \rho_1(g) = \frac{1}{|G|} \sum_{g \in G} \rho_2(gs^{-1})^{-1} h \rho_1(g) \\ &= \frac{1}{|G|} \sum_{g \in G} \rho_2(g)^{-1} h \rho_1(gs) = h^0 \rho_1(s), \end{aligned} \tag{48}$$

where we changed variable $g \mapsto gs$ and used that

$$\rho_2(s)\rho_2(g)^{-1} = \rho_2(s^{-1})^{-1}\rho_2(g)^{-1} = (\rho_2(g)\rho_2(s^{-1}))^{-1} = \rho_2(gs^{-1})^{-1}.$$

So h^0 is a G-intertwiner. If $\rho_1 \ncong \rho_2$, Schur's lemma I gives $h^0 = 0$. If $\rho = \rho_1 = \rho_2$ and $V = V_1 = V_2$, Schur's lemma II gives $h^0 = \lambda I_V$. To compute λ, take the trace:

$$\mathrm{Tr}\big(h^0\big) = \frac{1}{|G|} \sum_{g \in G} \mathrm{Tr}\left(\rho(g)^{-1} h \rho(g)\right) = \frac{1}{|G|} \sum_{g \in G} \mathrm{Tr}(h) = \mathrm{Tr}(h), \tag{49}$$

by cyclicity of the trace. But also $\mathrm{Tr}\big(h^0\big) = \lambda \dim V$, so $\lambda = \frac{1}{\dim V} \mathrm{Tr}(h)$. □

As a corollary of the previous proposition, we get:

Corollary III.30 (Average of irreducible representations matrix elements)**.** *Let* $\rho_1 : G \to \mathrm{GL}(d_1, \mathbb{C})$ *and* $\rho_2 : G \to \mathrm{GL}(d_2, \mathbb{C})$ *be irreducible matrix representations of a finite group* G*. Let* $[\rho_1(g)]_{j_1 i_1}$ *and* $[\rho_2(g)]_{j_2 i_2}$ *denote the matrix elements of* $\rho_1(g)$ *and* $\rho_2(g)$*, respectively. Then:*

1. *If* $\rho_1 \ncong \rho_2$*, then for all* $i_1, j_1 \in \{1, \dots, d_1\}$ *and* $i_2, j_2 \in \{1, \dots, d_2\}$*,*

$$\frac{1}{|G|} \sum_{g \in G} \left[\rho_2(g^{-1})\right]_{j_2 i_2} \left[\rho_1(g)\right]_{j_1 i_1} = 0. \tag{50}$$

2. *If* $\rho = \rho_1 = \rho_2$ *is an irreducible representation of dimension* d*, then for all* $i_1, j_1, i_2, j_2 \in \{1, \dots, d\}$*,*

$$\frac{1}{|G|} \sum_{g \in G} [\rho(g^{-1})]_{j_2 i_2} [\rho(g)]_{j_1 i_1} = \frac{1}{d} \delta_{i_2 j_1} \delta_{j_2 i_1}. \tag{51}$$

In compact notation: If ρ_α *and* ρ_β *are two inequivalent irreducible representations of* G *of dimensions* d_α *and* d_β*, then*

$$\frac{1}{|G|} \sum_{g \in G} [\rho_\alpha(g^{-1})]_{j_2 i_2} [\rho_\beta(g)]_{j_1 i_1} = \frac{1}{d_\alpha} \delta_{\alpha\beta} \delta_{i_2 j_1} \delta_{j_2 i_1} \tag{52}$$

Proof. Define the averaged operator:

$$h^0 := \frac{1}{|G|} \sum_{g \in G} \rho_2(g^{-1}) h \rho_1(g),$$

where $h = |i_2\rangle \langle j_1|$. By Proposition III.29, if $\rho_1 \ncong \rho_2$, then $h^0 = 0$. Taking matrix elements:

$$\langle j_2| h^0 |i_1\rangle = \frac{1}{|G|} \sum_{g \in G} \langle j_2| \rho_2(g^{-1}) |i_2\rangle \langle j_1| \rho_1(g) |i_1\rangle = \frac{1}{|G|} \sum_{g \in G} [\rho_2(g^{-1})]_{j_2 i_2} [\rho_1(g)]_{j_1 i_1}.$$

So the left-hand side equals zero. Now suppose $\rho_1 = \rho_2 = \rho$ of dimension d. Then by Proposition III.29, we have $h^0 = \lambda I$, where $\lambda = \frac{1}{d} \mathrm{Tr}(h)$. Setting $h = |i_2\rangle \langle j_1|$, we compute the (j_2, i_1)-entry:

$$\langle j_2| h^0 |i_1\rangle = \frac{1}{|G|} \sum_{g \in G} \langle j_2| \rho(g^{-1}) |i_2\rangle \langle j_1| \rho(g) |i_1\rangle = \frac{1}{|G|} \sum_{g \in G} [\rho(g^{-1})]_{j_2 i_2} [\rho(g)]_{j_1 i_1}.$$

On the other hand,

$$\langle j_2| h^0 |i_1\rangle = \lambda \delta_{j_2 i_1}, \qquad \text{and} \qquad \lambda = \frac{1}{d} \mathrm{Tr}(h) = \frac{1}{d} \delta_{i_2 j_1}.$$

Therefore,

$$\frac{1}{|G|} \sum_{g \in G} [\rho(g^{-1})]_{j_2 i_2} [\rho(g)]_{j_1 i_1} = \frac{1}{d} \delta_{i_2 j_1} \delta_{j_2 i_1},$$

as claimed. ∎

IV. CHARACTER THEORY

We have seen that finite-dimensional representation ρ of a finite group G over $\mathbb{C}$ can be decomposed as

$$\rho \cong \bigoplus_i \rho_i^{\oplus m_i}, \tag{53}$$

where the ρ_i are irreducible and pairwise inequivalent, and m_i is the multiplicity — the number of times ρ_i appears in the decomposition. However, many questions remain open at this point. What are these irreps? How many are there? Could there be infinitely many? Can new ones be invented (up to isomorphism)? These questions will be addressed in the section.

To understand and classify irreducible representations, we need a practical tool that captures how a representation decomposes — ideally without working in any specific basis. This tool is the *character* of a representation.

Definition IV.1 (Character)**.** Let $\rho : G \to \mathrm{GL}(V)$ be a finite-dimensional complex representation of a finite group G. The *character* of ρ is the function

$$\chi_\rho : G \to \mathbb{C}, \qquad \chi_\rho(g) \coloneqq \mathrm{Tr}(\rho(g)).$$

Characters are just traces of the representation matrices, but they encode a surprising amount of information. We will see how they allow us to detect irreducibility, distinguish non-isomorphic representations, compute multiplicities, and ultimately prove that the number of inequivalent irreducible representations of a finite group equals the number of its conjugacy classes — and is therefore finite. At first glance, this may seem surprising: a character assigns a single complex number to each group element, whereas a representation assigns a full matrix.

Remark IV.2 (Basis independence and spectral meaning)**.** The character function $\chi_\rho(g) = \mathrm{Tr}(\rho(g))$ encodes spectral information in a basis-independent way:

- **Basis independence:** The trace of a linear operator is invariant under change of basis. So the character is well defined — it does not depend on how $\rho(g)$ is represented as a matrix.
- **Unitary form:** From Corollary III.17, we know that for any finite-dimensional representation of a finite group, we can always pick a basis in which all the $\rho(g)$ are unitary matrices. In that case, all eigenvalues lie on the unit circle — they are roots of unity.
- **Spectral interpretation:** The trace equals the sum of the eigenvalues of $\rho(g)$, counted with multiplicity:

$$\chi_\rho(g) = \mathrm{Tr}(\rho(g)) = \sum_{i=1}^{\dim V} \lambda_i.$$

More generally, the character determines all power sums of the eigenvalues:

$$\chi_\rho(g^k) = \mathrm{Tr}\big(\rho(g^k)\big) = \mathrm{Tr}\big(\rho(g)^k\big) = \sum_{i=1}^{\dim V} \lambda_i^k.$$

Thus, characters give us all eigenvalues power sums as stressed in the previous remark — which strongly constrain the eigenvalues. Since two unitary matrices are unitarily equivalent if and only if they have the same eigenvalues, the fact that characters can detect so much structure (such as testing if two representations are equivalent) becomes less surprising — and highlights why they are so powerful.

A. Basic properties of characters

We begin by collecting some basic facts about characters. These follow easily from the definitions but already reveal useful structure.

Lemma IV.3 (Basic properties of characters)**.** *Let $\rho : G \to \mathrm{GL}(V)$ be a finite-dimensional complex representation of a finite group G, and let χ_ρ be its character. Then:*

1. ***Class function:** For all $g, h \in G$,*

$$\chi_\rho(hgh^{-1}) = \chi_\rho(g).$$

2. ***Additivity:*** *If* $\rho = \rho_1 \oplus \rho_2$*, then*

$$\chi_\rho = \chi_{\rho_1} + \chi_{\rho_2}.$$

3. ***Value on inverses:*** *For all* $g \in G$*,*

$$\chi_\rho(g^{-1}) = \chi_\rho(g)^*.$$

4. ***Value at the identity:***

$$\chi_\rho(e) = \dim V.$$

5. ***Trivial representation:*** *The character of the trivial representation is*

$$\chi_{triv}(g) = 1 \quad \text{for all } g \in G.$$

Proof.

1. The first point follows by noting that $\rho(hgh^{-1}) = \rho(h)\rho(g)\rho(h)^{-1}$ and by ciclicity of the trace.
2. The trace of a block-diagonal matrix is the sum of the traces of its blocks:

$$\mathrm{Tr}(\rho_1(g) \oplus \rho_2(g)) = \mathrm{Tr}(\rho_1(g)) + \mathrm{Tr}(\rho_2(g)).$$

3. Every finite-dimensional representation of a finite group is equivalent to a unitary representation (Corollary III.17). So we can choose a basis in which each $\rho(g)$ is a unitary matrix. In that basis, the matrix of $\rho(g^{-1})$ satisfies

$$\rho(g^{-1}) = \rho(g)^{-1} = \rho(g)^\dagger = \rho(g)^{*\mathrm{T}}.$$

Thus, we get

$$\chi_\rho(g^{-1}) = \mathrm{Tr}\big(\rho(g^{-1})\big) = \mathrm{Tr}\big(\rho(g)^\dagger\big) = \mathrm{Tr}(\rho(g))^* = \chi_\rho(g)^*.$$

4. Since $\rho(e) = \mathrm{Id}_V$, we have $\chi_\rho(e) = \mathrm{Tr}(\mathrm{Id}_V) = \dim V$.
5. The trivial representation maps every group element to the scalar 1, so its trace is always 1.

□

This first point tells us that characters are a special kind of function on the group, called *class functions*. (We will later see that the characters of irreducible representations form an orthonormal basis for the space of class functions on G.)

Definition IV.4 (Class function)**.** A function $f : G \to \mathbb{C}$ is called a *class function* if it is constant on conjugacy classes:

$$f(hgh^{-1}) = f(g) \qquad \text{for all } g, h \in G. \tag{54}$$

The set of all class functions on G is denoted

$$\mathrm{Fun}_{\mathrm{class}}(G, \mathbb{C}) \coloneqq \{f \in \mathrm{Fun}(G, \mathbb{C}) \mid f(hgh^{-1}) = f(g)\ \forall g, h \in G\}.$$

Equivalently, f is a class function if and only if $f(gh) = f(hg)$ for all $g, h \in G$.[2]

Lemma IV.5 (Dimension of function spaces)**.** *Let G be a finite group. Then:*

1. *The space* $\mathrm{Fun}(G, \mathbb{C})$ *of all functions* $f : G \to \mathbb{C}$ *has dimension* $|G|$*.*

[2] The condition $f(h^{-1}gh) = f(g)$ for all $g, h \in G$ is equivalent to $f(sh) = f(hs)$ for all $s, h \in G$, as follows by setting $s = h^{-1}g$.

2. The subspace of class functions $\mathrm{Fun}_{\mathrm{class}}(G,\mathbb{C})$ *has dimension equal to the number of conjugacy classes of* G.

Proof. (1) A function $f: G \to \mathbb{C}$ is determined by its values on each $g \in G$. The set $\{\delta_g\}_{g\in G}$, where $\delta_g(h) \coloneqq \delta_{g,h}$, forms a basis: they span the space and are linearly independent. Indeed, for any $f: G \to \mathbb{C}$, we can write $f(\cdot) = \sum_{g\in G} f(g)\,\delta_g(\cdot)$, so $\{\delta_g\}_{g\in G}$ generate the space. If $\sum_{g\in G} \alpha_g\,\delta_g(\cdot) = 0$ as a function, then evaluating at $h = g_0$ forces $\alpha_{g_0} = 0$ for all $g_0 \in G$, proving linear independence. Thus, $\dim \mathrm{Fun}(G,\mathbb{C}) = |G|$.

(2) If f is a class function, then $f(g) = f(hgh^{-1})$ for all $g, h \in G$. Hence f is determined by its values on the conjugacy classes of G. A basis is given by the indicator functions δ_C of each conjugacy class C, defined by

$$\delta_C(g) \coloneqq \begin{cases} 1 & \text{if } g \in C, \\ 0 & \text{otherwise.} \end{cases}$$

The fact that these functions form a basis is proven as above, so the dimension of $\mathrm{Fun}_{\mathrm{class}}(G,\mathbb{C})$ equals the number of conjugacy classes. ☐

We now equip the space of complex-valued functions on G with a natural inner product.

Definition IV.6. Let $\psi, \phi : G \to \mathbb{C}$ be functions on a finite group G. We define their inner product as

$$\langle \psi, \phi \rangle_G \coloneqq \frac{1}{|G|} \sum_{g\in G} \psi(g)^* \phi(g). \tag{55}$$

We now verify that this is indeed a valid inner product, and show how the formula simplifies for class functions.

Lemma IV.7 (Inner product on functions on G)**.**

- *The function* $\langle \cdot, \cdot \rangle_G$ *defines a Hermitian inner product on the space of functions* $G \to \mathbb{C}$.
- *Moreover, if* ψ *and* ϕ *are class functions (i.e., constant on conjugacy classes), then the inner product reduces to*

$$\langle \psi, \phi \rangle_G = \frac{1}{|G|} \sum_{C\in \mathrm{Cl}(G)} |C|\, \psi(c)^* \phi(c), \tag{56}$$

where the sum runs over the conjugacy classes of G*, and* $c \in C$ *is any representative.*

Proof. For the first point, we verify the three defining properties of a Hermitian inner product. Let $\psi, \phi, \chi : G \to \mathbb{C}$ and $\lambda_1, \lambda_2 \in \mathbb{C}$.

1. *Conjugate symmetry:*

$$\langle \phi, \psi \rangle_G = \frac{1}{|G|} \sum_{g\in G} \phi(g)^* \psi(g) = \left(\frac{1}{|G|} \sum_{g\in G} \psi(g)^* \phi(g) \right)^* = \langle \psi, \phi \rangle_G^*.$$

2. *Linearity in the second argument:*

$$\langle \psi, \lambda_1 \phi + \lambda_2 \chi \rangle_G = \frac{1}{|G|} \sum_{g\in G} \psi(g)^* \left(\lambda_1 \phi(g) + \lambda_2 \chi(g) \right) \tag{57}$$

$$= \lambda_1 \langle \psi, \phi \rangle_G + \lambda_2 \langle \psi, \chi \rangle_G. \tag{58}$$

3. *Positive definiteness:*

$$\langle \psi, \psi \rangle_G = \frac{1}{|G|} \sum_{g\in G} |\psi(g)|^2 \geq 0,$$

with equality if and only if $\psi = 0$.

For the second point, suppose ψ and ϕ are class functions. Since they are constant on conjugacy classes, we can group the sum accordingly:

$$\langle \psi, \phi \rangle_G = \frac{1}{|G|} \sum_{C\in \mathrm{Cl}(G)} \sum_{g\in C} \psi(g)^* \phi(g) = \frac{1}{|G|} \sum_{C\in \mathrm{Cl}(G)} |C|\, \psi(c)^* \phi(c),$$

where $c \in C$ is any fixed representative. ☐

Using the inner product on functions $f : G \to \mathbb{C}$ introduced in the previous section, we now state an important orthogonality result about the matrix elements of (unitary) irreducible representations — often called the Schur orthogonality relations for irrep matrix elements.

Theorem IV.8 (Matrix elements of irreducible representations are orthogonal)**.** *Let ρ_a, ρ_b be two irreducible representations of G, of dimensions d_a and d_b, respectively. Select a basis in which the matrices $\rho_a(g)$ and $\rho_b(g)$ are unitary for all $g \in G$ (this is always possible because of Corollary III.17). Then for all $i_1, j_1 \in \{1, \dots, d_a\}$ and $i_2, j_2 \in \{1, \dots, d_b\}$, we have:*

$$\langle [\rho_a(g)]_{i_1 j_1}, [\rho_b(g)]_{i_2 j_2} \rangle_G = \frac{1}{d_a}\, \delta_{ab}\, \delta_{i_1 i_2}\, \delta_{j_1 j_2}. \tag{59}$$

In particular, in such a unitary basis the matrix elements of irreducible representations form an orthogonal set in the Hilbert space $\mathrm{Fun}(G, \mathbb{C})$ *of complex-valued functions on G. The total number of these orthogonal functions is*

$$\sum_{\rho_a \in \widehat{G}} d_a^2,$$

where the sum runs over the set $\widehat{G}$ of all inequivalent irreducible representations of G, and $d_a = \dim(\rho_a)$.

Proof. This follows from the matrix element orthogonality formula (Corollary III.30) established earlier. There, we showed:

$$\frac{1}{|G|} \sum_{g \in G} \left[\rho_a(g^{-1})\right]_{j_2 i_2} \left[\rho_b(g)\right]_{j_1 i_1} = \frac{1}{d_a} \delta_{ab} \delta_{i_2 j_1} \delta_{j_2 i_1}.$$

Using that $\rho_a(g^{-1}) = \rho_a(g)^*$ — which holds if we assume (as we can) that the matrices $\rho_a(g)$ are unitary, by Corollary III.17 — and recognizing the inner product between matrix elements, we get:

$$\langle [\rho_a(g)]_{i_1 j_1}, [\rho_b(g)]_{i_2 j_2} \rangle_G = \frac{1}{|G|} \sum_{g \in G} [\rho_a(g)]^*_{i_1 j_1} \left[\rho_b(g)\right]_{i_2 j_2} = \frac{1}{d_a} \delta_{ab} \delta_{i_1 i_2} \delta_{j_1 j_2}.$$

□

This raises a natural question: do the matrix elements of irreducible representations span the entire space of functions $f : G \to \mathbb{C}$?

We've seen that there are exactly $\sum_{\rho \in \widehat{G}} \dim(\rho)^2$ orthonormal functions coming from irreducible representations matrix elements. On the other hand, we've already established that the space of all complex-valued functions on G has dimension $|G|$ (in Lemma IV.5).

Do these two numbers match? Spoiler: yes. We'll prove this in the next sections. It will show that the matrix elements of irreducible representations actually form an orthonormal basis for the space of functions $f : G \to \mathbb{C}$.

You might have already seen a (continuos group) version of this in disguise — for instance, in quantum mechanics: spherical harmonics form an orthonormal basis of the square-integrable functions on the sphere, and they arise as the matrix elements of irreducible representations of SO(3).

