Finite groups and their representations for the working quantum theorist

Fenghuan He

Jalex Stark

flind2005@gmail.com, jalex@cs.berkeley.edu

February 28, 2021

This paper is under preparation. Some of the exposition contains irregular breaks, and some of the proofs are not complete.

Abstract

We present the theory of finite group representations from a quantum computer scientist's perspective. We largely follow [Ser77] in terms of mathematical content, but we depend more heavily on the theory of finite-dimensional Hilbert spaces. Much of this dependence is made implicit by the use of kets and bras. We give a self-contained introduction to the ket-bra calculus for the mathematicians in the audience.

As an application of the theory, we initiate the study of the nonabelian Fourier analysis of the qubit Pauli group. We demonstrate an implementation of the regular representation of the single qubit Pauli group as a three-qubit circuit of depth 1, and we give an explicit form for the nonabelian Fourier transform on this representation space. This seems interesting in its own right, and we suspect it may have applications to self-testing.

1 Preliminaries

Technically speaking, we only assume familiarity with sets, functions, and complex numbers at the high-school level. Some prior exposure to linear algebra and group theory may be helpful.

1.1 Notation

$\mathcal{H}$ will be reserved for Hilbert spaces.

ρ will be reserved for density matrices.

τ and σ will be reserved for group representations.

$\mathcal{U}(\mathcal{H})$ is the space of unitary operators on $\mathcal{H}$. $\mathcal{L}(\mathcal{H}_1, \mathcal{H}_2)$ is the space of linear operators from $\mathcal{H}_1$ to $\mathcal{H}_2$. We write $\mathcal{L}(\mathcal{H}) := \mathcal{L}(\mathcal{H}, \mathcal{H})$. $\mathcal{U}(\mathcal{H}_1, \mathcal{H}_2)$ is the space of isometries from $\mathcal{H}_1$ to $\mathcal{H}_2$. We write $\mathcal{U}(\mathcal{H}) := \mathcal{U}(\mathcal{H}, \mathcal{H})$.

A typical element of $\mathcal{L}(\mathcal{H}_1, \mathcal{H}_2)$ is T. A typical element of $\mathcal{L}(\mathcal{H})$ is A. A typical element of $\mathcal{U}(\mathcal{H}_1, \mathcal{H}_2)$ is V. A typical element of $\mathcal{U}(\mathcal{H})$ is U.

X, Z are Pauli matrices with $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. I is either the identity matrix or the identity linear operator, depending on context.

G will be a finite group and g will be a typical element of G.

δ_i^j is the *Kronecker delta*, equal to 1 if $i = j$ and 0 otherwise.

For a complex number $c \in \mathbb{C}$ with $c = a + bi$, we use $\overline{c}$ for its complex conjugate $a - bi$.

1.2 Group Theory

We work with several groups via their presentations. For the basic definitions of group, quotient group, etc. see any abstract algebra text, e.g. [DF04].

Definition 1.1. Let S be a set of letters. We denote by $\mathcal{F}(S)$ the *free group on* S. As a set, $\mathcal{F}(S)$ consists of all finite words made from $\left\{s, s^{-1} \,\middle|\, s \in S\right\}$ such that no ss^{-1} or $s^{-1}s$ appears as a substring for any s. The group law is given by concatenation and cancellation.

Definition 1.2 (Group presentation)**.** Let S be finite and R a finite subset of $\mathcal{F}(S)$. Then $G = \langle S : R \rangle$ is the *finitely presented group* generated by S with relations from R. Explicitly, $G = \mathcal{F}(S) / \langle R \rangle$, where / is used to denote the quotient of groups, and $\langle R \rangle$ denotes the subgroup generated by R. We say that an equation $w = w'$ is *witnessed by* R if $w'w^{-1}$ (or some cyclic permutation thereof) is a member of R.

We emphasize that in this work, we sometimes distinguish between two presentations of the same group. If $G = \langle S : R \rangle, G' = \langle S' : R' \rangle$ are two finitely presented groups, we reserve equality for the case $S = S'$ and $R = R'$, and in this case we'll say $G = G'$. We'll say that $G \cong G'$ if there is a group isomorphism between them.

Definition 1.3 (Cosets)**.** Given a group G, H a subgroup of G and a an element of G. The notation aH stands for the set of all products ah with h in H:

$$aH = \{g \in G | g = ah \text{ for some } h \text{ in } H \tag{1}$$

This set is called a *left coset* of H in G, the word "left" referring to the fact that the element a appears on the left. *Right coset* of H in G is defined similarly.

Definition 1.4 (Equivalence relation)**.** An *equivalence relation* on a set S is a relation that holds between certain pairs of elements of S. We may write it as $a \sim b$ and speak of it as *equivalence* of a and b. An equivalence relation is required to be:

1. *reflective*: For all a, $a \sim a$
2. *symmetric*: If $a \sim b$, then $b \sim a$.

3. *transitive*: If $a \sim b$ and $b \sim c$, then $a \sim c$.

Definition 1.5 (Conjugacy classes)**.** *conjugacy* is an equivalence relation on a group. Two group elements are conjugate, $a \sim b$, if $b = gag^{-1}$ for some group element g. It is easy to check that the conjugacy relation satisfies transitivity, symmetry, and reflection.

The *orbit* of x for conjugation is called the *conjugacy class* of x, and is often denoted by $C(x)$. It consists all of the conjugates gxg^{-1}.

$$C(x) = \{x' \in G | x' = gxg^{-1} \text{ for some } g \text{ in } G\} \tag{2}$$

A *class function* is a function on a group G that is constant on the conjugacy classes of G.

Definition 1.6 (Homomorphism)**.** Let G and G' be two groups. A *homomorphism* $\phi : G \to G'$ is a map from G to G' such that for all a and b in G:

$$\phi(ab) = \phi(a)\phi(b) \tag{3}$$

Intuitively, a homomorphism is a map that is compatible with the laws of composition in the two groups.

In this paper, we heavily rely on the symmetric group S_3 in our representation theory examples, as well as the dihedral group D_4, which is isomorphic to the Pauli Group on one qubit P_1 shown in the later section. Here we define the basis group structures of S_3, D_4 and P_1.

Definition 1.7 (Symmetric Group)**.** The group of permutations of the set of indices $\{1, 2, ..., n\}$ is called the *symmetric group*, and is denoted by S_n with the group operation as the composition of functions.

There are $n!$ permutations of a set of n elements, so the symmetric group S_n is a finite group of order $n!$.

Now we describe the symmetric group S_3. To describe the group structure of S_3, we pick two particular permutations in which all other permutations can be written in terms of; in particular, we label x to be the cyclic permutation (123), and y to be the transposition (12).

Then the six elements of the group are given by:

$$S_3 = \{1, x, x^2, y, xy, x^2y\} \tag{4}$$

and we have the rules:

$$x^3 = 1, y^2 = 1, yx = x^2y \tag{5}$$

We note that S_3 has exactly three conjugacy classes, which is useful for later sections. They are given by:

$$\{(1)\}, \{(12)(13)(23)\}, \{(123), (132)\} \tag{6}$$

Definition 1.8 (Dihedral Group)**.** D_n is the group of rotations and reflections of the plane which preserve a regular polygon with n vertices. It contains n rotations, and n reflections. (the order of D_n is $2n$) Denote r as the rotation through an angle $\frac{2\pi}{n}$, and let s be one of its reflections, then we have:

$$r^n = 1, s^2 = 1, srs = r^{-1} \tag{7}$$

Each element of D_n can be written uniquely, either in the form r^k, where $0 \leq k \leq n-1$, or of the form sr^k, where $0 \leq k \leq n-1$.

The elements of D_n are:

$$1, r, r^2, ..., r^{n-1}; s, sr, s^2r, ..., s^{n-1}r \tag{8}$$

Now we introduce the group D_4:

$$D_4 = \langle r, s | r^4 = 1, s^2 = 1, srs = r^{-1} \rangle = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\} \tag{9}$$

Definition 1.9 (Pauli Group)**.** The Pauli group on one qubit has presentation:

$$P_1 = \langle x, J, | x^2 = J^2 = z^2 = 1, [J, x] = [J, z] = 1, [x, z] = J \rangle \tag{10}$$

2 Kets, bras, and all that

While this note as a whole exists to teach the representation theory to the quantum theorists, this section exists to teach quantum theory to the mathematicians.

2.1 Vector spaces

We're working up to the calculus of kets and bras in §2.2. We start from the beginning to emphasize that the amount of linear algebra we use is quite small.

Definition 2.1 (Vector space)**.** A *complex vector space* $(V, +)$ is an abelian group with a scalar multiplication $\cdot : V \times \mathbb{C} \to V$ so that multiplication by fixed scalar is a linear map, i.e.

$$\alpha \cdot (v + w) = \alpha \cdot v + \alpha \cdot w \tag{11}$$

A *subspace* of a vector space is a subgroup which is closed under scalar multiplication.