B. The Grand Orthogonality Theorem: orthogonality of irreducible characters

In this section we explore some of the most fundamental consequences of character theory. We begin with a cornerstone result: the characters of inequivalent irreducible complex representations form an orthonormal set with respect to the standard inner product on functions over a group. This result is known as the *Grand Orthogonality Theorem* (GOT), also referred to as the *First Orthogonality Relation for Characters*, or the *First Schur Orthogonality Theorem.*

Theorem IV.9 (The Grand Orthogonality Theorem: Orthogonality of irreducible characters)**.** *Let $\chi_{\rho_a}, \chi_{\rho_b} : G \to \mathbb{C}$ be the characters of two irreducible complex representations of a finite group G. Then*

$$\langle \chi_{\rho_a}, \chi_{\rho_b} \rangle_G := \frac{1}{|G|} \sum_{g \in G} \chi_{\rho_a}(g)^* \, \chi_{\rho_b}(g) = \delta_{a,b},$$

where $\delta_{a,b}$ equals 1 if $\rho_a \cong \rho_b$, and 0 otherwise.

That is, the characters of distinct inequivalent irreducible representations are orthogonal with respect to the chosen inner product and so they form an orthonormal set of class functions.

Proof. This follows from Theorem IV.8, which established that if ρ_a, ρ_b are irreducible representations of G of dimensions d_a and d_b, then for all matrix elements:

$$\langle [\rho_a(g)]_{i_1 j_1}, [\rho_b(g)]_{i_2 j_2} \rangle_G = \frac{1}{d_a} \delta_{ab}\, \delta_{i_1 i_2}\, \delta_{j_1 j_2}.$$

We set $j_1 = i_1$, $j_2 = i_2$, then sum over i_1 and i_2. This gives

$$\langle \chi_{\rho_a}, \chi_{\rho_b} \rangle_G = \sum_{i_1=1}^{d_a} \sum_{i_2=1}^{d_b} \langle [\rho_a]_{i_1 i_1}, [\rho_b]_{i_2 i_2} \rangle_G = \frac{1}{d_a} \delta_{ab} \sum_{i=1}^{d_a} 1 = \delta_{ab}$$

□

From the previous corollary, we deduce the following: characters let us tell whether two irreducible representations are equivalent or not.

Corollary IV.10 (Testing equivalence of irreducible representations using characters)**.** *Let ρ_a and ρ_b be irreducible representations of a finite group G, with characters χ_{ρ_a} and χ_{ρ_b}. Then*

$$\rho_a \cong \rho_b \quad \iff \quad \chi_{\rho_a} = \chi_{\rho_b} \quad \iff \quad \langle \chi_{\rho_a}, \chi_{\rho_b} \rangle_G = 1.$$

Proof. If $\rho_a \cong \rho_b$, then they are equivalent, so their characters are equal: $\chi_{\rho_a} = \chi_{\rho_b}$.
If $\chi_{\rho_a} = \chi_{\rho_b}$, then by the orthogonality relations for characters shown above we have

$$\langle \chi_{\rho_a}, \chi_{\rho_b} \rangle_G = \langle \chi_{\rho_a}, \chi_{\rho_a} \rangle_G = 1.$$

Now suppose that $\langle \chi_{\rho_a}, \chi_{\rho_b} \rangle_G = 1$, then if $\rho_a \ncong \rho_b$, by orthogonality of irreducible characters we should have

$$\langle \chi_{\rho_a}, \chi_{\rho_b} \rangle_G = 0,$$

a contradiction. So $\rho_a \cong \rho_b$. □

We will shortly generalize this result, by showing that any two representation (possibly reducible) are equivalent if and only if they have the same character. From now on, we use the shorthand term *irreducible characters* to refer to the characters of irreducible representations.

Remark IV.11. Let $\widehat{G}$ be the set of inequivalent irreducible complex representations of G. From the orthogonality of irreducible characters (Theorem IV.9), the set

$$\{\chi_\lambda : \lambda \in \widehat{G}\}$$

is orthonormal in $\mathrm{Fun}_{\mathrm{class}}(G, \mathbb{C})$. In particular, the irreducible characters are linearly independent because they are orthonormal, so

$$|\widehat{G}| \ \leq \ \dim \mathrm{Fun}_{\mathrm{class}}(G, \mathbb{C}) = \#\{\text{conjugacy classes of } G\}, \tag{60}$$

a finite number for finite G. We will later prove the reverse inequality (in fact, equality) by showing that irreducible characters *span* $\mathrm{Fun}_{\mathrm{class}}(G, \mathbb{C})$, thereby establishing that the number of inequivalent irreducible representations equals the number of conjugacy classes.

Recall that by Maschke's theorem, any finite-dimensional representation $\rho : G \to \mathrm{GL}(V)$ of a finite group G decomposes as a direct sum of irreducible representations:

$$\rho \cong \bigoplus_{\lambda \in \widehat{G}} \rho_\lambda^{\oplus m_\lambda},$$

where $\widehat{G}$ denotes a complete list of inequivalent irreducible representations of G, and $m_\lambda \in \mathbb{N}$ is the *multiplicity* of ρ_λ in ρ, i.e., the number of times ρ_λ appears as a direct summand. In terms of characters, this decomposition reads

$$\chi_\rho = \sum_{\lambda \in \widehat{G}} m_\lambda \, \chi_\lambda. \tag{61}$$

We now show that these multiplicities are entirely determined by the character χ_ρ, and can be computed using inner products.

Theorem IV.12 (Multiplicity formula via characters)**.** *Let $\rho : G \to \mathrm{GL}(V)$ be a finite-dimensional representation of a finite group G, with character χ_ρ. Let ρ_λ be an irreducible representation with character χ_λ. Then the multiplicity of ρ_λ in ρ is given by*

$$m_\lambda = \langle \chi_\rho, \chi_\lambda \rangle_G = \frac{1}{|G|} \sum_{g \in G} \chi_\rho(g)^* \, \chi_\lambda(g).$$

Proof. We write the decomposition:

$$\rho \cong \bigoplus_{\lambda \in \widehat{G}} \rho_\lambda^{\oplus m_\lambda}, \quad \text{so} \quad \chi_\rho = \sum_{\lambda \in \widehat{G}} m_\lambda \chi_\lambda.$$

Taking the inner product with χ_μ, we find:

$$\langle \chi_\rho, \chi_\mu \rangle_G = \sum_{\lambda \in \widehat{G}} m_\lambda \, \langle \chi_\lambda, \chi_\mu \rangle_G = m_\mu,$$

since $\langle \chi_\lambda, \chi_\mu \rangle_G = \delta_{\lambda,\mu}$ by orthogonality of irreducible characters. □

Therefore, the multiplicity of each irreducible representation in ρ is completely determined by the character χ_ρ, and in particular is independent of how we write the decomposition. This implies the uniqueness of the decomposition into irreducibles, up to isomorphism and reordering.

Corollary IV.13 (Uniqueness of decomposition into irreducibles)**.** *Let $\rho : G \to \mathrm{GL}(V)$ be a finite-dimensional representation of a finite group G. Suppose ρ admits two decompositions into irreducible subrepresentations:*

$$\rho \cong \bigoplus_{i=1}^{r} \rho_i, \tag{62}$$

$$\rho \cong \bigoplus_{j=1}^{s} \sigma_j, \tag{63}$$

where each ρ_i and σ_j is irreducible.

Then $r = s$, and there exists a bijection $\pi : \{1, \ldots, r\} \to \{1, \ldots, s\}$ such that

$$\rho_i \cong \sigma_{\pi(i)} \qquad \text{for all } i.$$

That is, the multiset of irreducible summands in ρ, counted with multiplicity and up to isomorphism, is uniquely determined by the character χ_ρ.

Proof. From the multiplicity formula,

$$m_\lambda = \langle \chi_\rho, \chi_\lambda \rangle_G,$$

we know that the number of times any irreducible representation ρ_λ appears in the decomposition of ρ depends only on χ_ρ, and not on the choice of decomposition.

Therefore, each irreducible ρ_λ appears the same number of times in both decompositions, which implies that the two lists $\{\rho_1, \ldots, \rho_r\}$ and $\{\sigma_1, \ldots, \sigma_s\}$ must be the same up to permutation and isomorphism. □

We now show that two representations are equivalent if and only they have the same characters (generalizing what we saw earlier for irreducible representations).

Corollary IV.14 (Testing equivalence using characters)**.** *Let ρ, σ be two finite-dimensional representations of a finite group G, with characters χ_ρ and χ_σ, respectively. Then*

$$\chi_\rho = \chi_\sigma \quad \Longleftrightarrow \quad \rho \cong \sigma.$$

Proof. If $\rho \cong \sigma$, then they are equivalent representations, so their characters are equal: $\chi_\rho = \chi_\sigma$, since trace is invariant under change of basis.

Conversely, assume $\chi_\rho = \chi_\sigma$. By the multiplicity formula, for any irreducible representation ρ_λ,

$$\langle \chi_\rho, \chi_\lambda \rangle_G = \langle \chi_\sigma, \chi_\lambda \rangle_G,$$

so ρ and σ contain the same irreducible representations with the same multiplicities. Hence, their decompositions into irreducibles are equivalent (up to isomorphism and ordering), which implies $\rho \cong \sigma$. □

Remark IV.15. That two equivalent representations have the same character is obvious: they are related by a change of basis, so their matrices are conjugate, and in particular have the same trace on each group element. What is *not* obvious is the converse — that if two representations have the same character, they must be equivalent. This is a nontrivial and powerful consequence of character theory.

To appreciate this, note that two matrices with the same trace need not be similar. For example,

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

both have trace 2 (and even the same eigenvalues), but they are not similar (equivalent): there is no invertible matrix S such that $SAS^{-1} = B$. (Indeed, they are already in Jordan canonical form — and their Jordan structures differ, so they are not similar [3].)

So, while trace equality does *not* determine matrix equivalence in general, it *does* determine equivalence of representations — provided we compare the trace $\mathrm{Tr}(\rho(g))$ for *every* group element $g \in G$.

We now introduce a useful formula relating the character of a representation to its multiplicities.

Lemma IV.16 (Norm of a character equals equals the sum of squared multiplicities)**.** *Let $\rho : G \to \mathrm{GL}(V)$ be a finite-dimensional representation of a finite group G, with character χ_ρ. Suppose $\rho \cong \bigoplus_{\lambda \in \widehat{G}} \rho_\lambda^{\oplus m_\lambda}$, where $\widehat{G}$ is the list of all inequivalent irreducible representations. Then the squared norm of χ_ρ equals the sum of squared multiplicities:*

$$\langle \chi_\rho, \chi_\rho \rangle_G = \frac{1}{|G|} \sum_{g \in G} |\chi_\rho(g)|^2 = \sum_{\lambda \in \widehat{G}} m_\lambda^2.$$

In particular, $\langle \chi_\rho, \chi_\rho \rangle_G$ it is a positive integer.

Proof. We have:

$$\chi_\rho = \sum_{\lambda \in \widehat{G}} m_\lambda \chi_\lambda.$$

Taking the inner product with itself and using orthonormality of the irreducible characters:

$$\langle \chi_\rho, \chi_\rho \rangle_G = \left\langle \sum_\lambda m_\lambda \chi_\lambda, \sum_\mu m_\mu \chi_\mu \right\rangle_G = \sum_{\lambda,\mu} m_\lambda m_\mu \langle \chi_\lambda, \chi_\mu \rangle_G = \sum_\lambda m_\lambda^2,$$

since $\langle \chi_\lambda, \chi_\mu \rangle_G = \delta_{\lambda\mu}$. □

This gives us a remarkably efficient test for irreducibility:

Theorem IV.17 (Testing irreducibility using characters)**.** *Let $\rho : G \to \mathrm{GL}(V)$ be a finite-dimensional representation of a finite group G, with character χ_ρ. Then ρ is irreducible if and only if*

$$\langle \chi_\rho, \chi_\rho \rangle_G = 1.$$

Proof. From the previous lemma, we know that

$$\langle \chi_\rho, \chi_\rho \rangle_G = \sum_\lambda m_\lambda^2,$$

where $m_\lambda \in \mathbb{N}$ are the multiplicities of irreducible representations in the decomposition of ρ.

If ρ is irreducible, then there is a unique λ such that $m_\lambda = 1$ and all others vanish, so the sum is 1.

Conversely, if the sum equals 1, then only one m_λ can be nonzero and equals 1, which means ρ is isomorphic to an irreducible representation ρ_λ, hence irreducible. □

[3] Over $\mathbb{C}$, two matrices are similar if and only if they have the same Jordan block structure.

C. Examples and applications

We have seen a simple and effective criterion to check whether a representation is irreducible. Previously, to verify irreducibility, especially for higher-dimensional representations, one had to search for proper invariant subspaces — a process that could be computationally involved. Now, we have a concrete method:

$$\rho \text{ is irreducible} \quad \Longleftrightarrow \quad \langle \chi_\rho, \chi_\rho \rangle_G = 1.$$

We see now an example.

Example IV.18 (Standard representation of S_3)**.** Let $\rho : S_3 \to \mathrm{GL}(\mathbb{C}^3)$ be the permutation representation acting on the basis $\{|0\rangle, |1\rangle, |2\rangle\}$, defined by

$$\rho(\sigma)|i\rangle = |\sigma(i)\rangle .$$

Equivalently, in operator form:

$$\rho(\sigma) = \sum_{i=0}^{2} |\sigma(i)\rangle \langle i| .$$

We want to decompose this representation into irreducibles.

- **Step 1.** The vector $|v\rangle = |0\rangle + |1\rangle + |2\rangle$ is invariant under all permutations:

$$\rho(\sigma)|v\rangle = |\sigma(0)\rangle + |\sigma(1)\rangle + |\sigma(2)\rangle = |0\rangle + |1\rangle + |2\rangle = |v\rangle .$$

  So $\mathbb{C}|v\rangle$ carries the trivial representation.

- **Step 2.** Define the 2-dimensional orthogonal complement subspace

$$W := \{a|0\rangle + b|1\rangle + c|2\rangle \mid a+b+c=0\} .$$

  This is also an invariant subspace, since it is orthogonal to an invariant subspace.

- **Step 3.** Note that the character of the permutation representation $\chi_\rho = \mathrm{Tr}(\rho(\sigma)) = \sum_{i=0}^{2} \langle i|\sigma(i)\rangle$ counts the number of fixed points of σ:

$$\chi_\rho = \begin{cases} 3 & \text{on } e, \\ 1 & \text{on transpositions}, \\ 0 & \text{on 3-cycles}. \end{cases}$$

- We have $\chi_\rho = \chi_{\text{triv}} + \chi_W$. But, the trivial character is constantly 1, so subtracting we get:

$$\chi_W = \chi_\rho - \chi_{\text{triv}} = \begin{cases} 2 & \text{on } e, \\ 0 & \text{on transpositions}, \\ -1 & \text{on 3-cycles}. \end{cases}$$

- Compute the inner product:

$$\langle \chi_W, \chi_W \rangle = \frac{1}{6}(1 \cdot 2^2 + 3 \cdot 0^2 + 2 \cdot (-1)^2) = \frac{1}{6}(4+0+2) = 1.$$

  So $\rho|_W$ is irreducible.

- **Conclusion.** The permutation representation decomposes as

$$\rho = \rho_{\text{triv}} \oplus \rho_{\text{std}},$$

  where $\rho_{\text{std}} := \rho|_W$ is an irreducible 2-dimensional representation of S_3, called the standard representation.

Remark IV.19. We saw that another representation of S_3 is the *sign representation* ρ_{sgn}, defined by

$$\rho_{\mathrm{sgn}}(\sigma) = \begin{cases} +1 & \text{if } \sigma \text{ is even,} \\ -1 & \text{if } \sigma \text{ is odd.} \end{cases}$$

This is a 1-dimensional representation, and hence irreducible.

We also observed in the previous example that it does *not* appear in the decomposition of the permutation representation ρ, i.e., we saw that $\rho = \rho_{\mathrm{triv}} \oplus \rho_{\mathrm{std}}$. Thus, the sign representation has multiplicity zero in the permutation representation, as one can also check from the formula

$$\langle \chi_\rho, \chi_{\mathrm{sgn}} \rangle = \frac{1}{|S_3|} \sum_{g \in S_3} \chi_\rho(g)^* \chi_{\mathrm{sgn}}(g) = \frac{1}{6} (1 \cdot 3 \cdot 1 + 3 \cdot 1 \cdot (-1) + 2 \cdot 0 \cdot 1) = \frac{1}{6}(3 - 3 + 0) = 0.$$

1. *Commutant dimension via norm of the character*

Recall that the *commutant* (or *centralizer algebra*) of a representation $\rho : G \to \mathrm{GL}(V)$ is the set of all linear operators on V that commute with the action of the group:

$$\mathrm{Comm}(\rho) := \{T : V \to V \mid T\rho(g) = \rho(g)T \text{ for all } g \in G\}. \tag{64}$$

Proposition IV.20 (Dimension of the commutant via character norm)**.** *Let $\rho : G \to \mathrm{GL}(V)$ be a finite-dimensional representation of a finite group G, with character χ_ρ. Then the dimension of its commutant is given by*

$$\dim\left(\mathrm{Comm}(\rho)\right) = \langle \chi_\rho, \chi_\rho \rangle_G = \frac{1}{|G|} \sum_{g \in G} |\chi_\rho(g)|^2 \tag{65}$$

Proof. By Corollary III.28, we have

$$\dim(\mathrm{Comm}(\rho)) = \sum_{\lambda \in \widehat{G}} m_\lambda^2, \tag{66}$$

where m_λ are the multiplicities of the irreducible representations ρ_λ in ρ. On the other hand, Lemma IV.16 states that

$$\langle \chi_\rho, \chi_\rho \rangle_G = \sum_{\lambda \in \widehat{G}} m_\lambda^2. \tag{67}$$

Combining the two gives the result. □

Remark IV.21 (Frame potential)**.** In quantum information theory, this quantity also appears under the name of the *frame potential*, particularly when studying the representation $U^{\otimes k} : G \to \mathrm{U}(d^k)$, where $U : G \to \mathrm{U}(d)$ is a unitary representation of a finite group G.

In that case, the character of the tensor power representation is

$$\chi_{U^{\otimes k}}(g) = \mathrm{Tr}(U(g)^{\otimes k}) = (\mathrm{Tr}(U(g)))^k = (\chi_U(g))^k. \tag{68}$$

Therefore, the dimension of the commutant becomes

$$\dim\left(\mathrm{Comm}(U^{\otimes k})\right) = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Tr}(U(g))|^{2k}. \tag{69}$$

This expression appears frequently when analyzing how well a set of unitaries mimics the statistical properties of the Haar measure—the theory of unitary k-designs.

As we saw earlier, among the irreducible representations of a group G, there is always a particularly simple one: the *trivial representation* $\rho_{\text{triv}} : G \to \mathrm{GL}(\mathbb{C})$, defined by

$$\rho_{\text{triv}}(g) = 1 \qquad \text{for all } g \in G.$$

Given any representation $\rho : G \to \mathrm{GL}(V)$, one may be interested in isolating the subspace on which ρ acts trivially—that is, the isotypic component corresponding to ρ_{triv}. As we now show, this can be achieved by a simple averaging trick (we will later generalize this result to any isotypical-components).

Lemma IV.22 (Averaging projects onto the trivial isotypic component)**.** *Let $\rho : G \to \mathrm{GL}(V)$ be a finite-dimensional representation of a finite group G, with character χ_ρ. Define the averaging operator:*

$$\Pi_{\text{triv}} := \frac{1}{|G|} \sum_{g \in G} \rho(g).$$

Then:

1. *Π_{triv} is a G-equivariant projection: $\Pi_{\text{triv}}^2 = \Pi_{\text{triv}}$, and $\rho(h)\Pi_{\text{triv}} = \Pi_{\text{triv}}\rho(h) = \Pi_{\text{triv}}$ for all $h \in G$.*
2. *The image of Π_{triv} is the fixed subspace*
$$V^G := \{v \in V : \rho(g)v = v \text{ for all } g \in G\}.$$
3. *In the decomposition of ρ into irreducible components:*
$$\rho \cong \bigoplus_{\lambda \in \widehat{G}} \rho_\lambda^{\oplus m_\lambda},$$
where $\widehat{G}$ denotes the set of irreducible representations of G, the fixed subspace V^G coincides with the subspace $\mathbb{C}^{m_{\text{triv}}}$ where ρ acts as the trivial representation. That is,
$$V^G \cong \mathbb{C}^{m_{\text{triv}}},$$
where m_{triv} is the multiplicity of ρ_{triv} in ρ.
4. *This multiplicity is given by the character inner product:*
$$m_{\text{triv}} = \langle \chi_\rho, \chi_{\text{triv}} \rangle_G = \frac{1}{|G|} \sum_{g \in G} \chi_\rho(g).$$
5. *If ρ is unitary, then Π_{triv} is self-adjoint: $\Pi_{\text{triv}} = \Pi_{\text{triv}}^\dagger$.*

Proof. We prove point by point.