We'll generally omit the $\cdot$, just using concatenation to denote the scalar product. By convention, the identity of an abelian group is written as 0.

Definition 2.2 (Linear map)**.** Fix complex vector spaces V and W. A linear map $T \in \mathcal{L}(V, W)$ is a function from V to W that distributes over addition and commutes with scalar multiplication.

Lemma 2.3. *For $T \in \mathcal{L}(V, W)$, $\ker T = \{v \,|\, Tv = 0\}$ is a subspace of V and $\operatorname{im} T = \{w \,|\, \exists v, Tv = w\}$ is a subspace of W.*

Proof. To check that a subset is a subspace, it suffices to check that it is closed under addition and scalar multiplication.

Suppose $v, w \in \ker T, \lambda \in C$. Then we can see that $\lambda v \in \ker T$ by computing

$$T(\lambda v) = \lambda T v = \lambda 0 = 0. \tag{12}$$

We can see $v + w \in \ker T$ by computing

$$T(v + w) = Tv + Tw = 0 + 0 = 0. \tag{13}$$

Next, suppose $v, w \in \operatorname{im} V$ with $Tv' = v, Tw' = w$. Then we can see that $\lambda v \in \operatorname{im} T$ by computing

$$T(\lambda v') = \lambda T v' = \lambda v, \tag{14}$$

and we can see that $v + w \in \operatorname{im} T$ by computing

$$T(v' + w') = Tv' + Tw' = v + w. \tag{15}$$

□

Definition 2.4 (Linear isomorphism)**.** A linear map $T : V \to W$ is a *linear isomorphism* if $\ker T = 0$ and $\operatorname{im} T = W$.

Definition 2.5 (Bases)**.** For a subset $S \subset V$, the *span* of S is the set of vectors which can be expressed as a *linear combination* of elements in S, i.e.

$$\operatorname{Span} S = \left\{ v \,\middle|\, v = \sum_i \alpha_i v_i \text{ for some } \alpha_i \in \mathbb{C}, v_i \in V \right\}. \tag{16}$$

We say S is a *spanning set* if $\operatorname{Span} S = V$.

We say S is *linearly independent* if every element $v \in S$ fails to be expressed as a linear combination of vectors from $S \setminus \{v\}$, i.e. $v \notin \operatorname{Span}(S \setminus \{v\})$.

We say S is a *basis for* V if S is linearly independent and spanning.

Lemma 2.6. *Every vector space has a basis.*

Proof. A spanning set S is linearly independent iff it is *minimal*, i.e. no proper subset of S is spanning. The intersection of a decreasing chain of spanning sets is spanning. By Zorn's Lemma, there is a minimal spanning set. □

Lemma 2.7. *If I is a finite independent set and T is a finite spanning set, then $|I| \leq |T|$.*

Proof. Suppose $0 < |I \setminus T|$, and in particular let $v \in I \setminus S$. $I \setminus \{v\}$ is an independent set which is not spanning. In particular, there must be $w \in T$ outside of $\operatorname{Span}(I \setminus \{v\})$. Then $I' := I \setminus \{v\} \cup \{w\}$ is an independent set with $|I'| = |I|$ and $|I' \setminus T| < |I \setminus T|$.

By induction, there is an independent set J with $|J \setminus T| = 0$ and $|J| = |I|$. Then $J \subseteq S$, so $|J| \leq |T|$ and we're done. □

Proposition 2.8 (Dimension)**.** *Every basis of a vector space has the same cardinality.*

Proof. Let S be a spanning set of minimum cardinality and let T be an arbitrary spanning set. Write every element of S as a finite linear combination of elements from T. Let $T' \subseteq T$ be the collection of elements that appear in any of these linear combinations. T' is a spanning set, since it spans S.

If S is infinite, then $|T'| \leq |S|$. Since S had minimum cardinality, in fact $|T'| = |S|$. Now every spanning set has a spanning set below it with

cardinality $|S|$, so every minimal spanning set (and therefore every basis) has cardinality $|S|$, and we're done.

If instead S is finite, we have only the weaker conclusion that T' is also finite. By the same reasoning as before, we now have that every basis is finite. Let S_1 and S_2 be any bases. Letting S_1 play the role of I and S_2 play the role of T in Lemma 2.7, we have $|S_1| \leq |S_2|$. By symmetry, $|S_1| = |S_2|$. □

Definition 2.9 (Eigenvector)**.** Let $T \in \mathcal{L}(V)$ be a linear operator and $\lambda \in \mathbb{C}$. A vector $v \in V$ is an *eigenvector with eigenvalue* λ (a λ-*eigenvector* for short) if

$$Tv = \lambda v. \tag{17}$$

The *spectral theorem* says that we can understand normal operators through their eigenvalues and eigenvectors. In these notes, we'll only need such understanding for projections.

Definition 2.10 (Projection)**.** Let $P : \mathcal{H} \to \mathcal{H}$ be a linear map. We say P is a *projection* if

$$P^2 = P. \tag{18}$$

Clearly 0 and I are projections. We sometimes refer to these as the *trivial projections*, and in particular any other projection may be referred to as *nontrivial*.

Lemma 2.11 (Orthogonal complement)**.** *Let P be a projection. Then $(I - P)$ is also a projection, called the* orthogonal complement *of P. The orthogonal complement enjoys the following properties:*

$$P(I - P) = 0. \tag{19}$$

$$\ker P = \mathrm{im}(I - P) \tag{20}$$

$$\mathrm{im}\, P = \ker(I - P). \tag{21}$$

Proof. To see that the complement is a projection, we compute:

$$(I - P)^2 = I^2 - 2P + P^2 = I - P. \tag{22}$$

Equation (19) is proven with a similar computation:

$$P(I - P) = P - P^2 = P - P = 0. \tag{23}$$

For the remainder, notice that (21) is equivalent to (20) by swapping the roles of P and $I - P$. We'll prove (20) by two containments, starting with $\mathrm{im}(I - P) \subseteq \ker P$.

Suppose $v = (I - P)v'$ is in $\mathrm{im}(I - P)$. Then

$$Pv = P(I - P)v' = 0v' = 0, \tag{24}$$

and v is in $\ker P$. Next, we see that $\ker P \subseteq \mathrm{im}(I - P)$.

Suppose $Pv = 0$. Then

$$v = v - 0 = v - Pv = (I - P)v, \tag{25}$$

and v is in $\mathrm{im}(I - P)$. □

Lemma 2.12. *Let P be a projection and v be a vector. v is an eigenvector with eigenvalue 1 if and only if $v \in \operatorname{im} P$.*

Proof. For one direction, suppose $v = Pv'$. Then

$$Pv = P^2v' = Pv' = v. \tag{26}$$

For the other direction, notice that $Pv = 1v = v$ puts v in the image of P. □

Lemma 2.13. *For $P \in \mathcal{L}(V)$ a projection,* $\operatorname{Span}(\operatorname{im} P \cup \ker P) = V$.

Proof. It suffices to write an arbitrary vector as a sum of two elements, one from $\operatorname{im} P$ and one from $\operatorname{im}(I - P) = \ker P$. We compute:

$$v = Iv = (P + (I - P))v = Pv + (I - P)v \tag{27}$$

□

Lemma 2.14. *For P a projection, P has a basis of eigenvectors.*

Proof. Concatenate a basis of $\operatorname{im} P$ with a basis of $\ker P$. This gives a spanning set by Lemma 2.13. Suppose towards a contradiction that there is a linear dependence among this spanning set. By multiplying both sides of the equation by P or $I - P$, we get a linear dependence among the basis of $\operatorname{im} P$ or among the basis of $\ker P$; contradiction.

The $\operatorname{im} P$ basis elements are 1-eigenvectors by Lemma 2.12, and the $\ker P$ basis elements are 0-eigenvectors by definition of ker. □

Proposition 2.15. *For $W \subseteq V$ a subspace, let $[W]$ be the projection onto W, i.e. the linear map which fixes every element of W and sends everything else to 0. Then for any projection P, $P = [\operatorname{im} P]$. In other words, a projection is uniquely determined by its image.*

Definition 2.16 (Direct sum, internal)**.** For $W_1, W_2 \subseteq V$, we say that V is a *direct sum* $W_1 \oplus W_2$ if $[W_1] = I - [W_2]$.

Reusing the proof of Lemma 2.14, we see that $\dim V = \dim V_1 + \dim V_2$.

Definition 2.17 (Direct sum, external)**.** The direct sum

Definition 2.18 (Tensor product)**.** For vector spaces V_A and V_B we have a vector space $V = V_A \otimes V_B$ generated by the *simple tensors* $v_A \otimes w_B$ subject to bilinearity relations. (We usually omit the subscripts and write $v \otimes w$).

$$(v_1 + v_2) \otimes w = v_1 \otimes w + v_2 \otimes w \tag{28}$$

$$v \otimes (w_1 + w_2) = v \otimes w_1 + v \otimes w_2 \tag{29}$$

$$(cv) \otimes w = v \otimes (cw) \tag{30}$$

Clearly, the map $\otimes : (u, v) \to u \otimes v$ is a bilinear map by the property of tensor product:

$$u \otimes v = \sum_{j,k} (u_j v_k) e_j \otimes f_k \tag{31}$$

where $u = \sum_j u_j e_j \in$ linear space L and $v = \sum_k u_k f_k \in$ linear space M and L, M are endowed with bases $\{e_1, ..., e_l\} \subseteq L$ and $\{f_1, ..., f_l\} \subseteq M$.

2.2 Hilbert spaces

Throughout, all of our vector spaces are finite-dimensional.

Definition 2.19 (Hermitian inner product)**.** Let V be a complex vector space. A *Hermitian inner product* is a function $(-,-) : V \times V \to \mathbb{C}$ which is conjugate-linear in the first argument and linear in the second:

$$\begin{aligned}(c\xi, \eta) &= c^*(\xi, \eta)\\ (\xi, c\eta) &= c(\xi, \eta)\\ (\xi_1 + \xi_2, \eta) &= (\xi_1, \eta) + (\xi_2, \eta)\\ (\xi, \eta_1 + \eta_2) &= (\xi, \eta_1) + (\xi, \eta_2)\end{aligned}$$

Definition 2.20 (Hilbert space)**.** A *finite-dimensional Hilbert space* $\mathcal{H}$ is a finite-dimensional complex vector space equipped with a Hermitian inner product $(-,-) : \mathcal{H} \times \mathcal{H} \to \mathbb{C}$. An element $|\psi\rangle \in \mathcal{H}$ of a (primal) Hilbert space is called a *ket*.

In infinite dimensions, we also require that the norm induced by the inner product gives the structure of a *Banach space*, but in finite dimensions this is automatic.

Definition 2.21 (Dual vector space)**.** Starting from a Hilbert space $\mathcal{H}$, the *dual space* $\mathcal{H}^* = \mathcal{L}(\mathcal{H}, \mathbb{C})$ is the space of linear functionals.

There is a map $\dagger : \mathcal{H} \to \mathcal{H}^*$ sending $|\psi\rangle$ to the linear functional represented by $|\phi\rangle \mapsto (|\psi\rangle, |\phi\rangle)$. We denote this functional as $\langle\psi|$ and write simply $\langle\psi|\phi\rangle$ for the application of $\langle\psi|$ to $|\phi\rangle$. This enables us to almost entirely forget the $(-,-)$ notation.

Definition 2.22 (Orthonormal basis)**.** A basis $\{|i\rangle\}_{i<\dim\mathcal{H}}$ is *orthonormal* if

$$\langle i|j\rangle = \delta_i^j. \tag{32}$$

Every basis can be converted to an orthonormal basis by the Gram–Schmidt procedure. In particular, every space has an orthonormal basis.

Proposition 2.23. *$\mathcal{H}$ and $\mathcal{H}^*$ are linearly isomorphic up to complex conjugate. Every element of $\mathcal{H}^*$ can be written as a bra.*

Proof. Fix a basis $\{|i\rangle\}$ for $\mathcal{H}$. Let $f \in \mathcal{H}^*$. f is completely determined by its action on a basis. In particular,

$$f\,|\phi\rangle = \sum_i f\,|i\rangle\,\langle i|\phi\rangle\,. \tag{33}$$

This leads to an equality of dual space elements:

$$f = \sum_i (f\,|i\rangle)\,\langle i|\,. \tag{34}$$

Setting $|\psi\rangle := \sum_i \overline{f\,|i\rangle}\,|i\rangle$, we have $\langle\psi| = f$.

This establishes that the map $\dagger : |\psi\rangle \mapsto \langle\psi|$ is bijective. It is also *conjugate linear* in the sense that it is additive and satisfies $(c\,|\psi\rangle)^\dagger = \overline{c}(|\psi\rangle)^\dagger$. □

This proof may fail in infinite dimension, where one has to worry about the sums converging.

Definition 2.24 (Hilbert space structure on the dual)**.** We define the inner product on the dual via the conjugate-linear isomorphism.

$$(\langle\psi|\,, \langle\phi|) := \langle\phi|\psi\rangle\,. \tag{35}$$

Iterating proposition 2.23, we get that $\mathcal{H}$ and $(\mathcal{H}^*)^*$ are linearly isomorphic with $\dagger \circ \dagger$ acting as identity, i.e. $(\langle\psi|)^\dagger = |\psi\rangle$.

Lemma 2.25. *$\mathcal{L}(\mathcal{H}_1, \mathcal{H}_2)$ is linearly isomorphic to $\mathcal{H}_2 \otimes \mathcal{H}_1^*$.*

Proof. Define $|i\rangle\langle j| \in \mathcal{L}(\mathcal{H}_1, \mathcal{H}_2)$ via the action $|\psi\rangle \mapsto \langle j|\psi\rangle\,|i\rangle$. Our isomorphism will be to identify $|i\rangle\langle j|$ with $|i\rangle \otimes \langle j|$. To check that this is an isomorphism it suffices to check that it sends a basis to a basis. To see this, pick any orthonormal bases $\{|i\rangle\}$, $\{\langle j|\}$ of $\mathcal{H}_2, \mathcal{H}_1^*$ and see that $\{|i\rangle\langle j|\}$ forms a basis for the space of linear maps. Let $A \in \mathcal{L}(\mathcal{H}_1, \mathcal{H}_2)$ be arbitrary. We claim that $A = \sum_{ij} \langle j|A|i\rangle\,|i\rangle\langle j|$. It suffices to check that they agree on a basis of $\mathcal{H}_1$.

$$\left(\sum_{ij} \langle i|A|j\rangle\,|i\rangle\langle j|\right)|j'\rangle = \sum_{ij} \langle i|A|j\rangle\,|i\rangle\,\langle j|j'\rangle \tag{36}$$

$$= \sum_{ij} \langle i|A|j\rangle\,|i\rangle\,\delta_j^{j'} \tag{37}$$

$$= \sum_{i} \langle i|A|j'\rangle\,|i\rangle \tag{38}$$

$$= A\,|j'\rangle \tag{39}$$

□

Just as in the case of the dual space, we can extend transport the inner product along the linear isomorphism to give a Hilbert space structure.

Definition 2.26 (Hilbert space structure on the tensor product)**.** To define an inner product on $\mathcal{H}_1 \otimes \mathcal{H}_2$, it's enough to define it on the pure tensors and extend linearly.

$$(|i\rangle \otimes |j\rangle\,, |k\rangle \otimes |l\rangle) := \langle i|k\rangle\,\langle j|l\rangle\,. \tag{40}$$

One can check that with this Hilbert space structure on the tensor product, we have $(\mathcal{H}_1 \otimes \mathcal{H}_2)^* = \mathcal{H}_1^* \otimes \mathcal{H}_2^*$. Notice that this puts a Hilbert space structure on $\mathcal{L}(\mathcal{H}_1, \mathcal{H}_2)$, which can be written as

$$(|i\rangle\langle j|\,, |k\rangle\langle l|) := \langle i|k\rangle\,\langle l|j\rangle\,. \tag{41}$$

Chaining these together, we have

$$\mathcal{L}(\mathcal{H}_1, \mathcal{H}_2)^* \cong (\mathcal{H}_2 \otimes \mathcal{H}_1^*)^* \cong \mathcal{H}_2^* \otimes (\mathcal{H}_1^*)^* \cong \mathcal{H}_1 \otimes \mathcal{H}_2^* \cong \mathcal{L}(\mathcal{H}_2, \mathcal{H}_1). \tag{42}$$

This duality gives us a useful representation of the inner product on $\mathcal{L}(\mathcal{H}_1, \mathcal{H}_2)$ via the *trace*.

Definition 2.27. Define a function $\operatorname{Tr} : \mathcal{L}(\mathcal{H}) \to \mathbb{C}$ as

$$\operatorname{Tr} |i\rangle\langle j| = \langle j|i\rangle \,, \tag{43}$$

extending to the whole space by linearity. To see that this is well-defined, it's enough to see that the trace does not depend on our choice for a basis of pure tensors.