1. We have:
$$\Pi_{\text{triv}}^2 = \left(\frac{1}{|G|} \sum_{g \in G} \rho(g) \right)^2 = \frac{1}{|G|^2} \sum_{g,h \in G} \rho(g)\rho(h) = \frac{1}{|G|^2} \sum_{g,h \in G} \rho(gh)$$
$$= \frac{1}{|G|^2} \sum_{k \in G} \left(\sum_{g \in G} 1 \right) \rho(k) = \frac{1}{|G|^2} \cdot |G| \sum_{k \in G} \rho(k) = \frac{1}{|G|} \sum_{k \in G} \rho(k) = \Pi_{\text{triv}},$$
where we changed variables $k = gh$. So $\Pi_{\text{triv}}^2 = \Pi_{\text{triv}}$.
Moreover, for all $h \in G$,
$$\rho(h)\Pi_{\text{triv}} = \frac{1}{|G|} \sum_{g \in G} \rho(hg) = \frac{1}{|G|} \sum_{g' \in G} \rho(g') = \Pi_{\text{triv}},$$
where we changed variable $g' = hg$. Similarly $\Pi_{\text{triv}}\rho(h) = \Pi_{\text{triv}}$, so Π_{triv} is G-equivariant.

2. Let $v \in \mathrm{Im}(\Pi_{\mathrm{triv}})$, so $v = \Pi_{\mathrm{triv}}(w)$ for some $w \in V$. Then for any $h \in G$,

$$\rho(h)v = \rho(h)\Pi_{\mathrm{triv}}(w) = \Pi_{\mathrm{triv}}(w) = v,$$

so $v \in V^G$, and thus $\mathrm{Im}(\Pi_{\mathrm{triv}}) \subseteq V^G$.
Conversely, if $v \in V^G$, then $\rho(g)v = v$ for all $g \in G$, hence

$$\Pi_{\mathrm{triv}}(v) = \frac{1}{|G|}\sum_{g\in G}\rho(g)v = v,$$

and $v \in \mathrm{Im}(\Pi_{\mathrm{triv}})$, so $V^G \subseteq \mathrm{Im}(\Pi_{\mathrm{triv}})$. Therefore, $\mathrm{Im}(\Pi_{\mathrm{triv}}) = V^G$.

3. By Maschke's theorem, we may write

$$V \cong \bigoplus_{\lambda\in\widehat{G}} V_\lambda^{\oplus m_\lambda},$$

where each V_λ is the irreducible representation space of ρ_λ. The fixed subspace V^G consists only of vectors invariant under $\rho(g)$ for all g, and this happens only in the trivial representation. Thus,

$$V^G \cong \mathbb{C}^{m_{\mathrm{triv}}},$$

where m_{triv} is the multiplicity of ρ_{triv} in ρ.

4. We compute the multiplicity using the character inner product:

$$m_{\mathrm{triv}} = \langle \chi_\rho, \chi_{\mathrm{triv}}\rangle_G = \frac{1}{|G|}\sum_{g\in G}\chi_\rho(g)^* = \frac{1}{|G|}\sum_{g\in G}\chi_\rho(g^{-1}) = \frac{1}{|G|}\sum_{g\in G}\chi_\rho(g),$$

since $\chi_{\mathrm{triv}}(g) = 1$ for all $g \in G$.

5. If ρ is unitary, then $\rho(g)^\dagger = \rho(g^{-1})$ for all $g \in G$. Thus,

$$\Pi_{\mathrm{triv}}^\dagger = \left(\frac{1}{|G|}\sum_{g\in G}\rho(g)\right)^\dagger = \frac{1}{|G|}\sum_{g\in G}\rho(g)^\dagger = \frac{1}{|G|}\sum_{g\in G}\rho(g^{-1}) = \frac{1}{|G|}\sum_{g\in G}\rho(g) = \Pi_{\mathrm{triv}},$$

since $g \mapsto g^{-1}$ is a bijection of G. Hence $\Pi_{\mathrm{triv}} = \Pi_{\mathrm{triv}}^\dagger$.

□

Example IV.23 (Projector on the symmetric subspace)**.** In quantum information theory, this averaging operator often appears in the context of the *symmetric subspace* of $(\mathbb{C}^d)^{\otimes k}$, defined as the subspace of tensors invariant under all permutations:

$$\mathrm{Sym}^k(\mathbb{C}^d) := \left\{ |\psi\rangle \in (\mathbb{C}^d)^{\otimes k} \;\middle|\; V(\pi)\,|\psi\rangle = |\psi\rangle \text{ for all } \pi \in S_k \right\}.$$

Here, the symmetric group S_k acts on the tensor power space via the unitary representation

$$V : S_k \to \mathrm{U}(d^k), \qquad V(\pi)\left(|i_1\rangle \otimes \cdots \otimes |i_k\rangle\right) = \left|i_{\pi^{-1}(1)}\right\rangle \otimes \cdots \otimes \left|i_{\pi^{-1}(k)}\right\rangle.$$

The orthogonal projector onto the symmetric subspace is given by

$$P_{\mathrm{sym}} := \frac{1}{k!}\sum_{\pi\in S_k} V(\pi),$$

which is precisely the averaging operator over the group action, and a special case of the lemma above.

D. The regular representation contains them all (the irreps)

Let G be a finite group. We recall that the *regular representation* of G is the representation

$$\rho_{\text{reg}} : G \to \mathrm{GL}(V), \qquad V = \mathrm{span}\{|g\rangle \mid g \in G\},$$

defined by left multiplication:

$$\rho_{\text{reg}}(g)\,|h\rangle = |gh\rangle\,, \qquad \text{for all } g, h \in G.$$

This is a *faithful* representation, meaning that it is injective as a group homomorphism. That is:

Definition IV.24 (Faithful representation)**.** A representation $\rho : G \to \mathrm{GL}(V)$ is called *faithful* if the only group element that acts trivially on all of V is the identity, i.e., $\ker\rho \coloneqq \{g \in G \mid \rho(g) = I_V\} = \{e\}$.

In other words, ρ is faithful if it embeds G into the group of invertible matrices, preserving the full group structure. The regular representation is always faithful. Indeed, if $g \neq e$, then $\rho_{\text{reg}}(g)\,|e\rangle = |g\rangle \neq |e\rangle$, so $g \notin \ker\rho_{\text{reg}}$. Thus, $\ker\rho_{\text{reg}} = \{e\}$. [4]

We now compute the character of the regular representation.

Lemma IV.25. *The character χ_{reg} of the regular representation satisfies:*

$$\chi_{\text{reg}}(g) = \begin{cases} |G| & \text{if } g = e, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. By definition, we have:

$$\chi_{\text{reg}}(g) = \mathrm{Tr}(\rho_{\text{reg}}(g)) = \sum_{h\in G} \mathrm{Tr}(|gh\rangle\langle h|) = \sum_{h\in G} \delta_{gh,h} = \sum_{h\in G} \delta_{g,e} = \delta_{g,e}|G|.$$

□

Proposition IV.26 (The regular representation contains them all)**.** *The regular representation contains every irreducible representation of G. In particular, the multiplicity of any irreducible representation is equal to its dimension:*

$$\rho_{\text{reg}} \cong \bigoplus_{\lambda\in\widehat{G}} \rho_\lambda^{\oplus\dim(\rho_\lambda)},$$

where $\widehat{G}$ is the set of all irreducible representations of G. Equivalently, for each $\lambda \in \widehat{G}$, the multiplicity m_λ of ρ_λ satisfies $m_\lambda = \dim(\rho_\lambda)$.

Proof. By the character inner product formula, the multiplicity m_λ of ρ_λ in ρ_{reg} is

$$m_\lambda = \langle\chi_{\text{reg}}, \chi_\lambda\rangle_G = \frac{1}{|G|}\sum_{g\in G} \chi_{\text{reg}}(g)^*\chi_\lambda(g).$$

Using the formula for χ_{reg} from the previous proposition, only $g = e$ contributes, giving

$$m_\lambda = \frac{1}{|G|}\cdot|G|\cdot\chi_\lambda(e) = \chi_\lambda(e) = \dim(\rho_\lambda).$$

□

From the previous proposition, we get the following:

---

[4] However, being faithful does not mean surjective: $\rho_{\text{reg}}(G)$ is a proper subgroup of $\mathrm{GL}(V)$, consisting only of permutation matrices acting on the basis $\{|g\rangle\}$.

Corollary IV.27 (Weighted character sum and dimension sum rule)**.** *For every $g \in G$,*

$$\frac{1}{|G|} \sum_{\lambda \in \widehat{G}} d_\lambda \, \chi_\lambda(g) = \delta_{g,e}, \tag{70}$$

where $\chi_\lambda(g)$ is the character of the irreducible representation ρ_λ, and $d_\lambda := \dim(\rho_\lambda)$.

In particular, at $g = e$ this reduces to the so-called dimension sum rule*:*

$$|G| = \sum_{\lambda \in \widehat{G}} d_\lambda^2. \tag{71}$$

Proof. From the decomposition of the regular representation (Proposition IV.26), we get

$$\chi_{\text{reg}}(g) = \sum_{\lambda \in \widehat{G}} d_\lambda \, \chi_\lambda(g). \tag{72}$$

By Lemma IV.25, $\chi_{\text{reg}}(g) = |G| \, \delta_{g,e}$. Dividing both sides by $|G|$ yields the stated identity. Setting $g = e$ gives $\chi_\lambda(e) = d_\lambda$ and hence the dimension sum rule. □

Remark IV.28. A practical use of the dimension sum rule is as a completeness test when classifying irreducible representations. After finding several inequivalent irreps $\rho_{\lambda_1}, \ldots, \rho_{\lambda_k}$ with dimensions $d_{\lambda_1}, \ldots, d_{\lambda_k}$, one can check whether the list is complete by verifying

$$d_{\lambda_1}^2 + \cdots + d_{\lambda_k}^2 = |G|. \tag{73}$$

If the equality holds, then no further irreps exist (up to isomorphism); if it fails, some irreps are still missing.

E. Matrix elements of irreps as an orthonormal basis for functions on a group

We now return to the question raised after Theorem IV.8: do the matrix elements of (unitary) irreducible representations span the entire space of complex-valued functions $f : G \to \mathbb{C}$?

Let $\widehat{G}$ denote the set of equivalence classes of irreducible complex representations of G. For each $\lambda \in \widehat{G}$, let

$$\rho_\lambda : G \to \mathrm{GL}(V_\lambda)$$

be a representative irreducible representation, and set $d_\lambda := \dim V_\lambda$. Once a basis of V_λ is fixed (in such a way that the associated representation matrices are unitary), the *matrix elements* of ρ_λ are the functions

$$\rho_\lambda(\,\cdot\,)_{ij} : G \to \mathbb{C}, \qquad g \mapsto \big[\rho_\lambda(g)\big]_{ij}, \quad 1 \le i, j \le d_\lambda. \tag{74}$$

These are simply the coordinate functions of the matrices representing $\rho_\lambda(g)$ in the chosen basis.

Theorem IV.29 (Finite-group Peter–Weyl theorem: matrix elements form a basis)**.** *The set of elements of the (unitary) matrices assoicated to the inequivalent irreducible representations,*

$$\big\{ \rho_\lambda(\,\cdot\,)_{ij} \;\big|\; \lambda \in \widehat{G}, \; 1 \le i, j \le d_\lambda \big\},$$

forms an orthonormal basis of $\mathrm{Fun}(G, \mathbb{C})$ *with respect to the inner product*

$$\langle f, h \rangle_G := \frac{1}{|G|} \sum_{g \in G} f(g)^* \, h(g).$$

In particular, every function $f : G \to \mathbb{C}$ admits the unique expansion

$$f(g) = \sum_{\lambda \in \widehat{G}} \sum_{i,j=1}^{d_\lambda} c_{\lambda,ij} \, \rho_\lambda(g)_{ij}, \tag{75}$$

where the coefficients are given by

$$c_{\lambda,ij} = d_\lambda \, \big\langle \rho_\lambda(\,\cdot\,)_{ij}, f \big\rangle_G. \tag{76}$$

Proof. By Theorem IV.8, the matrix elements satisfy

$$\left\langle \rho_\lambda(\,\cdot\,)_{i_1 j_1}, \rho_\mu(\,\cdot\,)_{i_2 j_2} \right\rangle_G = \frac{1}{d_\lambda}\, \delta_{\lambda\mu}\, \delta_{i_1 i_2}\, \delta_{j_1 j_2}. \tag{77}$$

Thus they are orthogonal (and become orthonormal upon rescaling by $\sqrt{d_\lambda}$ if desired), hence linearly independent. The total number of these functions is

$$\sum_{\lambda \in \widehat{G}} d_\lambda^2. \tag{78}$$

By the dimension sum rule (Corollary IV.27),

$$\sum_{\lambda \in \widehat{G}} d_\lambda^2 = |G|,$$

which is exactly the dimension of $\mathrm{Fun}(G, \mathbb{C})$ (Lemma IV.5). We therefore have an orthogonal set whose size equals the dimension of the space, so it must be an orthonormal basis. The formula for the coefficients follows immediately by taking the inner product of f with $\rho_\lambda(\,\cdot\,)_{ij}$ and using the orthogonality relation of such matrix elements. □

Remark IV.30 (Connection with the Fourier transform on finite groups)**.** Theorem IV.29 has the same form as a Fourier expansion of f over a "Fourier-like" basis of functions on G, namely the matrix elements of its irreducible representations. This is no coincidence: in a later section we will see that the coefficients $c_{\lambda,ij}$ are precisely the (nonabelian) Fourier coefficients of f, and that the expansion above is exactly the inverse Fourier transform on G, generalizing the familiar discrete Fourier transform (DFT) and its quantum version (QFT).

F. Irreducible characters as an orthonormal basis for class functions

We have seen that the matrix elements of irreducible representations form an orthonormal basis of $\mathrm{Fun}(G, \mathbb{C})$. We now show that irreducible characters form an orthonormal basis of the subspace of class functions. A useful preliminary fact is the following lemma, which describes the effect of summing the matrices of a representation against a class function.

Lemma IV.31 (Action of a class function on a representation)**.** *Let $f : G \to \mathbb{C}$ be a class function, and let $\rho : G \to \mathrm{GL}(V)$ be a representation of dimension d_ρ. Define*

$$P_f(\rho) := \sum_{g \in G} f(g)\, \rho(g) \quad \in\ \mathbb{C}^{d_\rho \times d_\rho}.$$

Then:

1. *$P_f(\rho)$ commutes with $\rho(h)$ for all $h \in G$.*
2. *If V is irreducible, then*

$$P_f(\rho) = \lambda_\rho\, I_V, \qquad \lambda_\rho = \frac{1}{d_\rho} \sum_{g \in G} f(g)\, \chi_\rho(g) = \frac{|G|}{d_\rho}\, \langle f^*, \chi_\rho \rangle_G.$$

3. *If ρ is reducible with decomposition*

$$\rho \cong \bigoplus_{\lambda \in \widehat{G}} \rho_\lambda^{\oplus m_\lambda} = \bigoplus_{\lambda \in \widehat{G}} \left(I_{m_\lambda} \otimes \rho_\lambda\right),$$

then

$$P_f(\rho) = \bigoplus_{\lambda \in \widehat{G}} \lambda_{\rho_\lambda} I_{\rho_\lambda}^{\oplus m_\lambda} = \bigoplus_{\lambda \in \widehat{G}} \lambda_{\rho_\lambda}\, (I_{m_\lambda} \otimes I_{\rho_\lambda}),$$

where λ_{ρ_λ} is given by the formula in (2).

Proof. We have:

1. For any $h \in G$,

$$\rho(h)\, P_f(\rho)\, \rho(h)^{-1} = \sum_{g\in G} f(g)\, \rho(hgh^{-1}) = \sum_{g\in G} f(hgh^{-1})\, \rho(hgh^{-1}) = \sum_{g'\in G} f(g')\, \rho(g') = P_f(\rho), \tag{79}$$

   using that f is a class function and relabeling $g' = hgh^{-1}$.

2. If V is irreducible, then by Schur's lemma any operator commuting with ρ is a scalar multiple of the identity:

$$P_f(\rho) = \lambda_\rho\, I_V.$$

   Taking traces gives

$$d_\rho\, \lambda_\rho = \mathrm{Tr}\,\big(P_f(\rho)\big) = \sum_{g\in G} f(g)\ \mathrm{Tr}\,\big(\rho(g)\big) = \sum_{g\in G} f(g)\, \chi_\rho(g), \tag{80}$$

   hence

$$\lambda_\rho = \frac{1}{d_\rho} \sum_{g\in G} f(g)\, \chi_\rho(g) = \frac{|G|}{d_\rho}\, \langle f^*, \chi_\rho\rangle_G.$$

3. Writing $\rho \cong \bigoplus_{\lambda\in\widehat{G}} (I_{m_\lambda} \otimes \rho_\lambda)$,

$$\begin{aligned} P_f(\rho) &= \sum_{g\in G} f(g) \bigoplus_{\lambda\in\widehat{G}} (I_{m_\lambda} \otimes \rho_\lambda(g)) && (81)\\ &= \bigoplus_{\lambda} \sum_{g\in G} f(g)\ (I_{m_\lambda} \otimes \rho_\lambda(g)) && (82)\\ &= \bigoplus_{\lambda} I_{m_\lambda} \otimes \sum_{g\in G} f(g)\rho_\lambda(g) && (83)\\ &= \bigoplus_{\lambda} I_{m_\lambda} \otimes P_f(\rho_\lambda) && (84)\\ &= \bigoplus_{\lambda} I_{m_\lambda} \otimes \lambda_{\rho_\lambda} I_{\rho_\lambda} && (85)\\ &= \bigoplus_{\lambda} \lambda_{\rho_\lambda}\, (I_{m_\lambda} \otimes I_{\rho_\lambda}), && (86) \end{aligned}$$

   where the fourth line applies part (2) to each ρ_λ.

□

Theorem IV.32 (Characters as an orthonormal basis of class functions)**.** *The characters of all inequivalent irreducible representations form an orthonormal basis of* $\mathrm{Fun}_{\mathrm{class}}(G, \mathbb{C})$ *with respect to the inner product* $\langle \cdot, \cdot\rangle_G$*.*

Equivalently, for all inequivalent irreducible representations $\rho, \sigma \in \widehat{G}$*,*

$$\begin{aligned} \langle \chi_\rho, \chi_\sigma\rangle_G &= \delta_{\rho,\sigma}, && (87)\\ f(g) &= \sum_{\rho\in\widehat{G}} \langle f, \chi_\rho\rangle_G\, \chi_\rho(g), \quad \forall\, f \in \mathrm{Fun}_{\mathrm{class}}(G, \mathbb{C}). && (88) \end{aligned}$$

Proof. Irreducible characters are class functions by definition, and Theorem IV.9 shows they are mutually orthogonal, hence they form an orthonormal set in $\mathrm{Fun}_{\mathrm{class}}(G, \mathbb{C})$. It remains to prove they span this space.