Fix an orthonormal basis $|i\rangle$ If we have $A = \sum_j \lambda_j |\psi_j\rangle\langle\phi_j|$, we can rewrite term-by-term with $|\psi_j\rangle = \sum_i \langle i|\psi_i\rangle |i\rangle$ and $\langle\phi_j| = \sum_{i'} \langle\phi_j|i'\rangle \langle i'|$. After all the rewrites, we've expressed A in the $|i\rangle\langle i'|$ basis. The coefficients in this basis do not depend on the $|\phi_j\rangle$ and $|\psi_j\rangle$. All that remains is to check that each rewrite preserves the overall trace. We compute:

$$\operatorname{Tr} |\psi\rangle\langle\phi| = \operatorname{Tr} \left(\sum_i |i\rangle\langle i| \, |\psi\rangle \right) \otimes \left(\sum_{i'} \langle\phi| \, |i'\rangle\langle i'| \right) \tag{44}$$

$$= \operatorname{Tr} \sum_{ii'} \langle i|\psi\rangle \, \langle\phi|i'\rangle \, |i\rangle\langle i'| \tag{45}$$

$$= \sum_{ii'} \langle i|\psi\rangle \, \langle\phi|i'\rangle \operatorname{Tr} |i\rangle\langle i'| \tag{46}$$

$$= \sum_i \langle i|\psi\rangle \, \langle\phi|i\rangle \tag{47}$$

$$= \langle\phi|\psi\rangle \,. \tag{48}$$

Notice that our proof that the trace is well-defined also gives an interpretation $\operatorname{Tr} A = \sum_i \langle i|A|i\rangle$ for any basis $|i\rangle$.

Lemma 2.28. *The inner product on $\mathcal{L}(\mathcal{H}_1, \mathcal{H}_2)$ is represented by*

$$(A, B) = \operatorname{Tr} A^\dagger B. \tag{49}$$

Proof. By linearity, we only need to check on basis elements. We compute:

$$\operatorname{Tr}(|i\rangle\langle j|)^\dagger \, |k\rangle\langle l| = \operatorname{Tr} |j\rangle\langle i| \, |k\rangle\langle l| \tag{50}$$

$$= \operatorname{Tr} |j\rangle \, \langle i|k\rangle \, \langle l| \tag{51}$$

$$= \langle i|k\rangle \operatorname{Tr} |j\rangle\langle l| \tag{52}$$

$$= \langle i|k\rangle \, \langle l|j\rangle \,. \tag{53}$$

This recovers equation (41), so we're done. □

Lemma 2.29 (Cyclicity of the trace)**.** *For $A \in \mathcal{L}(\mathcal{H}_1, \mathcal{H}_2)$, $B \in \mathcal{L}(\mathcal{H}_2, \mathcal{H}_1)$,*

$$\operatorname{Tr} AB = \operatorname{Tr} BA. \tag{54}$$

Proof.

$$\operatorname{Tr} AB = (A^\dagger, B) = (B^\dagger, A) = \operatorname{Tr} BA. \tag{55}$$

□

Notice that this proof requires repeated switching between spaces. The first trace is on $\mathcal{L}(\mathcal{H}_2)$, the first inner product is on $\mathcal{L}(\mathcal{H}_2, \mathcal{H}_1)$, the second inner product is on $\mathcal{L}(\mathcal{H}_1, \mathcal{H}_2)$ and the second trace is on $\mathcal{L}(\mathcal{H}_1)$.

Definition 2.30 (Isometry)**.** A linear isomorphism $V : \mathcal{H}_1 \to \mathcal{H}_2$ is an *isometry* if it preserves inner products, i.e. $(V|\psi\rangle, V|\phi\rangle) = (|\psi\rangle, |\phi\rangle)$ for all $|\psi\rangle, |\phi\rangle \in \mathcal{H}_1$. We denote the space of isometries by $\mathcal{U}(\mathcal{H}_1, \mathcal{H}_2)$.

Lemma 2.31. *The composition of isometries is an isometry.*

Lemma 2.32. *For any isometry V, $V^\dagger V = I$ and $VV^\dagger$ is a projection on the image of V.*

Proof. Fix an orthonormal basis of $\mathcal{H}_1$. It suffices to show $\langle j|U^\dagger U|i\rangle = \delta_i^j$. By the definition of isometries, we have $\langle j|U^\dagger U|i\rangle = \langle j|i\rangle$, so we're done.

To see that $VV^\dagger$ is a projection, we apply the previous observation: $(VV^\dagger)^2 = V(V^\dagger V)V^\dagger = VV^\dagger$. □

Definition 2.33 (Unitary operator)**.** A *unitary operator* $U \in \mathcal{U}(\mathcal{H})$ is an operator satisfying $UU^\dagger = U^\dagger U = I$.

Notice that $U^\dagger$ is also unitary, and that unitaries are also isometries.

Lemma 2.34. *If $\mathcal{H}$ is finite-dimensional and $V : \mathcal{H} \to \mathcal{H}$ is an isometry, then V is a unitary.*

Lemma 2.35. *If P is a projection on a finite-dimensional space, then* $\operatorname{Tr} P = \dim \operatorname{im} P$.

Proof. For any orthonormal basis $\{|i\rangle\}$ of $\operatorname{im} P$, $P = \sum_i |i\rangle\langle i|$. Taking the trace,

$$\operatorname{Tr} P = \sum_{i < \dim \operatorname{im} P} 1 = \dim \operatorname{im} P. \tag{56}$$

□

Proof of Lemma 2.34. It suffices to show that $VV^\dagger$ is identity. By Lemma 2.32, $VV^\dagger$ is a projection. By Lemma 2.35, the dimension of the image is $\operatorname{Tr} VV^\dagger = \operatorname{Tr} V^\dagger V = \operatorname{Tr} I$. The only subspace whose dimension is equal to $\operatorname{Tr} I$ is the whole space. □

There is a simple counterexample in infinite dimensions. Let $\mathcal{H} = \mathbb{C}^{\mathbb{N}} = \operatorname{Span}|i\rangle \; i \in \mathbb{N}$. This can be thought of as the state space of the quantum harmonic oscillator, with the $|i\rangle$ being thought of as eigenstates of the Hamiltonian. Let a be the raising operator, acting as $a|i\rangle := |i+1\rangle$. Then we have $a^\dagger a = I$ (raising and then lowering is identity) but $aa^\dagger = I - |0\rangle\langle 0|$ (lowering and then raising annihilates the ground state). So a is an isometry but not a unitary.

Lemma 2.36. *For unitary U, $U^\dagger$ is unitary and $UU^\dagger = U^\dagger U = I$.*

Proof. $U^\dagger U = I$ by lemma 2.32 since U is an isometry. Supposing $U^\dagger$ is an isometry, another application of the same lemma gives $UU^\dagger = (U^\dagger)^\dagger U^\dagger = I$. □

Lemma 2.37. *Unitaries form a group under composition.*

Proof. Clearly, the identity matrix $I_{2^n} \in A_n$. Moreover, the set of unitary matrices are closed under multiplication. Assume U and V are two unitary matrices. This mean that U take a set of orthonormal basis to another set of orthonormal basis, and V take a set of orthonormal basis to another set of orthonormal basis as well. Hence UV also take a set of orthonormal basis to another set of orthonormal basis, and therefore the operator UV is unitary as well. Now we show that if U is unitary, then U^{-1} is also unitary. We show that $U^{\dagger\dagger} = = U$. This is true because

$$U^{\dagger\dagger} = (\overline{U^T})^\dagger = U \tag{57}$$

□

3 Generalities on Linear Representations

Definition 3.1 (Unitary group)**.** The *unitary group* $\mathcal{U}(\mathcal{H})$ is defined as the group of unitary operators on $\mathcal{H}$.

Definition 3.2 (Unitary Representation)**.** A *unitary representation* of G in $\mathcal{H}$ is a homomorphism τ from the group G into the group $\mathcal{U}(\mathcal{H})$. We say that $\mathcal{H}$ is the *representation space* of τ.

We say a representation is *finite-dimensional* if $\dim H$ is a positive integer.

A *linear representation*, more generally, has its image in the *general linear group* consisting of all invertible operators. However, every linear representation of a finite group is automatically unitary. This happens because any normal operator which is a root of unity, i.e. $T^d = I$ for some integer d, is unitary.

Example 3.3. Let $\mathcal{H} = \mathbb{C}^3$ be spanned by $\{|1\rangle, |2\rangle, |3\rangle\}$. We have a representation $\tau : S_3 \to \mathcal{U}(\mathcal{H})$ on this space given by

$$\tau(\pi)\,|i\rangle = |\pi(i)\rangle\,. \tag{58}$$

It is easy to check that τ is a homomorphism – symbolically speaking, the group multiplication "happens inside the ket":

$$\tau(\pi)\tau(\sigma)\,|i\rangle = |\pi(\sigma(i))\rangle = \tau(\pi \circ \sigma)\,|i\rangle\,. \tag{59}$$

We give τ in explicit matrix form below.

$$\tau((1)) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad \tau((12)) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\tau((132)) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \qquad \tau((13)) = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

$$\tau((123)) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \qquad \tau((23)) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

Definition 3.4 (Intertwiner)**.** Let $\tau_1 : G \to \mathcal{U}(\mathcal{H}_1)$ and $\tau_2 : G \to \mathcal{U}(\mathcal{H}_2)$ be two unitary representations of G. We say $T : V_1 \to V_2$ is an *intertwiner between* τ_1 *and* τ_2 if for all $s \in G$:

$$\tau_2(s)T = T\tau_1(s) \tag{60}$$

τ_1 and τ_2 are *isomorphic* if T is invertible.

Example 3.5. Let $\omega = e^{2\pi i/3}$ and consider the representation τ' given by:

$$\tau'((1)) = \left(\begin{array}{c|cc} 1 & 0 & 0 \\ \hline 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right) \qquad \tau'((12)) = \left(\begin{array}{c|cc} 1 & 0 & 0 \\ \hline 0 & 0 & \omega \\ 0 & \overline{\omega} & 0 \end{array}\right)$$

$$\tau'((132)) = \left(\begin{array}{c|cc} 1 & 0 & 0 \\ \hline 0 & \overline{\omega} & 0 \\ 0 & 0 & \omega \end{array}\right) \qquad \tau'((13)) = \left(\begin{array}{c|cc} 1 & 0 & 0 \\ \hline 0 & 0 & \overline{\omega} \\ 0 & \omega & 0 \end{array}\right)$$

$$\tau'((123)) = \left(\begin{array}{c|cc} 1 & 0 & 0 \\ \hline 0 & \omega & 0 \\ 0 & 0 & \overline{\omega} \end{array}\right) \qquad \tau'((23)) = \left(\begin{array}{c|cc} 1 & 0 & 0 \\ \hline 0 & 0 & 1 \\ 0 & 1 & 0 \end{array}\right)$$

τ and τ' have an intertwiner given by the change of basis from $\{|i\rangle\}$ to $\{|\psi_i\rangle\}$, where the latter are defined as:

$$|\psi_1\rangle := \frac{1}{\sqrt{3}}\left(|1\rangle + |2\rangle + |3\rangle\right), \tag{61}$$

$$|\psi_2\rangle := \frac{1}{\sqrt{3}}\left(|1\rangle + \omega\,|2\rangle + \overline{\omega}\,|3\rangle\right), \text{ and} \tag{62}$$

$$|\psi_3\rangle := \frac{1}{\sqrt{3}}\left(|1\rangle + \overline{\omega}\,|2\rangle + \omega\,|3\rangle\right). \tag{63}$$

T takes an orthonormal basis to an orthonormal basis, so it is unitary and τ and τ' are isomorphic representations.

Definition 3.6 (Regular Representation)**.** Given a group G, the *regular representation space* $\mathbb{C}^G$ is the $|G|$-dimensional space spanned by $|g\rangle$ for $g \in G$. The *left regular representation* $L : G \to \mathbb{C}^G$ is defined by the equation

$$L(g)\,|h\rangle = |gh\rangle\,. \tag{64}$$

Similarly, the *right regular representation* $R : G \to \mathbb{C}^G$ is defined by the equation

$$R(g)\,|h\rangle = |hg^{-1}\rangle\,. \tag{65}$$

Notice that the left and right regular representations are intertwined by the unitary that acts as $|g\rangle \mapsto |g^{-1}\rangle$.

Definition 3.7 (Stable subspace)**.** Let $\tau : G \to \mathcal{U}(\mathcal{H})$ be a representation and $P \in \mathcal{L}(\mathcal{H})$ be a projection. We say τ *stabilizes* P if $P\tau(g) = \tau(g)P$ for all g.

Notice that the map τ^P defined by $g \mapsto P\tau(g)P$ is a representation on $\operatorname{im} P$. The following calculation illustrates this:

$$\tau_P(g)\tau_P(h) = P\tau(g)PP\tau(h)P = P^2\tau(g)\tau(h)P^2 = P\tau(gh)P = \tau_P(gh). \tag{66}$$

Definition 3.8 (Subrepresentation)**.** Let $\tau : G \to \mathcal{U}(\mathcal{H})$ be a representation which stabilizes P. Then the map τ^P defined above is a representation which we refer to as a *subrepresentation* of τ.

Notice that if τ stabilizes P, then it also stabilizes the orthogonal complement $I - P$. To see this, let g be an arbitrary group element and compute:

$$(I - P)\tau(g) = \tau(g) - P\tau(g) = \tau(g) - \tau(g)P = \tau(g)(I - P). \tag{67}$$

Example 3.9. Using the notation from Example 3.5, let $P_0 = |\psi_1\rangle\langle\psi_1|$ and $P_1 = I - P_0 = |\psi_2\rangle\langle\psi_2| + |\psi_3\rangle\langle\psi_3|$. τ stabilizes P_0. One can check this directly by noticing that $\tau(g)\,|\psi_1\rangle =$

We illustrate the concept of *projection* on the group S_3.

Let V be the three-dimensional vector space of the standard representation of S_3, which their matrix forms are given in **??**.

Let W be two-dimensional vector space spanned by the vectors $|1\rangle + w\,|2\rangle + w^2\,|3\rangle$ and $|1\rangle + w^2\,|2\rangle + w\,|3\rangle$, where $w = 3^{\frac{2\pi i}{3}}$. Then we have:

$$P(g) = \text{right bottom 2 by 2 submatrix of } TgT^{-1} \tag{68}$$

where T is defined in 3.5

To be explicit, we have

$$P(\rho(13)) = \begin{pmatrix} 0 & w^2 \\ w & 0 \end{pmatrix} \tag{69}$$

This is because:

$$T(\rho(13))T^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & w^2 \\ 0 & w & 0 \end{pmatrix} \tag{70}$$

Definition 3.10 (Irreducible Representation)**.** We say a representation $\tau : G \to \mathcal{U}(\mathcal{H})$ is *irreducible* if $\mathcal{H}$ is not 0 and the only projections stabilized by τ are the trivial projections 0 and I.

It is easy to see that all one-dimensional representations are irreducible and abelian.[1] Conversely, abelian representations are irreducible only if they are one-dimensional. To see this, recall that a finite collection of operators commute if and only if they have a simultaneous eigenbasis. If the image of a representation commutes, then the representation stabilizes these eigenspaces.

Going a touch further, we can see that a two-dimensional representation is irreducible iff it is nonabelian. If a two-dimensional representation has a nontrivial stable subspace P, both it and its complement would be one dimensional. Then we could repeat the trick from Example 3.9, writing the matrices in block-diagonal form with one block for the stable subspace and its complement. But both blocks are 1-dimensional, giving a full simultaneous eigenbasis.

The technique of decomposing representations into sums of irreducibles lies at the core of the theory.

[1] We say a representation τ is abelian if $\tau(g)\tau(h) = \tau(h)\tau(g)$ for all g, h. Notice that every group has an abelian representation given by sending everything to I.

Proposition 3.11. *Every finite-dimensional representation is a direct sum of irreducible representations.*

Proof. We proceed by strong induction on the dimension of $\mathcal{H}$. Let $\tau : G \to U(\mathcal{H})$ be a representation. If $\dim \mathcal{H} = 1$, the representation is irreducible and we're done. If not, then either the representation is irreducible (and we're done) or there is a nontrivial projection P stabilized by τ, and $\tau = \tau^P + \tau^{I-P}$. By the inductive hypothesis, each summand is a direct sum of irreducibles, and we're done. □

4 Character Theory

Definition 4.1 (Trace)**.** Given a square matrix A, we define the *trace* of A to be the sum of the entries on the main diagonal:

$$\mathrm{Tr}(A) = \sum_i a_{ii} \tag{71}$$

Lemma 4.2. *Let A, B be two matrices of dimensions $n \times m$, $m \times n$ respectively. Then*

$$\mathrm{Tr}(AB) = \mathrm{Tr}(BA) \tag{72}$$

Proof.

$$\mathrm{Tr}(AB) = \sum_j \sum_k a_{j,k} b_{k,j} \tag{73}$$

$$\mathrm{Tr}(BA) = \sum_k \sum_j b_{k,j} a_{j,k} \tag{74}$$

We have

$$\sum_j \sum_k a_{j,k} b_{k,j} = \sum_k \sum_j b_{k,j} a_{j,k} \tag{75}$$

as required.

□

Remark 4.3. 1. We can generalize dimension of a Hilbert space using trace:

$$\chi(I_G) = \mathrm{Tr}(I_v) = dim(\mathcal{H}) \tag{76}$$

2. One may also be able to take the trace of operators on an infinite-dimensional space. These are known as the "trace class operators" on a Hilbert space and the "nuclear operators" on a Banach space.