Assume, towards a contradiction, that there exists a nonzero $f \in \mathrm{Fun}_{\mathrm{class}}(G, \mathbb{C})$ orthogonal to all irreducible characters:

$$\langle f, \chi_\lambda\rangle_G = 0 \qquad \forall\, \lambda \in \widehat{G}. \tag{89}$$

Let $\tilde{f} \coloneqq f^*$. By Lemma IV.31, for any representation ρ decomposed as

$$\rho \cong \bigoplus_{\lambda \in \widehat{G}} \rho_\lambda^{\oplus m_\lambda}, \tag{90}$$

the operator

$$P_{\tilde{f}}(\rho) \coloneqq \sum_{g \in G} \tilde{f}(g)\, \rho(g)$$

takes the form

$$P_{\tilde{f}}(\rho) = \bigoplus_{\lambda \in \widehat{G}} \lambda_{\rho_\lambda} \left(I_{m_\lambda} \otimes I_{\rho_\lambda}\right),$$

where

$$\lambda_{\rho_\lambda} = \frac{|G|}{d_{\rho_\lambda}} \langle (\tilde{f})^*, \chi_{\rho_\lambda} \rangle_G = \frac{|G|}{d_{\rho_\lambda}} \langle f, \chi_{\rho_\lambda} \rangle_G = 0. \tag{91}$$

Thus $P_{\tilde{f}}(\rho) = 0$ for all ρ. Applying this to the left regular representation

$$\rho_{\text{reg}} : G \to \mathrm{GL}\big(\mathrm{span}_{\mathbb{C}}\{|g\rangle\}_{g \in G}\big), \quad \rho_{\text{reg}}(h)\, |g\rangle = |hg\rangle\,,$$

we find for all $|h\rangle$:

$$0 = P_{\tilde{f}}(\rho_{\text{reg}})\, |h\rangle = \sum_{g \in G} \tilde{f}(g) \rho_{\text{reg}}(g)\ |h\rangle = \sum_{g \in G} \tilde{f}(g)\ |gh\rangle = \sum_{g \in G} \tilde{f}(gh^{-1})\ |g\rangle\,.$$

Taking the overlap with $\langle s|$ gives $\tilde{f}(sh^{-1}) = 0$ for all $s, h \in G$, hence $\tilde{f} \equiv 0$. So $f = (\tilde{f})^* \equiv 0$, a contradiction.

Therefore, the orthogonal complement of $\{\chi_\lambda\}_{\lambda \in \widehat{G}}$ in $\mathrm{Fun}_{\text{class}}(G, \mathbb{C})$ is $\{0\}$, so the irreducible characters span the space. Combined with orthonormality, they form an orthonormal basis. ☐

1. Number of conjugacy classes equals the number of inequivalent irreducible representations

The following theorem establishes a fundamental numerical relation in the representation theory of finite groups: the number of inequivalent irreducible representations is exactly the number of conjugacy classes. In particular, every finite group has only finitely many inequivalent irreducible representations.

Theorem IV.33 (Number of conjugacy classes equals the number of inequivalent irreducible representations)**.** *The number of of inequivalent irreducible complex representations of a finite group G is equal to the number of conjugacy classes of G:*

$$\#\{\textit{inequivalent irreducible representations of } G\} \;=\; \#\{\textit{conjugacy classes of } G\}.$$

Proof. Let $\widehat{G}$ denote the set of inequivalent irreducible complex representations of a finite group G. By Theorem IV.32, the irreducible characters $\{\chi_\rho : \rho \in \widehat{G}\}$ form a basis of $\mathrm{Fun}_{\text{class}}(G, \mathbb{C})$, hence $\#\widehat{G} = \dim \mathrm{Fun}_{\text{class}}(G, \mathbb{C})$. Lemma IV.5 states that this dimension equals the number of conjugacy classes, proving the claim. ☐

As an immediate corollary of the previous result, we see that a finite group must have a non-trivial structure in order to possess irreducible representations of dimension strictly larger than one: the group must be non-abelian.

Theorem IV.34. *A finite group G is abelian if and only if every irreducible complex representation of G has dimension* 1.

Proof. *(⇒) If G is abelian, all irreps are* 1*-dimensional.* This was already established earlier (see Corollary III.23), by using Schur's Lemma.

(⇐) If all irreps are 1*-dimensional, then G is abelian.* By the dimension sum rule (Corollary IV.27),

$$|G| = \sum_{\rho \in \widehat{G}} d_\rho^2.$$

By assumption $d_\rho = 1$ for all $\rho \in \widehat{G}$, so

$$|G| = \sum_{\rho \in \widehat{G}} 1 = |\widehat{G}|.$$

By Theorem IV.33, $|\widehat{G}|$ equals the number of conjugacy classes of G. Thus G has $|G|$ conjugacy classes. Since conjugacy classes are disjoint and their union is G, each class must have size 1. Therefore every element is only conjugate to itself, meaning $hgh^{-1} = g$ for all for all $g, h \in G$. Hence $hg = gh$ for all $g, h \in G$, and G is abelian. □

G. The second orthogonality relation for irreducible characters

The first orthogonality relation (Theorem IV.9) shows that distinct irreducible characters are orthogonal as functions on G with respect to the standard inner product. The second orthogonality relation is a complementary statement: it shows that, if we fix a conjugacy class and look at the list of character values it produces across all irreps, these lists are orthogonal to each other.

Theorem IV.35 (Second orthogonality relation for irreducible characters)**.** *Let $\{\rho_\lambda\}_{\lambda \in \widehat{G}}$ be a complete set of inequivalent irreducible complex representations of a finite group G. Let $C_1, \ldots, C_k$ be the conjugacy classes of G, with $|C_j|$ the size of C_j and $g_j \in C_j$ a fixed representative. Then, for any $1 \le i, j \le k$,*

$$\sum_{\lambda \in \widehat{G}} \chi_\lambda(g_i)^* \, \chi_\lambda(g_j) = \frac{|G|}{|C_i|} \, \delta_{ij}.$$

Proof. From Theorem IV.32, the irreducible characters $\{\chi_\lambda\}_{\lambda \in \widehat{G}}$ form an orthonormal basis of $\mathrm{Fun}_{\mathrm{class}}(G, \mathbb{C})$. Hence, for the indicator function 1_{C_j} of the conjugacy class C_j,

$$1_{C_j}(g) = \sum_{\lambda \in \widehat{G}} \langle \chi_\lambda, 1_{C_j} \rangle_G \, \chi_\lambda(g). \tag{92}$$

Evaluating (92) at $g = g_i$ gives

$$\delta_{ij} = \sum_{\lambda \in \widehat{G}} \langle \chi_\lambda, 1_{C_j} \rangle_G \, \chi_\lambda(g_i). \tag{93}$$

Moreover,

$$\langle \chi_\lambda, 1_{C_j} \rangle_G = \frac{1}{|G|} \sum_{h \in G} \chi_\lambda(h)^* \, 1_{C_j}(h) = \frac{1}{|G|} \sum_{h \in C_j} \chi_\lambda(h)^* = \frac{|C_j|}{|G|} \, \chi_\lambda(g_j)^*. \tag{94}$$

Therefore,

$$\delta_{ij} = \frac{|C_j|}{|G|} \sum_{\lambda \in \widehat{G}} \chi_\lambda(g_j)^* \, \chi_\lambda(g_i), \tag{95}$$

and multiplying by $|G|/|C_j|$ yields the claimed formula. □

H. Projection onto an irreducible–isotypic component

In many applications it is useful to project onto a corresponding *isotypic component* — the direct sum of all copies of a given irreducible representation inside the representation. This construction is central in block–diagonalising a Hamiltonian, constructing symmetry–adapted bases, and, in quantum information, for tasks such as building projective measurements that respect a given symmetry (e.g., the so–called quantum Schur sampling [5, 6], which appears as a subroutine in algorithms for spectrum estimation or quantum state tomography).

Let $\widehat{G}$ denote the set of equivalence classes of irreducible representations of the finite group G. For each $\mu \in \widehat{G}$, write ρ_μ for a fixed representative of the class μ, $d_\mu = \dim \rho_\mu$ for its dimension, χ_μ for its character, and m_μ for the multiplicity of ρ_μ inside a given representation ρ.

Theorem IV.36 (Character projector)**.** *Let $\rho : G \to \mathrm{GL}(V)$ be any finite-dimensional representation with*

$$\rho \;\cong\; \bigoplus_{\mu\in\widehat{G}} \big(I_{m_\mu} \otimes \rho_\mu\big). \tag{96}$$

For a fixed $\lambda \in \widehat{G}$, define

$$\Pi_\lambda(\rho) \;:=\; \frac{d_\lambda}{|G|} \sum_{g\in G} \chi_\lambda(g)^*\, \rho(g). \tag{97}$$

Then:

1. *$\Pi_\lambda(\rho)$ is the identity on the λ-isotypic component and 0 on all other isotypic components:*

$$\Pi_\lambda(\rho) \;=\; \bigoplus_{\mu\in\widehat{G}} \delta_{\lambda\mu}\, \big(I_{m_\mu} \otimes I_{\rho_\mu}\big). \tag{98}$$

2. *In particular, $\Pi_\lambda(\rho)$ is a projector: $\Pi_\lambda(\rho)^2 = \Pi_\lambda(\rho)$, and $\Pi_\lambda(\rho)\,\Pi_\mu(\rho) = 0$ for $\lambda \neq \mu$.*
3. *The projectors resolve the identity:*

$$\sum_{\lambda\in\widehat{G}} \Pi_\lambda(\rho) \;=\; I_V. \tag{99}$$

4. *$\mathrm{Tr}\, \Pi_\lambda(\rho) = m_\lambda d_\lambda$ (so $\mathrm{rank}\,\Pi_\lambda(\rho) = m_\lambda d_\lambda$).*
5. *If ρ is unitary, then $\Pi_\lambda(\rho)$ is Hermitian.*

Proof. Apply Lemma IV.31 with $f = \chi_\lambda^*$. Part (3) of the lemma gives

$$\sum_{g\in G} \chi_\lambda(g)^*\, \rho(g) \;=\; \bigoplus_{\mu\in\widehat{G}} \lambda_{\rho_\mu}\, (I_{m_\mu} \otimes I_{\rho_\mu}), \qquad \lambda_{\rho_\mu} = \frac{|G|}{d_\mu}\, \langle \chi_\lambda, \chi_\mu\rangle_G. \tag{100}$$

By character orthogonality, $\langle \chi_\lambda, \chi_\mu\rangle_G = \delta_{\lambda\mu}$. Therefore

$$\sum_{g\in G} \chi_\lambda(g)^*\, \rho(g) \;=\; \frac{|G|}{d_\lambda}\, \big(I_{m_\lambda} \otimes I_{\rho_\lambda}\big), \tag{101}$$

and multiplying by $d_\lambda/|G|$ yields item (1). Items (2) and (3) follow immediately from the block form. For (4), $\mathrm{Tr}\,\Pi_\lambda(\rho) = \mathrm{Tr}(I_{m_\lambda} \otimes I_{\rho_\lambda}) = m_\lambda d_\lambda$. For (5), if ρ is unitary then $\rho(g)^\dagger = \rho(g^{-1})$ and $\chi_\lambda(g^{-1}) = \chi_\lambda(g)^*$, so $\Pi_\lambda(\rho)^\dagger = \Pi_\lambda(\rho)$. □

Remark IV.37. Lemma IV.22 is recovered as the special case of Theorem IV.36 obtained by taking the *trivial character* $\chi_{\mathrm{triv}}(g) \equiv 1$ (with $d_{\mathrm{triv}} = 1$). Substituting $\chi_\lambda = \chi_{\mathrm{triv}}$ into the formula for $\Pi_\lambda(\rho)$ gives

$$\Pi_{\mathrm{triv}}(\rho) = \frac{1}{|G|} \sum_{g\in G} \rho(g), \tag{102}$$

which is precisely the averaging operator projecting onto the fixed subspace V^G of G-invariant vectors.

Remark IV.38 (Projector onto the antisymmetric subspace)**.** Recall from Example IV.23 that the symmetric group S_k acts on $(\mathbb{C}^d)^{\otimes k}$ via the unitary representation

$$V : S_k \to \mathrm{U}(d^k), \qquad V(\pi)\big(|i_1\rangle \otimes \cdots \otimes |i_k\rangle\big) = \big|i_{\pi^{-1}(1)}\big\rangle \otimes \cdots \otimes \big|i_{\pi^{-1}(k)}\big\rangle\,.$$

Choosing the trivial character $\chi_{\mathrm{triv}}(\pi) \equiv 1$ in Theorem IV.36 yields the symmetric-subspace projector P_{sym} from Example IV.23. The group S_k also has the *sign character*

$$\chi_{\mathrm{sgn}}(\pi) := \mathrm{sgn}(\pi) \in \{\pm 1\}.$$

Applying Theorem IV.36 with $\chi_\lambda = \chi_{\mathrm{sgn}}$ and $d_{\mathrm{sgn}} = 1$ yields

$$P_{\mathrm{antisym}} \;=\; \frac{1}{k!} \sum_{\pi\in S_k} \mathrm{sgn}(\pi)\, V(\pi),$$

the orthogonal projector onto the *antisymmetric subspace*

$$\wedge^k(\mathbb{C}^d) := \big\{ |\psi\rangle \in (\mathbb{C}^d)^{\otimes k} \;\big|\; V(\pi)\,|\psi\rangle = \mathrm{sgn}(\pi)\,|\psi\rangle \quad \forall \pi \in S_k \big\}\,.$$

I. The character table

We now package all irreducible character values of a group into a single square matrix: the *character table.*

Definition IV.39 (The character table of a Group)**.** Let G be a finite group with conjugacy classes $C_1, \ldots, C_k$ and a complete set of inequivalent irreducible characters $\chi_{\lambda_1}, \ldots, \chi_{\lambda_k}$ (recall that the number of conjugacy classes equals the number of inequivalent irreducible characters). The *character table* of G is the $k \times k$ matrix

$$\mathrm{CT}(G) := \begin{pmatrix} \chi_{\lambda_1}(g_1) & \chi_{\lambda_1}(g_2) & \cdots & \chi_{\lambda_1}(g_k) \\ \chi_{\lambda_2}(g_1) & \chi_{\lambda_2}(g_2) & \cdots & \chi_{\lambda_2}(g_k) \\ \vdots & \vdots & \ddots & \vdots \\ \chi_{\lambda_k}(g_1) & \chi_{\lambda_k}(g_2) & \cdots & \chi_{\lambda_k}(g_k) \end{pmatrix},$$

where each g_j is a fixed representative of C_j. Rows correspond to inequivalent irreducible representation, and columns correspond to conjugacy classes.

As a convention, we usually arrange the table so that:

- The first row corresponds to the trivial irreducible representation, whose character is identically 1.
- The first column corresponds to the conjugacy class of the identity ($g_1 = e$), so its entries $\chi_{\rho_i}(e)$ give the dimensions d_{ρ_i} of the irreps.

Remark IV.40. The orthogonality relations endow $\mathrm{CT}(G)$ with a precise structure:

- **Row orthogonality:** By the first orthogonality relation (Theorem IV.9),

$$\sum_{j=1}^{k} \frac{|C_j|}{|G|} \chi_{\lambda_a}(g_j)^* \chi_{\lambda_b}(g_j) = \delta_{ab}.$$

  Thus, the rows of $\mathrm{CT}(G)$ are orthonormal in $\mathbb{C}^k$ when the j-th coordinate is weighted by $\sqrt{|C_j|/|G|}$.

- **Column orthogonality:** By the second orthogonality relation (Theorem IV.35),

$$\sum_{a=1}^{k} \chi_{\lambda_a}(g_i)^* \chi_{\lambda_a}(g_j) = \frac{|G|}{|C_i|} \delta_{ij}.$$

  Thus, the columns of $\mathrm{CT}(G)$ are orthogonal in $\mathbb{C}^k$ and have squared norm $\frac{|G|}{|C_i|}$.

Consequently, after scaling the j-th column by $\sqrt{|C_j|/|G|}$, the character table becomes a unitary matrix.

From the character table one can extract very useful information about the group and its representations.

Remark IV.41 (What the character table reveals at a glance)**.** Let G be a finite group with conjugacy classes $C_1, \ldots, C_k$ and inequivalent irreducible characters $\{\chi_\lambda\}_{\lambda \in \widehat{G}}$. Then:

1. **Irrep dimensions.** From the first column (corresponding to the identity class), we read

$$d_\lambda := \dim(\rho_\lambda) = \chi_\lambda(e). \tag{103}$$

2. **Group order (dimension sum rule).** Using the first column and Corollary IV.27,

$$|G| = \sum_{\lambda \in \widehat{G}} d_\lambda^2. \tag{104}$$

3. **Conjugacy class sizes.** For a representative $g_j \in C_j$, the second orthogonality relation gives

$$\sum_{\lambda \in \widehat{G}} \left|\chi_\lambda(g_j)\right|^2 = \frac{|G|}{|C_j|}, \tag{105}$$

   hence

$$|C_j| = \frac{|G|}{\sum_\lambda |\chi_\lambda(g_j)|^2}. \tag{106}$$

4. **Decomposition multiplicities.** If χ is the character of any finite-dimensional representation of G, then the multiplicity of ρ_λ in it is

$$m_\lambda = \langle \chi, \chi_\lambda \rangle_G = \frac{1}{|G|} \sum_{g \in G} \chi(g)^* \, \chi_\lambda(g). \tag{107}$$

5. **Detecting abelian groups.** G is abelian if and only if all $d_\lambda = 1$, i.e. the first column of the character table is entirely 1's.

Thus, the character table gives us a compact summary of deep structural properties of the group G. But what if the character table is not given to us? In that case, one can often reconstruct it by systematically applying the character theory tools developed so far. One starts by determining all conjugacy classes and their sizes, which already fixes the number of rows and columns of the table. The dimension sum rule

$$|G| = \sum_{\lambda \in \widehat{G}} d_\lambda^2, \quad d_\lambda \in \mathbb{Z}_{\geq 1},$$

then constrains the possible dimensions of the irreps. From here, one can try to fill in certain entries: the first row for the trivial representation (all 1's), the first column containing the dimensions, and the values of one-dimensional characters, which must be roots of unity[5]. The orthogonality relations for rows can then be used to solve for many of the remaining unknown entries, and the column orthogonality relations provide further constraints and consistency checks. In many small groups this process determines the entire table.

1. *Examples*

Example IV.42 (Reconstructing the character table of S_3)**.** The symmetric group S_3 has three conjugacy classes:

$$C_1 = \{e\}, \quad C_2 = \{(12), (13), (23)\}, \quad C_3 = \{(123), (132)\},$$

with sizes 1, 3, and 2, respectively. Since there are three classes, there are three inequivalent irreps. The dimension sum rule gives

$$6 = d_1^2 + d_2^2 + d_3^2,$$

and with $d_1 = 1$ (trivial rep), the only possibility is $(d_1, d_2, d_3) = (1, 1, 2)$. The one-dimensional irreps are the trivial and the sign representation, which fixes the first two rows. (Recall that the sign representation $\mathrm{sgn} : S_3 \to \{\pm 1\}$ sends even permutations to 1 and odd permutations to -1.[6])

Row and column orthogonality then determine the 2-dimensional row, giving:

	C_1	C_2	C_3
χ_{triv}	1	1	1
χ_{sgn}	1	-1	1
χ_{std}	2	0	-1

Example IV.43 (Two-qubit Heisenberg Hamiltonian from S_2 characters)**.** Let X, Y, Z be the Pauli matrices and consider the isotropic two-qubit Heisenberg Hamiltonian

$$H = J\,(X \otimes X + Y \otimes Y + Z \otimes Z), \qquad J \in \mathbb{R}.$$

Let $\rho := \rho_{\mathrm{perm}}$ be the permutation representation of S_2 on $\mathbb{C}^2 \otimes \mathbb{C}^2$, where $\rho(e) = I \otimes I$ and $\rho((12))$ swaps the two tensor factors. The swap operator satisfies the identity $\rho((12)) = \frac{1}{2}(I \otimes I + X \otimes X + Y \otimes Y + Z \otimes Z)$, so the Hamiltonian can be rewritten as

$$H = J\,(2\,\rho((12)) - I \otimes I).$$

---

[5] If $\rho : G \to \mathbb{C}/\{0\}$ is one-dimensional, then $\rho(g)^{|g|} = \rho(g^{|g|}) = \rho(e) = 1$, so $\rho(g)$ is a $|g|$-th root of unity, where $|g|$ is the order of $g \in G$.