Lemma 4.4. *Given a square matrix A, $\mathrm{Tr}(A)$ is equivalent to the sum of the eigenvalues of A counted with multiplicities, and does not depend on the choice of basis (e_i).*

Proof. For any square matrix A, there exists an invertible matrix V such that

$$V^{-1} A V = J \tag{77}$$

where J is of Jordan canonical form, and has the eigenvalues of A on the principal diagonal and elements of 1 or 0 next to the principal diagonal in the right and zeroes everywhere else.

$$\mathrm{Tr}(J) = \mathrm{Tr}(V^{-1}AV) = \mathrm{Tr}(VV^{-1}A) = \mathrm{Tr}(IA) = \mathrm{Tr}(A) \tag{78}$$

Then Jordan canonical form matrix J has the eigenvalues of A on its principal diagonal with multiplicities, hence the trace of J is equal to the sum of the eigenvalues of A. □

Definition 4.5 (Character)**.** For each $s \in G$, define

$$\chi_\tau(s) = \mathrm{Tr}(\tau(s)) \tag{79}$$

χ_τ on G is the *character* of the representation τ.

Lemma 4.6. *The character is invariant with respect to the basis of the vector space V.*

Proof. We use the proof of 4.4. The character is equivalent to the sum of eigenvalues, and the eigenvalues are invariant with respect to the basis. □

Proposition 4.7. *If χ is the character of a representation $\tau : G \to \mathcal{U}(\mathcal{H})$ of dimension n, then:*

1.

$$\chi(1) = n \tag{80}$$

2.

$$\textit{For all } s \in G, \chi(s^{-1}) = \chi(s)^* \tag{81}$$

3.

$$\textit{For all } s, t \in G, \chi(tst^{-1}) = \chi(s) \tag{82}$$

Proof. Since $\tau(1) = 1$,$\tau(1)$ is just the identity matrix of dimension n, which has trace equal to n.

$$\chi(s)^* = \mathrm{Tr}(\tau_s)^* = \sum_i {\lambda_i}^{-1} = \mathrm{Tr}({\tau_s}^{-1}) = \mathrm{Tr}(\tau_{s^{-1}}) = \chi(s^{-1}) \tag{83}$$

To prove the third property, note that by theorem 4.2

$$\mathrm{Tr}(AB) = \mathrm{Tr}(BA) \tag{84}$$

where A, B are two arbitrary linear isomorphisms of $\mathcal{H}$ into itself.

$$\chi_{uv} = \chi_{vu} \tag{85}$$

Take $u = ts, v = t^{-1}$,

$$\chi_{tst^{-1}} = \chi_s \tag{86}$$

as required. □

Proposition 4.8. *Let $\tau_1 : G \to \mathcal{U}(\mathcal{H}_1)$ and $\tau_2 : G \to \mathcal{U}(\mathcal{H}_2)$ be two unitary representations of G, and let χ_1 and χ_2 be their characters. Then:*

1. The character χ of the direct sum representation $V_1 \oplus V_2$ is equal to $\chi_1 + \chi_2$.

2. The character ϕ of the tensor product representation $V_1 \otimes V_2$ is equal to $\chi_1 \cdot \chi_2$.

Proof. Assume the matrix forms of τ_1 and τ_2 are given by $R_1(s)$ and $R_2(s)$ respectively, then the matrix form of the direct sum representation $R(s)$ is:

$$\begin{pmatrix} R_s^1 & 0 \\ 0 & R_s^2 \end{pmatrix} \tag{87}$$

Hence

$$\chi(R(s)) = \chi(R_1(s)) + \chi(R_2(s)) = \chi_1 + \chi_2 \tag{88}$$

as required.

To prove the second property, note that:

$$\chi_1(s) = \sum_{i_1} r_{i_1 i_1}(s) \tag{89}$$

$$\chi_2(s) = \sum_{i_2} r_{i_2 i_2}(s)$$

Therefore

$$\phi(s) = \sum_{i_1, i_2} r_{i_1 i_1}(s) r_{i_2 i_2}(s) = \chi_1(s) \cdot \chi_2(s) \tag{90}$$

as required. □

Example 4.9. Let $R_1(s)$ be the following:

$$R_1(s) = \begin{pmatrix} 1 & 2 & 0 \\ 0 & 4 & 6 \\ 3 & 1 & 3 \end{pmatrix} \tag{91}$$

$$\mathrm{Tr}(R_1(s)) = 8 \tag{92}$$

Let $R_2(s)$ be the following:

$$R_2(s) = \begin{pmatrix} 1 & 2 \\ 0 & 4 \end{pmatrix} \tag{93}$$

$$\mathrm{Tr}(R_2(s)) = 5 \tag{94}$$

Then the matrix $R(s) = R_1(s) \oplus R_2(s)$ is given as:

$$R(s) = \begin{pmatrix} 1 & 2 & 0 & 0 & 0 \\ 0 & 4 & 6 & 0 & 0 \\ 3 & 1 & 3 & 0 & 0 \\ 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 4 \end{pmatrix} \tag{95}$$

Then :

$$\mathrm{Tr}(R(s)) = 13 = \mathrm{Tr}(R_1(s)) + \mathrm{Tr}(R_2(s)) \tag{96}$$

The matrix representation of $R_1(s) \otimes R_2(s)$ is given by:

$$R_1(s) \otimes R_2(s) = \begin{pmatrix} 1 & 2 & 2 & 4 & 0 & 0 \\ 0 & 4 & 0 & 8 & 0 & 0 \\ 0 & 0 & 4 & 8 & 6 & 12 \\ 0 & 0 & 0 & 16 & 0 & 24 \\ 3 & 6 & 1 & 2 & 3 & 6 \\ 0 & 12 & 0 & 4 & 0 & 12 \end{pmatrix} \tag{97}$$

Then:

$$\mathrm{Tr}(R_1(s) \otimes R_2(s)) = 40 = \mathrm{Tr}(R_1(s)) \times \mathrm{Tr}(R_2(s)) \tag{98}$$

Example 4.10 (Exercise 2.3 of [Ser77]). Let $\tau : G \to \mathcal{U}(\mathcal{H})$ be a unitary representation with character χ and let $\mathcal{H}'$ be the dual of $\mathcal{H}$, i.e., the space of linear forms on $\mathcal{H}$, $\mathcal{L}(\mathcal{H})$.

For $|x\rangle \in \mathcal{H}, \langle x'| \in \mathcal{H}'$ let $\langle x, x'\rangle$ denote the value of $\langle x'|x\rangle$. Then there is a unique unitary linear representation $\tau' : G \to \mathcal{U}(\mathcal{H}')$ such that

$$\langle \tau(s) |x\rangle , \tau'(s) \langle x'|\rangle = \langle x, x'\rangle \text{ for } s \in G, |x\rangle \in V, \langle x'| \in V' \tag{99}$$

Proof. Define $\tau'(s)$ such that for all $s \in G, x \in V'$

$$\tau'(s) |x\rangle = |x\rangle \circ \tau(s^{-1}) \tag{100}$$

Then for all $s \in G$

$$\begin{aligned} \langle \tau(s) |e_g\rangle , \tau'(s) \langle e'_g|\rangle &= \langle \tau(s) |e_g\rangle , \langle e'_g| \circ \tau(s^{-1})\rangle && (101)\\ &= \langle \tau(s) |e_g\rangle , \langle e'_g| \circ \tau(s)^{-1}\rangle && (102)\\ &= \langle e'_g| \circ \tau(s)^{-1}(\tau(s) |e_g\rangle) && (103)\\ &= \langle e'_g|e_g\rangle && (104)\\ &= \langle e_g, e'_g\rangle && (105)\\ & && (106) \end{aligned}$$

Hence for all $|x\rangle \in \mathcal{H}$

$$\langle \tau(s) |x\rangle , \tau'(s) \langle x'|\rangle = \langle x, x'\rangle \tag{107}$$

Now we show the uniqueness of $\tau' : G \to \mathcal{U}(\mathcal{H}')$.

Assume that there exists another representation $\sigma : G \to \mathcal{U}(\mathcal{H}')$ such that

$$\langle \tau(s) |x\rangle , \sigma(s) \langle x'|\rangle = \langle x, x'\rangle = \langle \tau(s) |x\rangle , \tau'(s) \langle x'|\rangle \tag{108}$$

Then for all $|x\rangle \in \mathcal{H}$:

$$\begin{aligned} 0 &= \langle \tau(s) |x\rangle , \sigma(s) \langle x'|\rangle - \langle \tau(s) |x\rangle , \tau'(s) \langle x'|\rangle && (109)\\ &= \langle \tau(s) |x\rangle , \sigma(s) \langle x'| - \tau'(s) \langle x'|\rangle && (110)\\ &= \langle \tau(s) |x\rangle , (\sigma(s) - \tau'(s)) \langle x'|\rangle && (111) \end{aligned}$$

Hence

$$\langle \tau(s) |x\rangle , (\sigma(s) - \tau'(s)) \langle x'|\rangle = 0 \tag{112}$$

$$(\sigma(s) - \tau'(s)) \langle x'| (\tau(s) |x\rangle) = 0 \tag{113}$$

Since $\tau(s)|x\rangle$ spans the whole Hilbert space $\mathcal{H}$, we must have $(\sigma(s) - \tau'(s))x' = 0$. Hence we must have $\sigma(s) - \tau'(s) = 0$, which is equivalent to

$$\sigma(s) = \tau'(s) \tag{114}$$

This completes the proof that $\tau'(s)$ is unique. □

Remark 4.11. τ' is called the *dual representation* of τ, its character is X^*.

Example 4.12. T defined in example 3.5 is an intertwiner for two representations in example 3.5.

The following technical lemma comprises half of Lemma 4.14 (Schur's Lemma).

Lemma 4.13. *Suppose τ_1 and τ_2 are irreducible and T is an intertwiner. Then either $T = 0$ or T is a linear isomorphism.*

Proof. We show that τ_1 stabilizes $\ker T$ and τ_2 stabilizes $\operatorname{im} T$. By irreducibility of τ_1, either $T = 0$ ($\ker T = \mathcal{H}_2$) or T is injective ($\ker T = 0$). By irreducibility of τ_2, either $T = 0$ ($\operatorname{im} T = 0$) or T is surjective ($\operatorname{im} T = \mathcal{H}_1$).

To see that τ_1 stabilizes $\ker T$, let $T|\psi\rangle = 0$ and compute:

$$T\tau_1(g)|\psi\rangle = \tau_2(g)T|\psi\rangle = 0, \tag{115}$$

so that $\tau_1(g) \in \ker T$.

Similarly, to see that τ_2 stabilizes $\operatorname{im} T$, let $|\psi\rangle = T|\phi\rangle$ and compute:

$$\tau_2(g)|\psi\rangle = \tau_2(g)T|\phi\rangle = T\tau_1(g)|\phi\rangle, \tag{116}$$

so that $\tau_2(g)|\psi\rangle \in \operatorname{im} T$.

□

Lemma 4.14 (Schur's Lemma)**.** *Let $\tau : G \to \mathcal{U}(\mathcal{H})$ be an irreducible representation of G, and suppose that T commutes with $\tau(g)$ for all $g \in G$, i.e. $T\tau(g) = \tau(g)T$.*

Then T is a scalar multiple of identity, i.e. $T = cI$ for some scalar $c \in \mathbb{C}$. (Sometimes such a T is referred to as a homothety*.)*

Proof. Notice that T is an intertwiner between τ and τ, so Lemma 4.13 applies. Either $T = 0$ or T is a linear isomorphism. In the first case, we are done with $c = 0$. In the latter case, let $|\lambda\rangle$ be an eigenstate of T with eigenvalue λ, i.e. $T|\lambda\rangle = \lambda|\lambda\rangle$.

Consider the map $T' := T - \lambda$. We want to show that T' is identically zero so that $T = \lambda I$ and we're done with $c = \lambda$.

By Lemma 4.13 it suffices to show that T' is an intertwiner with nontrivial kernel. For the kernel, notice that $T'|\lambda\rangle = T|\lambda\rangle - \lambda|\lambda\rangle = 0$. It remains to show the intertwiner equation

$$\tau(s)T' = T'\tau(s). \tag{117}$$

We compute

$$\begin{aligned}\tau(s)T' &= \tau(s)(T-\lambda) && (118)\\ &= \tau(s)T - \lambda\tau(s) && (119)\\ &= T\tau(s) - \lambda\tau(s) && (120)\\ &= (T\tau(s) - \lambda\tau(s)) && (121)\\ &= (T-\lambda)\tau(s) && (122)\\ &= T'\tau(s) && (123)\end{aligned}$$

as required. □

Corollary 4.15. *Let H be a linear mapping of $\mathcal{H}_1$ into $\mathcal{H}_2$, $\tau_1 : G \to \mathcal{U}(\mathcal{H}_1)$ and $\tau_2 : G \to \mathcal{U}(\mathcal{H}_2)$ be two unitary representations. Moreover define*

$$H_0 = \mathop{\mathbb{E}}_t \left[(\tau_2(t))^{-1} H \tau_1(t)\right] \tag{124}$$

Then:

1. If τ_1 and τ_2 are not isomorphic, $H_0 = 0$.

2. If $\mathcal{H}_1 = \mathcal{H}_2$ and $\tau_1 = \tau_2$, then H_0 is a homothety ratio $\lambda = \frac{1}{n}\operatorname{Tr}(H)$, where $n = dim(\mathcal{H}_1)$.

Proof. To prove property 1, by the first part of Schur's Lemma, it suffices to show

$$\tau_2(s)H_0 = H_0\tau_1(s) \tag{125}$$

We compute:

$$\begin{aligned}(\tau_2(s))^{-1} H_0 \tau_1(s) &= (\tau_2(s))^{-1} \cdot \mathop{\mathbb{E}}_t \left[(\tau_2(t))^{-1} H \tau_1(t)\right] \cdot \tau_1(s)\\ &= \mathop{\mathbb{E}}_t \left[(\tau_2(s))^{-1}(\tau_2(t))^{-1}\right] H\tau_1(t) \cdot \tau_1(s)\\ &= \mathop{\mathbb{E}}_t \left[(\tau_2(ts))^{-1}\right] H\tau_1(st) && (126)\\ &= \mathop{\mathbb{E}}_t \left[(\tau_2(ts))^{-1} H\tau_1(st)\right]\\ &= H_0\end{aligned}$$

as required.

To prove the second part of the corollary, since trace is defined linearly:

$$\operatorname{Tr}(H_0) = \mathop{\mathbb{E}}_t \left[\operatorname{Tr}((\tau_1(t))^{-1} H\tau_1(t))\right] \tag{127}$$

Since

$$\operatorname{Tr}((\tau_1(t))^{-1} H\tau_1(t)) = \operatorname{Tr}(H) \tag{128}$$

Then:

$$\operatorname{Tr}(H_0) = \frac{1}{g} \cdot g \cdot \operatorname{Tr}(h) = \operatorname{Tr}(h) \tag{129}$$

where g is the order of G.

Since $\operatorname{Tr}(h) = n \cdot \lambda$,

$$\lambda = \frac{1}{n}\operatorname{Tr}(H) \tag{130}$$

as required. □

Corollary 4.16. *Let $\tau_1 : G \to \mathcal{U}(\mathcal{H}_1)$ and $\tau_2 : G \to \mathcal{U}(\mathcal{H}_2)$ be given in matrix form such that for all $t \in G$:*

$$\tau_1(t) = (r_{i_1 j_1}(t)) \tag{131}$$

$$\tau_2(t) = (r_{i_2 j_2}(t)) \tag{132}$$

Let the linear map H from $\mathcal{H}_1$ to $\mathcal{H}_2$ be defined by the matrix $(x_{i_2 i_1})$ and let H_0 be defined by the matrix $(x_{0 i_2 i_1})$, then by definition of H_0 for all $t \in G$:

$$x_{0 i_2 i_1} = \mathop{\mathbb{E}}_{t} \left[r_{i_2 j_2}(t^{-1}) x_{i_2 i_1} r_{i_1 j_1}(t) \right] \tag{133}$$

Then in case 1:

$$\mathop{\mathbb{E}}_{t} [r]_{i_2 j_2} (t^{-1}) r_{j_1 i_1}(t) = 0 \text{ for arbitrary } i_1, i_2, j_1, j_2 \tag{134}$$

In case 2:

$$\mathop{\mathbb{E}}_{t} [r]_{i_2 j_2} (t^{-1}) r_{j_1 i_1}(t) = \frac{1}{n} \delta_{i_2 i_1} \delta_{j_2 j_1} = \begin{cases} \frac{1}{n} \text{ if } i_1 = i_2 \text{ and } j_1 = j_2 \\ 0 \text{ otherwise} \end{cases} \tag{135}$$

Proof. To prove the first part, we have $H_0 = 0$.

$$x_{0 i_2 i_1} = \mathop{\mathbb{E}}_{t} \left[r_{i_2 j_2}(t^{-1}) x_{i_2 i_1} r_{i_1 j_1}(t) \right] = 0 \tag{136}$$

Note that

$$x r_{i_2 j_2}(t^{-1}) x_{i_2 i_1} r_{i_1 j_1}(t) \tag{137}$$

is a linear functional with respect to $x_{i_2 i_1}$. Hence the linear functional

$$\mathop{\mathbb{E}}_{t} \left[r_{i_2 j_2}(t^{-1}) r_{j_1 i_1}(t) \right] = 0 \tag{138}$$

For the second part, we have $H_0 = \lambda$, where $\lambda = \frac{1}{n} Tr(h)$.
Note that

$$\lambda = \frac{1}{n} \sum \delta_{i_2 i_1} x_{i_2 i_1}, \text{ where } \delta_{j_2 j_1} \text{ is the Kronecker symbol} \tag{139}$$