[6] Recall: an even permutation is a permutation that can be written as a product of an even number of transpositions; odd otherwise. If a permutation of n elements has m disjoint cycles (counting fixed points), it is even iff $n - m$ is even, and odd otherwise.

The character values of ρ are

$$\chi_\rho(e) = 4, \qquad \chi_\rho((12)) = 2.$$

From the S_2 character table

	e	(12)
χ_{triv}	1	1
χ_{sgn}	1	-1

the multiplicities

$$m_\lambda = \frac{1}{2}\sum_{g\in S_2} \chi_\lambda(g)^* \, \chi_\rho(g)$$

are $m_{\text{triv}} = 3$ and $m_{\text{sgn}} = 1$. Hence

$$\mathbb{C}^2 \otimes \mathbb{C}^2 \cong V_{\text{triv}}^{\oplus 3} \oplus V_{\text{sgn}}.$$

Since $\rho((12))$ acts as $+1$ on V_{triv} and -1 on V_{sgn}, the energy spectrum is

$$E_{\text{triv}} = J \quad (\text{deg. } 3), \qquad E_{\text{sgn}} = -3J \quad (\text{deg. } 1).$$

Thus, we have found the energy spectrum of H using just the S_2 character table.

J. Fourier analysis from representation theory

The link with classical Fourier analysis becomes most transparent if we begin with the simple case of the cyclic group $\mathbb{Z}_n$. We will see how the *discrete Fourier transform* arises naturally from expanding a function $f : \mathbb{Z}_n \to \mathbb{C}$ in the orthonormal basis given by the irreducible characters of the abelian group $\mathbb{Z}_n$. This viewpoint will then be generalized to define the Fourier transform on arbitrary finite groups.

1. The cyclic group and the discrete Fourier transform

Let us look at the cyclic group $\mathbb{Z}_n$ in detail. We begin by finding all of its irreducible representations.

Example IV.44 (Irreps of the cyclic group $\mathbb{Z}_n$)**.** Let $G = \mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ with addition modulo n. Since G is abelian, every complex irreducible representation is 1-dimensional (Theorem III.23). By the dimension sum rule,

$$\sum_{\rho\in\widehat{G}} d_\rho^2 = |G| = n, \tag{108}$$

and with $d_\rho = 1$ for all ρ, there must be exactly n inequivalent irreps.

The group $\mathbb{Z}_n$ is generated by the element 1, and in G we have

$$\underbrace{1 + 1 + \cdots + 1}_{n \text{ times}} = 0.$$

A 1-dimensional representation ρ is determined by $\rho(1)$. Applying ρ to the above relation yields

$$\rho(1)^n = \rho(0) = 1, \tag{109}$$

so $\rho(1)$ must be an n-th root of unity.

Let $\omega := e^{2\pi i/n}$. For each $k \in \{0, \ldots, n-1\}$ define

$$\rho_k(m) := \omega^{km}. \tag{110}$$

These are all 1-dimensional irreps, and $\rho_k \not\cong \rho_\ell$ if $k \neq \ell$ (since two 1-dimensional representation are equivalent if and only if they are the same function). Since they are 1-dimensional, their characters coincide with the representations:

$$\chi_k(m) = e^{2\pi i km/n}. \tag{111}$$

Example IV.45 (Characters as a basis for functions on $\mathbb{Z}_n$)**.** For a general finite group, characters form an orthonormal basis for the space of *class functions*. Since $\mathbb{Z}_n$ is abelian, every function $f : \mathbb{Z}_n \to \mathbb{C}$ is a class function, so the characters

$$\chi_k(m) = e^{2\pi i k m/n}, \quad k = 0, \dots, n-1,$$

form an orthonormal basis of $\mathrm{Fun}(\mathbb{Z}_n, \mathbb{C})$ with respect to

$$\langle h, f \rangle_{\mathbb{Z}_n} := \frac{1}{n} \sum_{m=0}^{n-1} h(m)^* f(m).$$

Thus any function f can be expanded uniquely as

$$f(m) = \sum_{k=0}^{n-1} \langle \chi_k, f \rangle_{\mathbb{Z}_n} \chi_k(m), \tag{112}$$

where the coefficients are

$$\widehat{f}(k) := \langle \chi_k, f \rangle_{\mathbb{Z}_n} = \frac{1}{n} \sum_{m=0}^{n-1} f(m)\, e^{-2\pi i k m/n}. \tag{113}$$

Substituting $\chi_k(m)$ back into the expansion gives

$$f(m) = \sum_{k=0}^{n-1} \widehat{f}(k)\, e^{2\pi i k m/n}. \tag{114}$$

This is exactly the *discrete Fourier transform* (possibly, up to a complex conjugation in the coefficient formula, which comes from the inner product convention).

2. *Fourier transform of class functions*

The $\mathbb{Z}_n$ example shows that characters can form an orthonormal basis for the space of functions on the group. For abelian groups, every function is a class function, so the character expansion applies to all of them, and the discrete Fourier transform emerges naturally. We now extend this idea to arbitrary finite groups, where characters form an orthonormal basis of the (generally smaller) space of class functions.

Definition IV.46 (Fourier transform of class functions via irreducible characters)**.** Let G be a finite group, and let $\{\chi_\rho\}_{\rho \in \widehat{G}}$ be the characters of its inequivalent irreducible complex representations. For a class function $f : G \to \mathbb{C}$, its *Fourier coefficient* at ρ is

$$\widehat{f}(\rho) := \langle \chi_\rho, f \rangle_G = \frac{1}{|G|} \sum_{g \in G} \chi_\rho(g)^* f(g), \tag{115}$$

where the inner product on functions is

$$\langle u, v \rangle_G := \frac{1}{|G|} \sum_{g \in G} u(g)^* v(g).$$

Theorem IV.47 (Fourier inversion and Plancherel)**.** *Let $f : G \to \mathbb{C}$ be a class function. Then:*

$$\text{(Inversion)} \quad f(g) = \sum_{\rho \in \widehat{G}} \widehat{f}(\rho)\, \chi_\rho(g), \tag{116}$$

$$\text{(Plancherel)} \quad \langle f, h \rangle_G = \sum_{\rho \in \widehat{G}} \widehat{f}(\rho)^*\, \widehat{h}(\rho). \tag{117}$$

Proof. By Theorem IV.9, $\{\chi_\rho\}_{\rho\in\widehat{G}}$ is an orthonormal basis of the space of class functions. Thus

$$f = \sum_{\rho\in\widehat{G}} \langle \chi_\rho, f\rangle_G \, \chi_\rho = \sum_{\rho\in\widehat{G}} \widehat{f}(\rho)\, \chi_\rho.$$

Evaluating at $g \in G$ gives the inversion formula. For Plancherel, expand both f and h in the $\{\chi_\rho\}$ basis:

$$\langle f, h\rangle_G = \left\langle \sum_\rho \widehat{f}(\rho)\, \chi_\rho, \ \sum_\sigma \widehat{h}(\sigma)\, \chi_\sigma \right\rangle_G = \sum_{\rho,\sigma} \widehat{f}(\rho)^* \, \widehat{h}(\sigma)\, \langle \chi_\rho, \chi_\sigma\rangle_G = \sum_\rho \widehat{f}(\rho)^* \, \widehat{h}(\rho).$$

□

3. *Fourier transform on non-abelian groups*

The character Fourier transform applies only to *class functions*, where each Fourier coefficient $\widehat{f}(\rho)$ is a single complex number for each irrep ρ. For an abelian group, every function is a class function, so this covers all $f : G \to \mathbb{C}$.

For general (non-abelian) groups, functions need not be constant on conjugacy classes. The appropriate generalization is the *non-abelian Fourier transform*, where the Fourier coefficient at ρ is a matrix.

Definition IV.48 (Non-abelian Fourier transform)**.** Let G be a finite group and $\widehat{G}$ a complete set of inequivalent irreducible unitary representations. For $f : G \to \mathbb{C}$, its *non-abelian Fourier coefficient* at $\rho \in \widehat{G}$ is the $d_\rho \times d_\rho$ matrix

$$\widehat{f}(\rho) := \frac{1}{|G|} \sum_{g\in G} f(g)\, \rho(g)^\dagger \quad \in \mathbb{C}^{d_\rho \times d_\rho}. \tag{118}$$

The collection $\{\widehat{f}(\rho)\}_{\rho\in\widehat{G}}$ is called the *non-abelian Fourier transform* of f.

By Theorem IV.8, the set of all matrix elements $\rho_{ij}(g)$, over all $\rho \in \widehat{G}$ and $1 \le i, j \le d_\rho$, is an *orthogonal* basis of $\mathrm{Fun}(G, \mathbb{C})$ with

$$\langle \rho_{ij}, \sigma_{k\ell}\rangle_G = \frac{\delta_{\rho,\sigma}\, \delta_{i,k}\, \delta_{j,\ell}}{d_\rho}.$$

Thus f has the expansion

$$f(g) = \sum_{\rho\in\widehat{G}} d_\rho \sum_{i,j=1}^{d_\rho} \langle \rho_{ij}, f\rangle_G \, \rho_{ij}(g), \tag{119}$$

where

$$\langle \rho_{ij}, f\rangle_G = \frac{1}{|G|} \sum_{x\in G} \rho_{ij}(x)^* \, f(x) = \left[\, \widehat{f}(\rho)\, \right]_{ji}.$$

Theorem IV.49 (Fourier inversion and Plancherel, non-abelian case)**.** *Let* $f, h \in \mathrm{Fun}(G, \mathbb{C})$*. Then:*

$$\text{(Inversion)} \quad f(g) = \sum_{\rho\in\widehat{G}} d_\rho \ \mathrm{Tr}\left(\widehat{f}(\rho)\, \rho(g)\right), \tag{120}$$

$$\text{(Plancherel)} \quad \langle f, h\rangle_G = \sum_{\rho\in\widehat{G}} d_\rho \ \mathrm{Tr}\left(\widehat{f}(\rho)^\dagger \, \widehat{h}(\rho)\right). \tag{121}$$

Proof. From the orthogonal basis property,

$$f(g) = \sum_{\rho\in\widehat{G}} d_\rho \sum_{i,j=1}^{d_\rho} \langle \rho_{ij}, f\rangle_G \, \rho_{ij}(g) = \sum_{\rho\in\widehat{G}} d_\rho \sum_{i,j=1}^{d_\rho} \left[\widehat{f}(\rho)\right]_{ji} [\rho(g)]_{ij}.$$

The sum over i, j is exactly $\mathrm{Tr}\left(\widehat{f}(\rho)\,\rho(g)\right)$, giving the inversion formula.

For Plancherel, expand both f and h in the above basis:

$$\langle f, h\rangle_G = \sum_{\rho,\sigma} d_\rho d_\sigma \sum_{i,j,k,\ell} \langle \rho_{ij}, f\rangle_G^* \,\langle \sigma_{k\ell}, h\rangle_G \,\langle \rho_{ij}, \sigma_{k\ell}\rangle_G.$$

By orthogonality of matrix elements,

$$\langle \rho_{ij}, \sigma_{k\ell}\rangle_G = \frac{\delta_{\rho,\sigma}\,\delta_{i,k}\,\delta_{j,\ell}}{d_\rho}.$$

This collapses the sum to

$$\langle f, h\rangle_G = \sum_{\rho\in\widehat{G}} d_\rho \sum_{i,j} \left[\widehat{f}(\rho)\right]_{ij}^* \left[\widehat{h}(\rho)\right]_{ij}.$$

Recognizing the Hilbert–Schmidt inner product, we obtain

$$\langle f, h\rangle_G = \sum_{\rho\in\widehat{G}} d_\rho \,\mathrm{Tr}\left(\widehat{f}(\rho)^\dagger\,\widehat{h}(\rho)\right).$$

□

Remark IV.50. The Fourier transform on the abelian group $\mathbb{Z}_n$ that we saw earlier is exactly the transformation implemented by the standard *quantum Fourier transform* (QFT) in quantum computing, which is a key ingredient in algorithms such as Shor's factoring algorithm. The non-abelian Fourier transform defined here is the natural generalization to arbitrary finite groups.

V. COMPACT GROUPS: GENERALIZING FINITE-GROUP REPRESENTATION THEORY

Up to this point, we have considered only finite groups. However, many of the structural results we have seen extend, with suitable modifications, to an important class of possibly infinite groups called *compact groups*. These include, for example, U(n), SU(n), and SO(n), which occur naturally in quantum information theory.

Informally, a compact group is one whose elements form a set that is both *bounded* (it fits in a finite region) and *closed* (it contains all its limit points), with multiplication and inverse operations continuous. It may have infinitely many elements, but there is no way to "go off to infinity" within the group. For a precise, formal definition — which requires some notions from topology and measure theory — we refer the reader, e.g., to [1, 12, 13].

Remark V.1 (Key facts for compact groups)**.** Many fundamental theorems for finite groups remain valid for compact groups if one replaces normalized sums over G by integrals with respect to the *Haar measure* μ:

- **Haar measure.** Every compact group G has a unique normalized probability measure μ that is invariant under both left and right multiplication:

$$\int_G f(hg)\,d\mu(g) = \int_G f(g)\,d\mu(g) = \int_G f(gh)\,d\mu(g), \quad \forall\, h \in G, \tag{122}$$

$$int_G 1\,d\mu(g) = 1 \tag{123}$$

  In formulas, one makes the replacement

$$\frac{1}{|G|}\sum_{g\in G} \quad \longrightarrow \quad \int_G d\mu(g).$$

- **Unitarizability and complete reducibility.** Let $\rho : G \to \mathrm{GL}(V)$ be a finite-dimensional complex representation, and let $\langle\cdot,\cdot\rangle$ be any Hermitian inner product on V. Define the averaged inner product

$$\langle v, w\rangle_G := \int_G \langle \rho(g)v, \rho(g)w\rangle\, d\mu(g). \tag{124}$$

  This is G–invariant, and in a suitable orthonormal basis all $\rho(g)$ are unitary. As in the finite case, this implies complete reducibility (Maschke's theorem remains valid).

- **Irreducible representations.** A compact group may have infinitely many inequivalent irreducible representations. For example:
  - SU(2) has irreps labeled by $j \in \{0, \frac{1}{2}, 1, \frac{3}{2}, \dots\}$ with dimension $2j+1$.
  - SO(3) has irreps labeled by $j \in \{0, 1, 2, \dots\}$, also with dimension $2j+1$.

- **Schur orthogonality.** For finite-dimensional irreps ρ and σ of G,

$$\int_G \rho_{ij}(g^{-1})\,\sigma_{k\ell}(g)\,d\mu(g) = \frac{1}{d_\rho}\,\delta_{\rho,\sigma}\,\delta_{i,k}\,\delta_{j,\ell}, \tag{125}$$

$$\int_G \chi_\rho(g)^*\,\chi_\sigma(g)\,d\mu(g) = \delta_{\rho,\sigma}. \tag{126}$$

- **Peter–Weyl theorem.** The matrix coefficients of all finite-dimensional unitary irreps of G form an orthogonal set. Moreover, finite linear combinations of these coefficients are dense in the space of continuous functions on G. For $G = \mathrm{SO}(3)$, the matrix elements are the spherical harmonics, which therefore form an orthogonal basis for functions on the sphere.

In summary, by replacing sums with integrals over the Haar measure, the core results of finite-group representation theory — unitarizability, complete reducibility, Schur's lemmas, orthogonality, and the Peter–Weyl theorem — extend directly to the compact-group setting.

VI. SCHUR–WEYL DUALITY

Schur–Weyl duality is a cornerstone of representation theory, with far-reaching applications in quantum information theory [4, 7]. Before presenting the duality in full generality, we begin with a particular case that already forms the basis of many of its applications: the characterization of the commutant of the tensor-power representation of the unitary group. Consider the Hilbert space

$$\mathcal{H} := (\mathbb{C}^d)^{\otimes k}. \tag{127}$$

Our goal is to determine the operators on $\mathcal{H}$ that commute with $U^{\otimes k}$ for every $U \in U(d)$. We will show that this commutant is exactly the linear span of the permutation operators $V(\pi)$, $\pi \in S_k$:

$$\mathrm{Comm}\big(\{U^{\otimes k} : U \in U(d)\}\big) \;=\; \mathrm{span}\{\, V(\pi) : \pi \in S_k \,\}. \tag{128}$$

A. Commutant of tensor-power unitaries: span of permutations

Let us start with some formal definitions.

Definition VI.1 (Tensor-power and permutation representations)**.** Let $\mathcal{H} = (\mathbb{C}^d)^{\otimes k}$.

- The *tensor-power representation* of $U(d)$ is

$$\rho : U(d) \to U(\mathcal{H}), \qquad \rho(U) := U^{\otimes k}. \tag{129}$$

- The *permutation representation* of S_k is

$$V : S_k \to U(\mathcal{H}), \qquad V(\pi)\, |v_1\rangle \otimes \cdots \otimes |v_k\rangle \;=\; \big|v_{\pi^{-1}(1)}\big\rangle \otimes \cdots \otimes \big|v_{\pi^{-1}(k)}\big\rangle\,. \tag{130}$$

Both are unitary representations:

$$\rho(U_1U_2) = \rho(U_1)\rho(U_2), \quad V(\pi\sigma) = V(\pi)V(\sigma),$$

and

$$\rho(U)^\dagger = \rho(U^\dagger), \quad V(\pi)^\dagger = V(\pi^{-1}).$$

Definition VI.2 (Commutant)**.** For a subset $\mathsf{S} \subseteq \mathrm{End}(V)$, the *commutant* is

$$\mathrm{Comm}(\mathsf{S}) := \{\, X \in \mathrm{End}(V) : [X, S] = 0 \text{ for all } S \in \mathsf{S} \,\}. \tag{131}$$

We start with an elementary observation: permutation operators belong to the commutant of the tensor-power representation $U^{\otimes k}$, and conversely $U^{\otimes k}$ belongs to the commutant of the permutation representation.

Lemma VI.3 (Commuting actions)**.** *For all $U \in U(d)$ and $\pi \in S_k$,*

$$V(\pi)\, U^{\otimes k} \;=\; U^{\otimes k}\, V(\pi). \tag{132}$$

Proof. It suffices to verify the identity on pure tensors and extend by linearity:

$$\begin{aligned} V(\pi)U^{\otimes k}\, |v_1 \cdots v_k\rangle &= V(\pi)\big(|Uv_1\rangle \otimes \cdots \otimes |Uv_k\rangle\big) && (133)\\ &= \big|Uv_{\pi^{-1}(1)}\big\rangle \otimes \cdots \otimes \big|Uv_{\pi^{-1}(k)}\big\rangle && (134)\\ &= U^{\otimes k}\big(\big|v_{\pi^{-1}(1)}\big\rangle \otimes \cdots \otimes \big|v_{\pi^{-1}(k)}\big\rangle\big) && (135)\\ &= U^{\otimes k} V(\pi)\, |v_1 \cdots v_k\rangle\,. && (136) \end{aligned}$$

□

From Lemma VI.3 we obtain

$$\mathrm{span}\{V(\pi) : \pi \in S_k\} \;\subseteq\; \mathrm{Comm}\big(\{U^{\otimes k} : U \in U(d)\}\big). \tag{137}$$

In the following theorem we prove the reverse inclusion, and so showing that the commutant of the tensor-power representation of the unitary group is exactly the linear span of the permutation operators.

Theorem VI.4 (Unitary commutant)**.** *For all $d, k \in \mathbb{N}$,*

$$\mathrm{Comm}\big(\{U^{\otimes k} : U \in U(d)\}\big) = \mathrm{span}\{\, V(\pi) : \pi \in S_k \,\}, \tag{138}$$

where $V(\pi)$ permutes tensor slots via

$$V(\pi)\,|i_1, \ldots, i_k\rangle = \big|i_{\pi^{-1}(1)}, \ldots, i_{\pi^{-1}(k)}\big\rangle\,. \tag{139}$$

Proof. We proceed in several steps.

Step 1 (Inclusion $\supseteq$). For every $U \in U(d)$ and $\pi \in S_k$,

$$V(\pi)\, U^{\otimes k}\, V(\pi)^\dagger = U^{\otimes k}, \tag{140}$$

since $V(\pi)$ merely permutes tensor slots. Thus $\mathrm{span}\{V(\pi) : \pi \in S_k\} \subseteq \mathrm{Comm}(\{U^{\otimes k}\})$.

We are left to prove the reverse inclusion, for this we require that a generic element in the commutant must commute with tensor powers of diagonal unitaries, computational basis permutations tensor powers, and Discrete Fourier Transform tensor powers.

Step 2 (Diagonal phase restriction). Write

$$Q = \sum_{I,J} Q_{I,J}\, |I\rangle\langle J|, \qquad I = (i_1, \ldots, i_k),\ J = (j_1, \ldots, j_k). \tag{141}$$

Let $D = \mathrm{diag}(z_1, \ldots, z_d)$ with $z_r \in U(1)$. Then

$$D^{\otimes k}|I\rangle = \Big(\prod_{r=1}^{d} z_r^{n_r(I)}\Big)|I\rangle, \tag{142}$$

where $n_r(I) = |\{\ell : i_\ell = r\}|$. Thus

$$D^{\otimes k}|I\rangle\langle J|D^{\dagger\otimes k} = \Big(\prod_{r=1}^{d} z_r^{n_r(I)-n_r(J)}\Big)\,|I\rangle\langle J|. \tag{143}$$

Commutation $D^{\otimes k} Q D^{\dagger\otimes k} = Q$ for all phases forces

$$Q_{I,J} \neq 0 \quad \Rightarrow \quad n_r(I) = n_r(J)\ \ \forall r. \tag{144}$$

Equivalently, I and J must contain the same multiset of symbols. So J is obtained from I by some permutation of slots. Hence

$$Q = \sum_{\substack{I,J:\\ J \text{ is a permutation of } I}} Q_{I,J}\, |I\rangle\langle J|. \tag{145}$$

Step 3 (Alphabet permutation restriction). Let $P \in S_d$ act as $P|r\rangle = |p(r)\rangle$. Then

$$P^{\otimes k}|I\rangle\langle J|P^{\dagger\otimes k} = |p(I)\rangle\langle p(J)|. \tag{146}$$

Commutation $P^{\otimes k} Q P^{\dagger\otimes k} = Q$ forces

$$Q_{I,J} = Q_{p(I),p(J)}. \tag{147}$$

So coefficients cannot depend on the actual alphabet symbols, only on the *equality pattern* $\mathfrak{p}(I)$, i.e. the partition of $\{1, \ldots, k\}$ into blocks of equal entries of I.

Thus there exist coefficients $c_{\pi,\mathfrak{p}}$ such that

$$Q = \sum_{\mathfrak{p}} \sum_{\pi \in S_k} c_{\pi,\mathfrak{p}}\, T_{\pi,\mathfrak{p}}, \qquad T_{\pi,\mathfrak{p}} := \sum_{I:\, \mathfrak{p}(I)=\mathfrak{p}} |I\rangle\langle \pi(I)|. \tag{148}$$

Step 4 (Avoiding repetitions). If I has repeated entries, then two different π may yield the same operator $|I\rangle\langle\pi(I)|$. For example, $(i_1, i_2) = (1, 1)$ is invariant under (12). This duplication is exactly the action of the stabilizer subgroup

$$\mathrm{Stab}(\mathfrak{p}) = \{\, s \in S_k : s(I) = I \text{ for all } I \text{ with } \mathfrak{p}(I) = \mathfrak{p} \,\}. \tag{149}$$

So distinct operators $T_{\pi,\mathfrak{p}}$ are in bijection with cosets $\pi \cdot \mathrm{Stab}(\mathfrak{p})$. Choose a set of representatives $\mathcal{R}(\mathfrak{p}) \subset S_k$. Then we may write

$$Q = \sum_{\mathfrak{p}} \sum_{\pi \in \mathcal{R}(\mathfrak{p})} c_{\pi,\mathfrak{p}}\, T_{\pi,\mathfrak{p}}. \tag{150}$$

Step 5 (Matrix elements of $T_{\pi,\mathfrak{p}}$). For basis states N, M,

$$\begin{aligned}\langle N|T_{\pi,\mathfrak{p}}|M\rangle &= \sum_{I:\,\mathfrak{p}(I)=\mathfrak{p}} \langle N|I\rangle\langle\pi(I)|M\rangle &(151)\\ &= \mathbf{1}\{\mathfrak{p}(N) = \mathfrak{p}\}\, \mathbf{1}\{M = \pi(N)\}. &(152)\end{aligned}$$

So

$$\langle N|Q|M\rangle = \sum_{\pi \in \mathcal{R}(\mathfrak{p}(N))} c_{\pi,\mathfrak{p}(N)}\, \mathbf{1}\{M = \pi(N)\}. \tag{153}$$

By the coset-representative choice, there is at most one π with $M = \pi(N)$. Thus

$$\langle N|Q|M\rangle = \begin{cases} c_{\pi,\mathfrak{p}(N)}, & M = \pi(N) \text{ for the unique } \pi \in \mathcal{R}(\mathfrak{p}(N)),\\ 0, & \text{otherwise.}\end{cases} \tag{154}$$

Step 6 (Fourier transform conjugation). Let U be the discrete Fourier transform

$$U|j\rangle \;=\; \tfrac{1}{\sqrt{d}} \sum_{x=0}^{d-1} \omega^{jx}|x\rangle, \qquad \omega = e^{2\pi i/d}. \tag{155}$$

The relevant matrix elements are

$$\langle x|U|j\rangle = \tfrac{1}{\sqrt{d}}\,\omega^{jx}, \qquad \langle j|U^{\dagger}|x\rangle = \tfrac{1}{\sqrt{d}}\,\omega^{-jx}. \tag{156}$$

For $N = (n_1, \dots, n_k)$ and $M = (m_1, \dots, m_k)$ we compute

$$\langle N|U^{\otimes k} T_{\pi,\mathfrak{p}} U^{\dagger\otimes k}|M\rangle = \sum_{I:\,\mathfrak{p}(I)=\mathfrak{p}} \langle N|U^{\otimes k}|I\rangle\, \langle\pi(I)|U^{\dagger\otimes k}|M\rangle. \tag{157}$$

First factor. We have

$$\langle N|U^{\otimes k}|I\rangle = \prod_{\ell=1}^{k} \langle n_\ell|U|i_\ell\rangle = \prod_{\ell=1}^{k} \tfrac{1}{\sqrt{d}}\,\omega^{i_\ell n_\ell} = d^{-k/2}\,\omega^{\sum_{\ell=1}^{k} i_\ell n_\ell}. \tag{158}$$

Second factor. Using $\pi(I) = (i_{\pi^{-1}(1)}, \dots, i_{\pi^{-1}(k)})$,

$$\begin{aligned}\langle\pi(I)|U^{\dagger\otimes k}|M\rangle &= \prod_{\ell=1}^{k} \langle i_{\pi^{-1}(\ell)}|U^{\dagger}|m_\ell\rangle = \prod_{\ell=1}^{k} \tfrac{1}{\sqrt{d}}\,\omega^{-i_{\pi^{-1}(\ell)} m_\ell} &(159)\\ &= d^{-k/2}\,\omega^{-\sum_{\ell=1}^{k} i_{\pi^{-1}(\ell)} m_\ell}. &(160)\end{aligned}$$

Product. Multiplying the two gives

$$\langle N|U^{\otimes k}|I\rangle\, \langle\pi(I)|U^{\dagger\otimes k}|M\rangle = d^{-k}\,\omega^{\sum_{\ell=1}^{k} i_\ell n_\ell - \sum_{\ell=1}^{k} i_{\pi^{-1}(\ell)} m_\ell}. \tag{161}$$

Equivalently,

$$= d^{-k}\,\omega^{\sum_{\ell=1}^{k} i_\ell\,(n_\ell - m_{\pi(\ell)})}. \tag{162}$$

Block parametrisation. If $\mathfrak{p}(I) = \mathfrak{p}$, then for each block $S \in \mathfrak{p}$ all entries i_ℓ with $\ell \in S$ are equal to some $x_S \in \{0, \ldots, d-1\}$. So the exponent becomes

$$\sum_{\ell=1}^{k} i_\ell(n_\ell - m_{\pi(\ell)}) = \sum_{S\in\mathfrak{p}} x_S\Big(\sum_{\ell\in S} n_\ell - \sum_{t\in\pi(S)} m_t\Big). \tag{163}$$

Summing over all I with pattern $\mathfrak{p}$ is equivalent to summing over each choice of block variables x_S. Hence

$$\langle N|U^{\otimes k}T_{\pi,\mathfrak{p}}U^{\dagger\otimes k}|M\rangle = d^{-k}\prod_{S\in\mathfrak{p}}\left(\sum_{x_S=0}^{d-1}\omega^{\,x_S\left(\sum_{\ell\in S} n_\ell - \sum_{t\in\pi(S)} m_t\right)}\right). \tag{164}$$

Geometric sum. For any integer a,

$$\sum_{x=0}^{d-1}\omega^{ax} = \begin{cases} d, & a \equiv 0 \pmod d, \\ 0, & \text{otherwise.}\end{cases} \tag{165}$$

Final result. Therefore,

$$\langle N|U^{\otimes k}T_{\pi,\mathfrak{p}}U^{\dagger\otimes k}|M\rangle = d^{|\mathfrak{p}|-k}\prod_{S\in\mathfrak{p}}\mathbf{1}\left\{\sum_{\ell\in S} n_\ell \equiv \sum_{t\in\pi(S)} m_t \pmod d\right\}. \tag{166}$$

Step 7 (Fourier comparison). We now compare the matrix elements of Q before and after Fourier conjugation. *LHS.* From Step 5 we know

$$\langle N|Q|M\rangle = \sum_{\pi\in\mathcal{R}(\mathfrak{p}(N))} c_{\pi,\mathfrak{p}(N)}\,\mathbf{1}\{M = \pi(N)\}. \tag{167}$$

By the coset-representative choice, there exists at most one $\pi \in \mathcal{R}(\mathfrak{p}(N))$ with $M = \pi(N)$. If such a π exists, denote it π_0. Then

$$\langle N|Q|M\rangle = \begin{cases} c_{\pi_0,\mathfrak{p}(N)}, & \text{if } M = \pi_0(N) \text{ for some } \pi_0 \in \mathcal{R}(\mathfrak{p}(N)), \\ 0, & \text{otherwise.}\end{cases} \tag{168}$$

RHS. From Step 6 we have

$$\langle N|U^{\otimes k}QU^{\dagger\otimes k}|M\rangle = \sum_{\mathfrak{p}}\sum_{\pi\in\mathcal{R}(\mathfrak{p})} c_{\pi,\mathfrak{p}}\,d^{|\mathfrak{p}|-k}\prod_{S\in\mathfrak{p}}\mathbf{1}\Big\{\sum_{\ell\in S} n_\ell \equiv \sum_{t\in\pi(S)} m_t \pmod d\Big\}. \tag{169}$$

Now assume that M and N have the same multiset of symbols. Then there exists a unique representative $\pi_0 \in \mathcal{R}(\mathfrak{p}(N))$ such that $M = \pi_0(N)$. For $(\pi, \mathfrak{p}) = (\pi_0, \mathfrak{p}')$, all the congruence conditions are satisfied identically, hence the product of indicators equals 1. For all other representatives $\pi \neq \pi_0$, the condition $M = \pi(N)$ is not met, so the product of indicators vanishes. Therefore

$$\langle N|U^{\otimes k}QU^{\dagger\otimes k}|M\rangle = \sum_{\mathfrak{p}} c_{\pi_0,\mathfrak{p}}\,d^{|\mathfrak{p}|-k}. \tag{170}$$

Comparison. Commutation requires

$$c_{\pi_0,\mathfrak{p}(N)} = \sum_{\mathfrak{p}} c_{\pi_0,\mathfrak{p}}\,d^{|\mathfrak{p}|-k}, \qquad \forall N. \tag{171}$$

Since the right-hand side is independent of the actual pattern $\mathfrak{p}(N)$, it follows that $c_{\pi_0,\mathfrak{p}}$ is independent of $\mathfrak{p}$. Denote this common value by c_{π_0}.

Step 8 (Collapse to permutation operators). From Step 7 we know that the coefficients are pattern-independent:

$$c_{\pi,\mathfrak{p}} = c_\pi, \qquad \forall\, \pi, \mathfrak{p}. \tag{172}$$

Hence

$$Q \;=\; \sum_{\mathfrak{p}} \sum_{\pi \in \mathcal{R}(\mathfrak{p})} c_\pi\, T_{\pi,\mathfrak{p}}. \tag{173}$$

Regrouping by π. For each fixed $\pi \in S_k$, collect all contributions where π was chosen as the representative in $\mathcal{R}(\mathfrak{p})$. Then

$$Q \;=\; \sum_{\pi \in S_k} c_\pi \Bigg(\sum_{\substack{\mathfrak{p}:\\ \pi \in \mathcal{R}(\mathfrak{p})}} T_{\pi,\mathfrak{p}} \Bigg). \tag{174}$$

Matrix elements of the inner sum. Fix $\pi \in S_k$ and basis states N, M. Then

$$\sum_{\substack{\mathfrak{p}:\\ \pi \in \mathcal{R}(\mathfrak{p})}} \langle N | T_{\pi,\mathfrak{p}} | M \rangle = \sum_{\substack{\mathfrak{p}:\\ \pi \in \mathcal{R}(\mathfrak{p})}} \mathbf{1}\{\mathfrak{p}(N) = \mathfrak{p}\}\, \mathbf{1}\{M = \pi(N)\}. \tag{175}$$

For given N, only the pattern $\mathfrak{p}(N)$ is relevant, and it belongs to the indexing set. Thus

$$\sum_{\substack{\mathfrak{p}:\\ \pi \in \mathcal{R}(\mathfrak{p})}} \langle N | T_{\pi,\mathfrak{p}} | M \rangle = \mathbf{1}\{M = \pi(N)\}. \tag{176}$$

This is precisely the matrix element of the permutation operator $V(\pi)$. Hence

$$\sum_{\substack{\mathfrak{p}:\\ \pi \in \mathcal{R}(\mathfrak{p})}} T_{\pi,\mathfrak{p}} \;=\; V(\pi). \tag{177}$$

Final expression. Therefore

$$Q \;=\; \sum_{\pi \in S_k} c_\pi V(\pi). \tag{178}$$

Step 9 (Conclusion). We have shown

$$\mathrm{Comm}\big(\{U^{\otimes k}\}\big) \subseteq \mathrm{span}\{V(\pi) : \pi \in S_k\}. \tag{179}$$

Combined with Step 1, this proves equality. □

a. Consequences for quantum information theory. Theorem VI.4 immediately implies a simple but powerful fact: any linear map that commutes with $U^{\otimes k}$ for all $U \in U(d)$ must be a linear combination of permutation operators. A particularly important example is the *k-th moment twirling channel*, defined by

$$\Phi_k(X) \coloneqq \int_{U(d)} U^{\otimes k} X\, U^{\dagger \otimes k}\, \mathrm{d}U,$$

where the integral is over the Haar measure on $U(d)$. Haar invariance ensures that $\Phi_k(X)$ commutes with $U^{\otimes k}$ for all U, and so by Theorem VI.4 it must take the form

$$\Phi_k(X) = \sum_{\pi \in S_k} c_\pi(X)\, V(\pi),$$

for certain coefficients $c_\pi(X) \in \mathbb{C}$.

This simple structural fact is the basis for many standard tools in quantum information theory, including the analysis of unitary designs, the Weingarten calculus, and Schur–Weyl–based protocols; see, e.g., [7, 14, 15].

B. Full Schur–Weyl duality

In Theorem VI.4 we established one direction: the commutant of the tensor-power representation $\{U^{\otimes k} : U \in U(d)\}$ is precisely the linear span of the permutation operators $\{V(\pi) : \pi \in S_k\}$.

We now turn to the converse: the commutant of the permutation representation $\{V(\pi) : \pi \in S_k\}$ is exactly the linear span of the tensor-power unitaries $\{U^{\otimes k} : U \in U(d)\}$.

Combining these results yields the more general powerful version of Schur–Weyl duality: the two actions $U^{\otimes k}$ and $V(\pi)$ commute, each forms the full commutant of the other, and together they give a simultaneous block decomposition of $(\mathbb{C}^d)^{\otimes k}$ into a direct sum of tensor products of two irreducible spaces — one carrying an irreducible representation of $U(d)$ and the other of S_k — with each group acting nontrivially only on its own factor.

We will now state the theorem.

Theorem VI.5 (Schur–Weyl duality)**.** *There exists a unitary decomposition*

$$\mathcal{H} \;\cong\; \bigoplus_{\lambda\in\Lambda} M_\lambda \otimes P_\lambda, \tag{180}$$

where Λ is a finite index set labeling the inequivalent irreducible components that occur in $(\mathbb{C}^d)^{\otimes k}$ under either action. For each $\lambda \in \Lambda$, M_λ is the $U(d)$–multiplicity space and P_λ is the S_k–multiplicity space.[7]

Moreover, for all $U \in U(d)$ and $\pi \in S_k$,

$$U^{\otimes k}\big|_{M_\lambda\otimes P_\lambda} \;=\; A_\lambda(U)\otimes I_{P_\lambda}, \qquad V(\pi)\big|_{M_\lambda\otimes P_\lambda} \;=\; I_{M_\lambda}\otimes \Pi_\lambda(\pi), \tag{181}$$

where each $A_\lambda : U(d) \to U(M_\lambda)$ and each $\Pi_\lambda : S_k \to U(P_\lambda)$ is an irreducible unitary representation. In particular,

$$\mathrm{Comm}\big(\{U^{\otimes k} : U \in U(d)\}\big) \;=\; \mathrm{span}\{V(\pi) : \pi \in S_k\}, \tag{182}$$

$$\mathrm{Comm}\big(\{V(\pi) : \pi \in S_k\}\big) \;=\; \mathrm{span}\{U^{\otimes k} : U \in U(d)\}. \tag{183}$$

To complete the proof, we must first prove two facts:

1. The commutant of the permutation operators $\{V(\pi)\}$ is exactly the span of $\{U^{\otimes k}\}$.
2. In the decomposition (180), the subrepresentations A_λ and Π_λ are irreducible.

The first will follow from the so-called double commutant theorem that we present below together with (182). The second will be shown by observing that any proper invariant subspace of M_λ (respectively P_λ) would lead to a nontrivial operator in the commutant of $U^{\otimes k}$ (respectively $V(\pi)$), contradicting the commutant identities above.

We will start with proving the so-called double commutant theorem.

1. *Double commutant theorem*

To prove the doulbe commutant theorem, we first need a lemma.

Lemma VI.6 (Block commutant)**.** *Let X, Y be finite-dimensional complex Hilbert spaces. Then*

$$\mathrm{Comm}\big(I_X \otimes \mathrm{End}(Y)\big) \;=\; \mathrm{End}(X)\otimes I_Y.$$

Proof. Fix an orthonormal basis $\{|i\rangle\}_{i=1}^n$ of Y and write $E_{ij} := |i\rangle\langle j|$. Every $T \in \mathrm{End}(X \otimes Y)$ has a unique expansion

$$T = \sum_{i,j=1}^{n} T_{ij}\otimes E_{ij}, \qquad T_{ij}\in \mathrm{End}(X).$$

The commutation relations $[T,\, I_X \otimes E_{pq}] = 0$ for all p, q are equivalent to

$$\sum_j T_{qj}\otimes E_{pj} \;=\; \sum_i T_{ip}\otimes E_{iq} \qquad (\forall\, p,q),$$

---

[7] A convenient choice is to take Λ to be the set of partitions $\lambda \vdash k$ with at most d parts (Young diagrams). With this identification, A_λ is the irreducible $U(d)$-representation of highest weight λ, and Π_λ is the Specht module S^λ of S_k. However, we will not need these details here.

using $E_{ab}E_{cd} = \delta_{bc}E_{ad}$. Since the matrix units $\{E_{rs}\}$ are linearly independent, comparing coefficients yields: (i) $T_{qj} = 0$ for all $j \neq q$; (ii) $T_{ip} = 0$ for all $i \neq p$; and (iii) $T_{pp} = T_{qq}$ for all p, q. Thus $T_{ij} = 0$ when $i \neq j$, and all diagonal blocks coincide with some $S \in \mathrm{End}(X)$, i.e., $T_{11} = T_{22} = \cdots = T_{nn} = S$. Hence

$$T = \sum_{j=1}^{n} S \otimes E_{jj} = S \otimes I_Y \in \mathrm{End}(X) \otimes I_Y,$$

which shows $\mathrm{Comm}(I_X \otimes \mathrm{End}(Y)) \subseteq \mathrm{End}(X) \otimes I_Y$. The reverse inclusion is immediate because $S \otimes I_Y$ commutes with $I_X \otimes B$ for every $B \in \mathrm{End}(Y)$. □

Proof. Fix an orthonormal basis $\{|i\rangle\}_{i=1}^{n}$ of Y and set $E_{ij} := |i\rangle\langle j|$. Every $T \in \mathrm{End}(X \otimes Y)$ has a unique expansion $T = \sum_{i,j} T_{ij} \otimes E_{ij}$ with $T_{ij} \in \mathrm{End}(X)$. Imposing $(I \otimes E_{pq})T = T(I \otimes E_{pq})$ for all p, q gives $\sum_j T_{qj} \otimes E_{pj} = \sum_i T_{ip} \otimes E_{iq}$. By linear independence of $\{E_{rs}\}$, for each p, q: $T_{qj} = 0$ for $j \neq q$, $T_{ip} = 0$ for $i \neq p$, and $T_{pp} = T_{qq}$ for all p, q. Thus $T = \sum_j T_{jj} \otimes E_{jj} = S \otimes I_Y$ with $S \in \mathrm{End}(X)$, proving the claim. □

Theorem VI.7 (Double commutant for compact-group unitary reps)**.** *Let G be a compact group and $\rho : G \to U(V)$ a finite-dimensional unitary representation. Let*

$$\mathcal{A} := \mathrm{span}\{\rho(g) : g \in G\} \;\subseteq\; \mathrm{End}(V). \tag{184}$$

Then

$$\mathrm{Comm}\big(\mathrm{Comm}(\mathcal{A})\big) \;=\; \mathcal{A}. \tag{185}$$

Proof. We have:

1. **Isotypic decomposition and the first commutant.** By complete reducibility of unitary reps of compact groups, there is a unitary decomposition

$$V \cong \bigoplus_{\alpha \in \Lambda} V_\alpha \otimes M_\alpha, \qquad \rho(g) \cong \bigoplus_{\alpha \in \Lambda} \rho_\alpha(g) \otimes I_{M_\alpha}, \tag{186}$$

   where the ρ_α are pairwise-inequivalent irreducible representations on V_α. By one of the main consequences of Schur's lemma we explored in the previous sections (see Proposition III.24), we get

$$\mathrm{Comm}(\mathcal{A}) = \bigoplus_{\alpha \in \Lambda} I_{V_\alpha} \otimes \mathrm{End}(M_\alpha). \tag{187}$$

2. **Second commutant via the block-commutant lemma.** Applying Lemma VI.6 to each block gives

$$\mathrm{Comm}\big(\mathrm{Comm}(\mathcal{A})\big) = \bigoplus_{\alpha \in \Lambda} \mathrm{End}(V_\alpha) \otimes I_{M_\alpha}. \tag{188}$$

3. **Identify the bicommutant with $\mathcal{A}$.** We want to show that $\mathcal{A} = \bigoplus_\alpha \mathrm{End}(V_\alpha) \otimes I_{M_\alpha}$. The inclusion

$$\mathcal{A} \;\subseteq\; \bigoplus_{\alpha} \mathrm{End}(V_\alpha) \otimes I_{M_\alpha} \tag{189}$$

   is immediate from the block form of $\rho(g)$. For the reverse inclusion, fix α and choose an orthonormal basis $\{|e_i\rangle\}_{i=1}^{d_\alpha}$ of V_α with $d_\alpha = \dim V_\alpha$. Using normalized Haar measure $\mathrm{d}g$ on G, define

$$X_{ij}^{(\alpha)} \;:=\; d_\alpha \int_G \overline{\rho_\alpha(g)_{ij}}\; \rho(g)\, \mathrm{d}g \;\in\; \mathcal{A}. \tag{190}$$

   On the $V_\beta \otimes M_\beta$ block we have

$$X_{ij}^{(\alpha)}\big|_{V_\beta \otimes M_\beta} = \Big(d_\alpha \int_G \overline{\rho_\alpha(g)_{ij}}\; \rho_\beta(g)\, \mathrm{d}g\Big) \otimes I_{M_\beta}. \tag{191}$$

By the Schur orthogonality relations for matrix coefficients,

$$\int_G \overline{\rho_\alpha(g)_{ij}}\ \rho_\beta(g)_{i'j'}\,\mathrm{d}g = \frac{\delta_{\alpha\beta}\,\delta_{ii'}\,\delta_{jj'}}{d_\alpha}. \tag{192}$$

Hence

$$d_\alpha \int_G \overline{\rho_\alpha(g)_{ij}}\ \rho_\beta(g)\,\mathrm{d}g = \delta_{\alpha\beta}\ |e_i\rangle\langle e_j|\,. \tag{193}$$

It follows that $X_{ij}^{(\alpha)}$ acts as $|e_i\rangle\langle e_j| \otimes I_{M_\alpha}$ on the α-block and vanishes on all others. Since $X_{ij}^{(\alpha)}$ is a linear combination (in fact, an integral) of $\rho(g)$'s, each matrix unit $|e_i\rangle\langle e_j| \otimes I_{M_\alpha}$ belongs to $\mathcal{A}$. As the $\{|e_i\rangle\langle e_j|\}_{i,j}$ span $\mathrm{End}(V_\alpha)$, we have

$$\mathrm{End}(V_\alpha) \otimes I_{M_\alpha}\ \subseteq\ \mathcal{A}. \tag{194}$$

Summing over α and comparing with (188) yields

$$\mathrm{Comm}\big(\mathrm{Comm}(\mathcal{A})\big) = \bigoplus_\alpha \mathrm{End}(V_\alpha) \otimes I_{M_\alpha} = \mathcal{A}. \tag{195}$$

□

Proposition VI.8 (Commutant of the permutation representation)**.** *Let $\mathcal{H} = (\mathbb{C}^d)^{\otimes k}$. Then*

$$\mathrm{Comm}\big(\{V(\pi) : \pi \in S_k\}\big) = \mathrm{span}\{\,U^{\otimes k} : U \in U(d)\,\}. \tag{196}$$

Proof. We have

$$\begin{aligned}\mathrm{Comm}\big(\{V(\pi) : \pi \in S_k\}\big) &= \mathrm{Comm}\big(\mathrm{span}\{V(\pi) : \pi \in S_k\}\big) &(197)\\ &= \mathrm{Comm}\big(\mathrm{Comm}(\{U^{\otimes k} : U \in U(d)\})\big) &(198)\\ &= \mathrm{span}\{\,U^{\otimes k} : U \in U(d)\,\}. &(199)\end{aligned}$$

In the first step we used the fact that $\mathrm{Comm}(S) = \mathrm{Comm}(\mathrm{span}(S))$ for any set of operators S. In the second step we used Theorem VI.4, which identifies $\mathrm{Comm}(\{U^{\otimes k} : U \in U(d)\})$ with $\mathrm{span}\{V(\pi) : \pi \in S_k\}$. In the third step we applied the double commutant theorem (Theorem VI.7). □

2. Irreducibility in the Schur–Weyl blocks

We have established that the commutant of the tensor-power representation is the span of permutation operators, and conversely, the commutant of the permutation representation is the span of tensor powers. To complete the proof of Schur–Weyl duality, it remains to show that, in the decomposition (180), each factor carries an *irreducible* representation of its respective group.

We first record a useful converse to Schur's lemma.

Proposition VI.9 (Converse to Schur's lemma)**.** *Let $U : G \to U(\mathcal{H})$ be a finite-dimensional unitary representation. Then*

$$\mathcal{H} \text{ is irreducible} \quad\Longleftrightarrow\quad \mathrm{Comm}\big(\{U(g) : g \in G\}\big) = \mathbb{C}\,I_{\mathcal{H}}.$$

Proof. ($\Rightarrow$) This is Schur's lemma.

($\Leftarrow$) Suppose $0 \neq W \neq \mathcal{H}$ is a nontrivial invariant subspace. Unitarity implies $W^\perp$ is also invariant. Let P_W be the orthogonal projector onto W. Then $U(g)P_W U(g)^\dagger = P_W$ for all g, so $P_W \in \mathrm{Comm}(\{U(g)\})$ but $P_W \notin \mathbb{C}I_{\mathcal{H}}$, contradicting the assumption. □

We can now prove that the two families of subrepresentations in (181) are irreducible.

Lemma VI.10 (Irreducibility in the S_k–decomposition)**.** *Let $\mathcal{H} = (\mathbb{C}^d)^{\otimes k}$ and first decompose $\mathcal{H}$ by fully reducing the S_k–action:*

$$\mathcal{H} \;\cong\; \bigoplus_{\lambda\in\Lambda} M_\lambda \otimes P_\lambda,$$

where $V(\pi)$ acts as

$$V(\pi)\big|_{M_\lambda\otimes P_\lambda} \;=\; I_{M_\lambda} \otimes \Pi_\lambda(\pi),$$

and each $\Pi_\lambda : S_k \to U(P_\lambda)$ is irreducible by construction of the decomposition. The $U^{\otimes k}$ action is block diagonal with

$$U^{\otimes k}\big|_{M_\lambda\otimes P_\lambda} \;=\; A_\lambda(U) \otimes I_{P_\lambda}.$$

Then both $A_\lambda : U(d) \to U(M_\lambda)$ and $\Pi_\lambda : S_k \to U(P_\lambda)$ are irreducible.

Proof. By how the decomposition is constructed, each Π_λ acts irreducibly on P_λ.o For A_λ, from (182) we have

$$\mathrm{Comm}\big(\{U^{\otimes k}\}\big)\Big|_{M_\lambda\otimes P_\lambda} = I_{M_\lambda} \otimes \mathrm{End}(P_\lambda).$$

This implies that the only operators on M_λ commuting with all $A_\lambda(U)$ are scalar multiples of the identity:

$$\{X \in \mathrm{End}(M_\lambda) : [X, A_\lambda(U)] = 0 \;\forall U\} = \mathbb{C}\, I_{M_\lambda}.$$

By Proposition VI.9, A_λ is irreducible. □

We now have all the ingredients to state and prove the full Schur–Weyl duality.

Theorem VI.11 (Full Schur–Weyl duality)**.** *Let $\mathcal{H} = (\mathbb{C}^d)^{\otimes k}$. There exists a unitary decomposition*

$$\mathcal{H} \;\cong\; \bigoplus_{\lambda\in\Lambda} M_\lambda \otimes P_\lambda, \tag{200}$$

such that:

- *$U^{\otimes k}$ acts as $A_\lambda(U) \otimes I_{P_\lambda}$ for some irreducible representation $A_\lambda : U(d) \to U(M_\lambda)$;*
- *$V(\pi)$ acts as $I_{M_\lambda} \otimes \Pi_\lambda(\pi)$ for some irreducible representation $\Pi_\lambda : S_k \to U(P_\lambda)$.*

Moreover, the commutants are

$$\mathrm{Comm}\big(\{U^{\otimes k} : U \in U(d)\}\big) = \mathrm{span}\{V(\pi) : \pi \in S_k\}, \tag{201}$$

$$\mathrm{Comm}\big(\{V(\pi) : \pi \in S_k\}\big) = \mathrm{span}\{U^{\otimes k} : U \in U(d)\}. \tag{202}$$

Proof. The commutant identities follow from Theorem VI.4 and Proposition VI.8. To obtain the decomposition, we first block-diagonalise the S_k-action:

$$\mathcal{H} \cong \bigoplus_{\lambda\in\Lambda} M_\lambda \otimes P_\lambda, \qquad V(\pi)\big|_{M_\lambda\otimes P_\lambda} = I_{M_\lambda} \otimes \Pi_\lambda(\pi),$$

where each Π_λ is irreducible by construction, and $U^{\otimes k}$ acts trivially on P_λ. Defining A_λ by

$$U^{\otimes k}\big|_{M_\lambda\otimes P_\lambda} = A_\lambda(U) \otimes I_{P_\lambda},$$

Lemma VI.10 shows A_λ is irreducible. □

C. Applications in quantum information

Schur–Weyl duality has several direct applications in quantum information theory [5, 7]. A key example is the simplification of measurements on i.i.d. quantum states.

D. Learning properties of a state from i.i.d. copies

Suppose we are given k i.i.d. copies of an unknown state ρ on $\mathbb{C}^d$, i.e. the joint state $\rho^{\otimes k}$ on $\mathcal{H} = (\mathbb{C}^d)^{\otimes k}$, and we wish to measure it to infer some property of ρ.

A measurement is described by a *positive operator-valued measure* (POVM), i.e. a family of positive semidefinite operators $\{E_x\}_{x\in\mathcal{X}} \subset \mathrm{End}(\mathcal{H})$ satisfying $\sum_{x\in\mathcal{X}} E_x = I_{\mathcal{H}}$. If outcome x occurs, the probability is

$$\mathrm{Prob}(x) = \mathrm{Tr}\big(E_x\, \rho^{\otimes k}\big).$$

Since $\rho^{\otimes k}$ is invariant under any permutation of its k subsystems, we may *permute-twirl* each POVM element without changing the measurement statistics:

$$\widetilde{E}_x := \frac{1}{k!} \sum_{\pi\in S_k} V(\pi)\, E_x\, V(\pi)^\dagger, \tag{203}$$

$$\mathrm{Tr}\big(\widetilde{E}_x\, \rho^{\otimes k}\big) = \mathrm{Tr}\big(E_x\, \rho^{\otimes k}\big). \tag{204}$$

Here $V(\pi)$ is the unitary that permutes tensor factors. Each $\widetilde{E}_x$ commutes with all $V(\pi)$, hence lies in

$$\mathrm{Comm}(\{V(\pi)\}) = \mathrm{span}\{U^{\otimes k} : U \in U(d)\}.$$

By Schur–Weyl duality, in the block decomposition

$$(\mathbb{C}^d)^{\otimes k} \;\cong\; \bigoplus_{\lambda\in\Lambda} M_\lambda \otimes P_\lambda, \tag{205}$$

each $\widetilde{E}_x$ acts as

$$\widetilde{E}_x \cong \bigoplus_{\lambda\in\Lambda} F_{\lambda,x} \otimes I_{P_\lambda}, \tag{206}$$

with arbitrary $F_{\lambda,x}$ on the M_λ factors (where $U(d)$ acts irreducibly) and identity on the P_λ factors (carrying the S_k action).

Hence, *without loss of generality*, for any task involving i.i.d. copies (e.g. full state tomography), one may choose POVM elements to be supported only on the M_λ factors.

E. Learning properties of the spectrum

Many important tasks in quantum information aim to determine properties of the *spectrum* (the eigenvalues) of a quantum state ρ, rather than its eigenvectors. Examples include estimating purity, reconstructing the entanglement spectrum, or fully learning the eigenvalues of ρ (also known as *spectrum estimation* [16]).

Since the spectrum is invariant under conjugation $\rho \mapsto U\rho U^\dagger$ by any $U \in U(d)$, these tasks satisfy the invariance property

$$\mathrm{Prob}(x \mid \rho) \;=\; \mathrm{Prob}\big(x \,\big|\, U\rho U^\dagger\big), \quad \forall\, U \in U(d),\ \forall\, x \in \mathcal{X}, \tag{207}$$

where $\mathrm{Prob}(x \mid \rho)$ denotes the probability of obtaining outcome x when measuring $\rho^{\otimes k}$ with a POVM $\{E_x\}_{x\in\mathcal{X}}$. In other words, the outcome x — which encodes the property of the spectrum that we wish to estimate — must be unchanged if ρ is conjugated by an arbitrary unitary.

The $U(d)$-invariance (207) allows us to replace each POVM element by its $U(d)$-*twirl*:

$$\widehat{E}_x := \int_{U(d)} U^{\otimes k}\, E_x\, U^{\dagger\otimes k}\, \mathrm{d}\mu_{\mathrm{Haar}}(U), \tag{208}$$

without changing the measurement statistics. Indeed,

$$\mathrm{Tr}\big(\widehat{E}_x\, \rho^{\otimes k}\big) = \int_{U(d)} \mathrm{Tr}\big(E_x\, (U^\dagger \rho U)^{\otimes k}\big)\, \mathrm{d}\mu_{\mathrm{Haar}}(U) \tag{209}$$

$$= \int_{U(d)} \mathrm{Prob}\big(x \,\big|\, U^\dagger \rho U\big)\, \mathrm{d}\mu_{\mathrm{Haar}}(U) \tag{210}$$

$$= \mathrm{Prob}(x \mid \rho), \tag{211}$$

where the last equality follows from (207).

By construction, $\widehat{E}_x$ commutes with all $U^{\otimes k}$ (by left- and right-invariance of the Haar measure), hence lies in

$$\mathrm{Comm}(\{U^{\otimes k}\}) = \mathrm{span}\{V(\pi) : \pi \in S_k\}.$$

In the Schur–Weyl block decomposition,

$$(\mathbb{C}^d)^{\otimes k} \;\cong\; \bigoplus_{\lambda\in\Lambda} M_\lambda \otimes P_\lambda,$$

this means

$$\widehat{E}_x \cong \bigoplus_{\lambda\in\Lambda} c_{\lambda,x}\, I_{M_\lambda} \otimes I_{P_\lambda},$$

with scalar coefficients $c_{\lambda,x}$.

Thus, for $U(d)$-invariant tasks, optimal POVMs may be taken to be *blockwise scalars* in the Schur–Weyl basis, acting trivially on both M_λ and P_λ except for an overall weight per block.

Positivity of the POVM and the completeness relation $\sum_x E_x = I$ translate into simple constraints on the coefficients $\{c_{\lambda,x}\}$:

$$c_{\lambda,x} \geq 0, \quad \forall\,\lambda \in \Lambda,\ \forall\, x \in \mathcal{X}, \tag{212}$$

$$\sum_{x\in\mathcal{X}} c_{\lambda,x} = 1, \quad \forall\,\lambda \in \Lambda. \tag{213}$$

In the special case of projective measurements, these coefficients are further restricted to

$$c_{\lambda,x} \in \{0,1\}, \quad \forall\,\lambda, x.$$

A particularly natural choice is $c_{\lambda,x} = \delta_{\lambda,x}$, which corresponds to a projective measurement onto the λ–isotypic component in the Schur–Weyl decomposition. In this case, the POVM element for outcome λ is the orthogonal projector

$$\Pi_\lambda \cong I_{M_\lambda} \otimes I_{P_\lambda}.$$

From the general representation theory result (Theorem IV.36), the projector onto the λ–isotypic component of the permutation representation

$$V : S_k \to U\big((\mathbb{C}^d)^{\otimes k}\big)$$

is given by

$$\Pi_\lambda = \frac{d_\lambda}{|S_k|} \sum_{\pi\in S_k} \chi_\lambda(\pi)^*\, V(\pi), \tag{214}$$

where $d_\lambda = \dim P_\lambda$ and χ_λ is its character. The probability of outcome λ when measuring $\rho^{\otimes k}$ is then

$$p(\lambda) = \mathrm{Tr}\big(\Pi_\lambda\, \rho^{\otimes k}\big) = \frac{d_\lambda}{k!} \sum_{\pi\in S_k} \chi_\lambda(\pi)^*\ \mathrm{Tr}\big(V(\pi)\rho^{\otimes k}\big), \tag{215}$$

where $\mathrm{Tr}\big(V(\pi)\rho^{\otimes k}\big) = \prod_{c\in\mathrm{Cycles}(\pi)} \mathrm{Tr}\big(\rho^{|c|}\big)$, and the product runs over the disjoint cycles c of π, with $|c|$ the length of each cycle. In particular, $p(\lambda)$ depends only on the spectrum of ρ through its power sums $\mathrm{Tr}(\rho^m)$.

This is exactly the *Schur measurement* used in *Schur sampling* protocols [5], where one first measures the irrep label λ (the symmetry type) and then optionally processes the residual state within the corresponding block.

In summary, the combination of permutation symmetry (from identical copies) and unitary invariance (from dependence only on the spectrum) forces the optimal POVM to lie in a highly symmetry-constrained subspace. This illustrates the power of exploiting symmetry in quantum information theory, and underlies the *Schur sampling* technique widely used in the literature [5, 7].

VII. TENSOR PRODUCT OF REPRESENTATIONS

Given two representations of the same group, we can combine them to form a new one acting on the tensor product space.

Definition VII.1 (Tensor product representation)**.** Let $\rho_1 : G \to \mathrm{GL}(V_1)$ and $\rho_2 : G \to \mathrm{GL}(V_2)$ be (finite-dimensional) representations of a group G over $\mathbb{C}$. The *tensor product representation* is the map

$$\rho_1 \otimes \rho_2 : G \to \mathrm{GL}(V_1 \otimes V_2), \qquad (\rho_1 \otimes \rho_2)(g) := \rho_1(g) \otimes \rho_2(g). \tag{216}$$

Lemma VII.2 (Basic properties of the tensor product representation)**.** *Let $\rho_1 : G \to \mathrm{GL}(V_1)$ and $\rho_2 : G \to \mathrm{GL}(V_2)$ be (finite-dimensional) complex representations. Then:*

- ***Representation property:*** *$\rho_1 \otimes \rho_2$ is a well-defined representation of G, and the identity acts as $I_{V_1} \otimes I_{V_2}$.*
- ***Character of a tensor product:*** *The character of $\rho_1 \otimes \rho_2$ is the pointwise product of the characters:*

$$\chi_{\rho_1 \otimes \rho_2}(g) = \chi_{\rho_1}(g)\, \chi_{\rho_2}(g), \qquad \forall g \in G. \tag{217}$$

- ***One representation 1-dimensional:*** *If $\dim V_1 = 1$ and ρ_2 is irreducible, then $\rho_1 \otimes \rho_2$ is irreducible. The same holds with the roles of ρ_1, ρ_2 swapped.*
- ***General reducibility:*** *If $\dim V_1 > 1$ and $\dim V_2 > 1$ are irreducible, then $\rho_1 \otimes \rho_2$ need not be irreducible.*

Proof. We have:

- For $g, h \in G$,

$$(\rho_1 \otimes \rho_2)(g)(\rho_1 \otimes \rho_2)(h) = (\rho_1(g)\rho_1(h)) \otimes (\rho_2(g)\rho_2(h)) = \rho_1(gh) \otimes \rho_2(gh) = (\rho_1 \otimes \rho_2)(gh), \tag{218}$$

  and $(\rho_1 \otimes \rho_2)(e) = I_{V_1} \otimes I_{V_2}$.
- This follows from the fact that $\mathrm{Tr}(A \otimes B) = \mathrm{Tr}(A)\ \mathrm{Tr}(B)$ for matrices A, B.
- If $\dim V_1 = 1$ with basis $|v\rangle$ and $\rho_1(g)\,|v\rangle = \lambda(g)\,|v\rangle$, then

$$(\rho_1 \otimes \rho_2)(g) = \lambda(g)\ |v\rangle\langle v| \otimes \rho_2(g).$$

  Hence $U \subseteq V_1 \otimes V_2$ is G-invariant iff $U = |v\rangle \otimes W$ with $W \subseteq V_2$ G-invariant. In particular, $\rho_1 \otimes \rho_2$ is irreducible iff ρ_2 is (and vice versa).
- Let $V = V_1 = V_2$ with $\dim V > 1$. The subspace

$$\mathrm{Sym}(V) := \mathrm{span}\{|v_1\rangle \otimes |v_2\rangle + |v_2\rangle \otimes |v_1\rangle : v_1, v_2 \in V\}$$

  is not the whole $V \otimes V$ (for example, any vector in $\mathrm{Sym}(V)$ is orthogonal to any vector of the form $|w_1\rangle \otimes |w_2\rangle - |w_2\rangle \otimes |w_1\rangle$ with $|w_1\rangle$ and $|w_2\rangle$ linearly independent). Moreover, $\mathrm{Sym}(V)$ is G-invariant: if $u = |v_1\rangle \otimes |v_2\rangle + |v_2\rangle \otimes |v_1\rangle$, then

$$(\rho(g) \otimes \rho(g))u = \rho(g)\,|v_1\rangle \otimes \rho(g)\,|v_2\rangle + \rho(g)\,|v_2\rangle \otimes \rho(g)\,|v_1\rangle \in \mathrm{Sym}(V).$$

  Since $\mathrm{Sym}(V)$ is a proper nonzero G-invariant subspace, $V \otimes V$ is reducible.

□

Thus, $\rho \otimes \rho$ is a representation of G, and therefore it can be decomposed as a direct sum of irreducible representations with certain multiplicities. This leads us to introduce the so–called *Clebsch–Gordan integers.*

Definition VII.3 (Clebsch–Gordan integers)**.** Let $\rho_\lambda, \rho_\mu, \rho_\nu$ be irreducible representations of G. The *Clebsch–Gordan integer* $N^{\nu}_{\lambda\mu}$ is the multiplicity of ρ_ν in the decomposition of the tensor product $\rho_\lambda \otimes \rho_\mu$:

$$\rho_\lambda \otimes \rho_\mu \ \cong\ \bigoplus_{\nu} N^{\nu}_{\lambda\mu}\, \rho_\nu, \tag{219}$$

with each $N^{\nu}_{\lambda\mu} \in \mathbb{Z}_{\geq 0}$.

Proposition VII.4 (Character formula for Clebsch–Gordan integers)**.** *Let $\chi_\lambda, \chi_\mu, \chi_\nu$ be the characters of $\rho_\lambda, \rho_\mu, \rho_\nu$, respectively. Then*

$$N^{\nu}_{\lambda\mu} \;=\; \langle \chi_\lambda \chi_\mu, \chi_\nu \rangle_G, \tag{220}$$

where $\chi_\lambda\chi_\mu$ denotes the pointwise product of characters and $\langle \cdot, \cdot \rangle_G$ is the usual character inner product. (Thus, we also have $N^{\nu}_{\lambda\mu} = N^{\nu}_{\mu\lambda}$.)

Proof. We have $\chi_{\lambda\otimes\mu} = \chi_\lambda\chi_\mu$. And by definition of $N^{\nu}_{\lambda\mu}$, we also have

$$\chi_{\lambda\otimes\mu} = \sum_{\nu'} N^{\nu'}_{\lambda\mu}\, \chi_{\nu'}. \tag{221}$$

Taking the inner product with χ_ν and using the orthonormality of irreducible characters,

$$\langle \chi_\lambda\chi_\mu, \chi_\nu \rangle_G = \sum_{\nu'} N^{\nu'}_{\lambda\mu}\, \langle \chi_{\nu'}, \chi_\nu \rangle_G = N^{\nu}_{\lambda\mu}. \tag{222}$$

□

Remark VII.5. From a quantum mechanics course, you might remember this example. Take $G = SU(2)$, the group of single-qubit rotations. The standard (fundamental) irreducible representation is $\rho : G \to \mathrm{GL}(\mathbb{C}^2)$, given by $\rho(U) = U$ acting on a single qubit in the computational basis $\{|0\rangle, |1\rangle\}$. This representation is irreducible, since no nontrivial subspace of $\mathbb{C}^2$ is invariant under all single-qubit rotations — this is clear by thinking in terms of the Bloch sphere, where any nonzero state vector can be rotated.

For two qubits, the group acts via the tensor product representation

$$\rho\otimes\rho : G \to \mathrm{GL}(\mathbb{C}^2\otimes\mathbb{C}^2), \qquad (\rho\otimes\rho)(U) = U\otimes U,$$

with respect to the computational basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. In this case, it is possible to show that the Clebsch–Gordan decomposition for $SU(2)$ is

$$\mathbb{C}^2\otimes\mathbb{C}^2 \;\cong\; \mathbb{C}^3\oplus\mathbb{C}^1,$$

where the 3-dimensional part is the symmetric (triplet) subspace and the 1-dimensional part is the antisymmetric (singlet) subspace. Here the Clebsch–Gordan integers (with irreps labelled by their dimensions) are $N^3_{2,2} = 1$ and $N^1_{2,2} = 1$.

It is important to note that the *Clebsch–Gordan coefficients* are not the same as these integers: the integers give the multiplicities in the decomposition, while the coefficients are the entries of the unitary change of basis from the computational basis to one adapted to this decomposition.

For $SU(2)$ it is standard to label irreps by a spin $j \in \{0, \frac{1}{2}, 1, \frac{3}{2}, \dots\}$, denoted V_j, with $\dim V_j = 2j+1$. Here $V_{1/2} = \mathrm{span}\{|0\rangle, |1\rangle\}$ is the spin-$\frac{1}{2}$ irrep. Then, the above decomposition

$$\mathbb{C}^2\otimes\mathbb{C}^2 \cong \mathbb{C}^3\oplus\mathbb{C}^1$$

corresponds to

$$V_{1/2}\otimes V_{1/2} \cong V_1\oplus V_0,$$

with $V_1 = \mathrm{span}\{|00\rangle, \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), |11\rangle\}$ (spin-1, triplet) and $V_0 = \mathrm{span}\{\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)\}$ (spin-0, singlet).

ACKNOWLEDGMENTS

I am grateful to Dmitry Grinko for valuable discussions and for pointing out a gap in an earlier version of the linear-algebraic proof I provided for the characterization of the unitary commutant (Schur–Weyl duality).

NOTATION (QUICK REFERENCE)

Symbol	Meaning
G	Finite group; identity e; operation written multiplicatively.
$\|G\|$	Order (number of elements) of G.
$H \leq G$	H is a subgroup of G.
$H \trianglelefteq G$	H is a normal subgroup ($gHg^{-1} = H$ for all $g \in G$).
$C(g)$	Conjugacy class of g: $C(g) = \{hgh^{-1} : h \in G\}$.
$\mathrm{Cl}(G)$	Set of conjugacy classes of G.
V	Complex vector space (representation space).
$\rho : G \to \mathrm{GL}(V)$	(Finite-dimensional) representation of G on V.
d_ρ	Dimension of ρ (i.e. $\dim V$).
χ_ρ	Character of ρ: $\chi_\rho(g) = \mathrm{Tr}(\rho(g))$.
$\widehat{G}$	A complete set of inequivalent irreducible representations (irreps).
d_λ	Dimension of irrep $\lambda \in \widehat{G}$.
m_λ	Multiplicity of irrep λ in a given representation ρ.
$C_1, \dots, C_k$	Conjugacy classes of G; $g_j \in C_j$ a fixed representative.
$\langle \psi, \phi \rangle_G$	Inner product on functions $G \to \mathbb{C}$: $\frac{1}{\|G\|} \sum_{g \in G} \psi(g)^* \phi(g)$.
$\mathrm{Comm}(\rho)$	Commutant: $\{T \in \mathrm{End}(V) : T\rho(g) = \rho(g)T \ \forall g \in G\}$.
V^G	Fixed subspace: $\{v \in V : \rho(g)v = v \ \forall g \in G\}$.
$\Pi_\lambda(\rho)$	Projector onto the λ-isotypic component of ρ.

BASICS OF REPRESENTATION THEORY — CHEAT SHEET

Groups. A *group* $(G, \cdot)$ satisfies closure, associativity, has an identity e, and inverses g^{-1} for all $g \in G$. The *order* of G is $|G|$.

A *subgroup* $H \leq G$ is a subset that is itself a group under the same operation.

A *left coset* of H is $gH := \{gh : h \in H\}$; a *right coset* is $Hg := \{hg : h \in H\}$. Cosets partition G; the number of cosets $[G : H]$ is the *index* of H in G.

A *normal subgroup* $H \trianglelefteq G$ satisfies $gH = Hg$ for all $g \in G$ (equivalently, $gHg^{-1} = H$). These are exactly the kernels of *group homomorphisms*.

A *group homomorphism* is a map $\varphi : G \to K$ between groups such that

$$\varphi(g_1 g_2) = \varphi(g_1)\,\varphi(g_2) \quad \forall\, g_1, g_2 \in G.$$

The *kernel* is $\ker \varphi = \{g \in G : \varphi(g) = e_K\}$, and it is always a normal subgroup.

The *conjugacy class* of g is $C(g) := \{hgh^{-1} : h \in G\}$. Two elements are conjugate if they lie in the same conjugacy class.

Representations. A representation is a homomorphism $\rho : G \to \mathrm{GL}(V)$. Over $\mathbb{C}$ and finite G, one can choose a basis where $\rho(g)$ are unitary. Irreducible $\iff$ no nontrivial G-invariant subspace. Equivalent reps: $\rho' = T\rho T^{-1}$.

Maschke: Every finite-dimensional ρ over $\mathbb{C}$ decomposes as

$$\rho \;\cong\; \bigoplus_{\lambda \in \widehat{G}} \rho_\lambda^{\oplus m_\lambda}, \quad V \;\cong\; \bigoplus_{\lambda \in \widehat{G}} \big(\mathbb{C}^{m_\lambda} \otimes V_\lambda\big). \tag{223}$$

Schur's Lemma. For irreps ρ, σ:

$$\rho \not\cong \sigma \;\Rightarrow\; \mathrm{Hom}_G(V_\rho, V_\sigma) = \{0\}, \tag{224}$$

$$\rho \cong \sigma \;\Rightarrow\; \mathrm{Hom}_G(V_\rho, V_\rho) = \mathbb{C} \cdot I. \tag{225}$$

Corollary: If G is abelian, all irreps are 1-dimensional.

Characters. $\chi_\rho(g) = \mathrm{Tr}(\rho(g))$ is a class function. Basic facts:

$$\chi_{\rho_1\oplus\rho_2}(g) = \chi_{\rho_1}(g) + \chi_{\rho_2}(g), \qquad \chi_\rho(g^{-1}) = \chi_\rho(g)^*, \qquad \chi_\rho(e) = d_\rho. \tag{226}$$

Orthogonality. (Row)

$$\langle \chi_\lambda, \chi_\mu \rangle_G = \frac{1}{|G|} \sum_{g\in G} \chi_\lambda(g)^* \chi_\mu(g) = \delta_{\lambda\mu}. \tag{227}$$

(Matrix elements) For unitary irrep λ of dim d_λ:

$$\big\langle (\rho_\lambda)_{ij}, (\rho_\mu)_{kl} \big\rangle_G = \frac{\delta_{\lambda\mu}\, \delta_{ik}\, \delta_{jl}}{d_\lambda}. \tag{228}$$

(Column) For $g_i \in C_i$, $g_j \in C_j$:

$$\sum_{\lambda\in\widehat{G}} \chi_\lambda(g_i)^* \chi_\lambda(g_j) = \frac{|G|}{|C_i|}\, \delta_{ij}. \tag{229}$$

Key formulas. Multiplicity:

$$m_\lambda = \langle \chi_\rho, \chi_\lambda \rangle_G = \frac{1}{|G|} \sum_{g\in G} \chi_\rho(g)^*\, \chi_\lambda(g). \tag{230}$$

Dimension sum:

$$|G| = \sum_{\lambda\in\widehat{G}} d_\lambda^2. \tag{231}$$

Projector onto λ-isotypic:

$$\Pi_\lambda(\rho) = \frac{d_\lambda}{|G|} \sum_{g\in G} \chi_\lambda(g)^*\, \rho(g), \quad \mathrm{rank}\, \Pi_\lambda = m_\lambda d_\lambda. \tag{232}$$

Commutant dimension:

$$\dim \mathrm{Comm}(\rho) = \langle \chi_\rho, \chi_\rho \rangle_G = \frac{1}{|G|} \sum_{g\in G} |\chi_\rho(g)|^2. \tag{233}$$

Regular representation:

$$\chi_{\mathrm{reg}}(g) = \begin{cases} |G|, & g = e, \\ 0, & g \neq e, \end{cases} \quad m_\lambda^{\mathrm{reg}} = d_\lambda. \tag{234}$$

Character tables (at a glance). A fundamental fact:

$$\#\{\text{conjugacy classes of } G\} = \#\{\text{inequivalent irreducible representations of } G\}.$$

This is why the character table is a square matrix. Rows $\leftrightarrow$ irreps, columns $\leftrightarrow$ conjugacy classes, $g_j \in C_j$:

$$\sum_j \frac{|C_j|}{|G|} \chi_\lambda(g_j)^*\, \chi_\mu(g_j) = \delta_{\lambda\mu}, \tag{235}$$

$$\sum_{\lambda\in\widehat{G}} \chi_\lambda(g_i)^*\, \chi_\lambda(g_j) = \frac{|G|}{|C_i|}\, \delta_{ij}. \tag{236}$$

[1] W. Fulton and J. Harris, *Representation Theory: A First Course* (Springer, 2004).
[2] J.-P. Serre, *Linear Representations of Finite Groups* (Springer, 1977).
[3] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2010).
[4] D. Bacon, I. L. Chuang, and A. W. Harrow, Efficient quantum circuits for schur and clebsch–gordan transforms, Physical Review Letters **97**, 170502 (2006).
[5] A. W. Harrow, Applications of coherent classical communication and the schur transform to quantum information theory (2005), arXiv:quant-ph/0512255 [quant-ph].
[6] M. Keyl, Fundamentals of quantum information theory, Physics Reports **369**, 431 (2002).
[7] M. Christandl, The structure of bipartite quantum states - insights from group theory and cryptography (2006), arXiv:quant-ph/0604183 [quant-ph].
[8] D. A. Varshalovich, A. N. Moskalev, and V. K. Khersonskii, *Quantum Theory of Angular Momentum* (World Scientific, 1988).
[9] M. S. Dresselhaus, G. Dresselhaus, and A. Jorio, *Group Theory: Application to the Physics of Condensed Matter* (Springer, 2007).
[10] M. Tinkham, *Group Theory and Quantum Mechanics* (Dover Publications, 2003).
[11] H. Georgi, *Lie Algebras in Particle Physics* (Westview Press, 1999).
[12] R. Goodman and N. R. Wallach, *Symmetry, Representations, and Invariants* (Springer, 2009).
[13] B. C. Hall, *Quantum Theory for Mathematicians* (Springer, 2013).
[14] A. W. Harrow, The church of the symmetric subspace (2013), arXiv:1308.6595 [quant-ph].
[15] A. A. Mele, Introduction to haar measure tools in quantum information: A beginner's tutorial, Quantum **8**, 1340 (2024).
[16] M. Keyl and R. F. Werner, Estimating the spectrum of a density operator, Physical Review A **64**, 10.1103/physreva.64.052311 (2001).