Hence:

$$\mathop{\mathbb{E}}_{t} \left[r_{i_2 j_2}(t^{-1}) x_{i_2 i_1} r_{j_1 i_1}(t) \right] = \frac{1}{n} \sum_{j_1, j_2} \delta_{i_2 i_1} \delta_{j_2 j_1} x_{i_2 i_1} \tag{140}$$

as required. □

Remark 4.17. Let ϕ and φ be functions on G, define $\langle \phi, \varphi \rangle$ as follows:

$$\langle \phi, \varphi \rangle = \mathop{\mathbb{E}}_{t} [\phi] (t^{-1}) \varphi(t) = \frac{1}{g} \sum_{t \in G} \phi(t) \varphi(t^{-1}) \tag{141}$$

Therefore by definition, we have

$$\langle \phi, \varphi \rangle = \langle \varphi, \phi \rangle \tag{142}$$

With this notation, the previous corollary becomes the following:

$$\langle r_{i_2 j_2}, r_{j_1 i_1} \rangle = 0 \tag{143}$$

$$\langle r_{i_2 j_2}, r_{j_1 i_1} \rangle = \frac{1}{n} \delta_{i_2 i_1} \delta_{j_2 j_1} \tag{144}$$

Remark 4.18. Suppose the matrices $(r_{ij}(t))$ are unitary matrices. Then we have:

$$r_{ij}(t^{-1}) = r_{ji}(t)^* \tag{145}$$

(This is equivalent to $U^{-1} = U^\dagger$)

And the previous corollary just become the *orthogonality relations* for the scalar product $(\phi|\varphi)$ defined in the following section.

We'll do some work in the Hilbert space $\mathbb{C}^G$ with its standard basis $\{|g\rangle \mid g \in G\}$.

If $\chi : G \to \mathbb{C}$ is a character, let $|\chi\rangle := \frac{1}{\sqrt{|G|}} \sum_g \chi(g) |g\rangle$, so that

$$\langle \chi | \chi \rangle = \mathop{\mathbb{E}}_g \left[\overline{\chi(g)} \chi(g) \right]. \tag{146}$$

Theorem 4.19. *1. If χ is the character of an irreducible representation, then $\|\chi\| = \langle \chi | \chi \rangle = 1$.*

2. If χ and χ' are the characters of two inequivalent irreducible representations, then χ and χ' are orthogonal, i.e. $\langle \chi | \chi' \rangle = 0$.

Proof. Let τ be a linear representation of G on $\mathcal{H}$ with character χ. Assume $\tau(t)$ has matrix form $(r_{ij}(t))$. Then $\chi(t) = \sum_i r_{ii}(t)$. Hence we have:

$$(\chi|\chi) = \langle \chi, \chi \rangle = \sum_{i,j} \langle r_{ii}, r_{jj} \rangle = \frac{\sum_{i,j} \delta_{ij}}{n} = \frac{n}{n} = 1 \tag{147}$$

where n is the dimension of τ.

To prove the second statement:

$$(\chi|\chi') = \langle \chi, \chi' \rangle = \sum_{i,j} \langle r_{ii}, r'_{jj} \rangle = 0 \tag{148}$$

(We note that both $(\chi|\chi) = \langle \chi, \chi \rangle$ and $(\chi|\chi') = \langle \chi, \chi' \rangle$ rely on remark **??**) □

Corollary 4.20. *Inequivalent irreducible representations have distinct characters.*

Proof. For inequivalent σ_1, σ_2 with characters χ_1, χ_2, the states $|\chi_1\rangle$ and $|\chi_2\rangle$ are both nonzero (they each have norm 1) and they are orthogonal, so in particular they are not equal. □

Corollary 4.21. *The irreducible characters form an orthonormal basis for the Hilbert space of class functions.*

Proof. We've already shown that they have unit norm and are orthogonal to each other. So they form an orthonormal basis for their span, whatever that is. All characters are already class functions, so it suffices to show that the dimension of the space of class functions is equal to the number of irreducible characters. (TODO: is this already a lemma we can reference? or does the proof go here?) □

Theorem 4.22. *Let τ be a linear representation of G on $\mathcal{H}$ with character ϕ, and suppose $\mathcal{H}$ decomposes into a direct sum of irreducible representations:*

$$\mathcal{H} = W_1 \oplus ... \oplus W_k \tag{149}$$

Then, if an arbitrarily chosen W is an irreducible representation with character χ, the number of W_i isomorhpic to W is equal to the scalar product:

$$(\phi|\chi) = \langle \phi, \chi \rangle \tag{150}$$

Proof. Let χ_i be the character of W_i, then by proposition 4.8:

$$\phi = \chi_1 + ... + \chi_k \tag{151}$$

Therefore:

$$(\phi|\chi) = (\chi_1 + ... + \chi_k|\chi) = (\chi_1|\chi) + ...(\chi_k|\chi) \tag{152}$$

Then by theorem 4.22:

$$(\chi_i|\chi) = \begin{cases} 1 \text{ if } \chi_i, \chi \text{ are isomorphic} \\ 0 \text{ if } \chi_i, \chi \text{ are not isomorphic} \end{cases} \tag{153}$$

Then the result of the theorem easily follows. □

Example 4.23. Note that the two representations of $\rho(13)$ given in matrix form are isomorphic:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & w^2 \\ 0 & w & 0 \end{pmatrix} = T(\rho(13))T^{-1} \simeq \rho(13) = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \tag{154}$$

Remark 4.24. Given a tensor product $W_i \otimes W_j$, the product $\chi_i \cdot \chi_j$ decomposes into

$$\chi_i \cdot \chi_j = \sum_{i,j} m_{ij}^k \chi_k \tag{155}$$

where m_{ij}^k are integers ≥ 0.

Theorem 4.25. *If ϕ is the character of a representation $\mathcal{H}$, $(\phi|\phi)$ given is a positive integer, then:*

$$(\phi|\phi) = 1 \text{ if and only if } \mathcal{H} \text{ is irreducible.} \tag{156}$$

Proof. We write the representation space $\mathcal{H}$ as a direct sum of irreducible representation spaces:

$$\mathcal{H} = m_1 W_1 \oplus ... \oplus m_h W_h \tag{157}$$

By theorem 4.22:

$$m_i = (\phi|\chi_i) \tag{158}$$

Then by theorem 4.22:

$$(\phi|\phi) = (\sum_{i=1}^{h} m_i \cdot \chi_i | \sum_{i=1}^{h} m_i \cdot \chi_i) \tag{159}$$

$$= \sum_{i=1}^{h} {m_i}^2 \tag{160}$$

$\sum_{i=1}^{h} {m_i}^2$ is equal to 1 if and only if one of the m_i is equal to 1 and all other m_is equal to 0. Then $\mathcal{H}$ is isomorphic to exactly one of the W_is. Since all W_is are irreducible, $\mathcal{H}$ is irreducible as well. □

Definition 4.26 (regular representation)**.** Recall the definition of regular representation (3.6) of G, which has basis $|t\rangle_{t\in G}$ indexed by the elements t of G. τ is defined such that for all $s \in G, |t\rangle \in \mathcal{H}$:

$$\tau(s)\,|t\rangle = |st\rangle \tag{161}$$

Lemma 4.27. *Given τ as the regular representation of G on $\mathcal{H}$, then for $s \neq 1$ and $s \in G$, the diagonal terms of the matrix of $\tau(s)$ are all zero. In particular,* $\operatorname{Tr}\tau(s) = 0$.

Proof.

$$\langle s|\tau(g)|s\rangle = \langle s|gs\rangle = \delta_s^{gs} = \delta_1^g. \tag{162}$$

□

Proposition 4.28. *The character r_G of the regular representation is given by the following formulas:*

$$r_G(1) = g, \textit{where}\,|G| = g \tag{163}$$

$$r_G(s) = 0 \textit{ if } s \neq 1 \tag{164}$$

Proof. To prove the first equation, we have:

$$\operatorname{Tr}(\tau(1)) = \operatorname{Tr}(I) = dim(R) = g \tag{165}$$

To prove the second equation, by lemma 4.27, if $s \neq 1$, all the diagonal terms are equal to 0, hence the result follows. □

Corollary 4.29. *Every irreducible representation W_i is contained in the regular representation with multiplicity equal to its degree n_i.*

Proof. By theorem 4.22:

$$n_i = (r_G|\chi_i) = \langle r_G, \chi_i \rangle = \frac{1}{g} \sum_{s \in G} r_G(s^{-1}) \chi_i(s) \tag{166}$$

Hence:

$$r_G(1) = g, \text{where } |G| = g \tag{167}$$

$$r_G(s) = 0 \text{ if } s \neq 1 \tag{168}$$

Therefore:

$$\frac{1}{g} \sum_{s \in G} r_G(s^{-1}) \chi_i(s) = \frac{1}{g} r_G(1) \chi_i(1^{-1}) = \frac{1}{g} g \chi_i(1) = \chi_i(1) = n_i \tag{169}$$

This completes the proof. □

Corollary 4.30. *1. The degrees n_i satisfy the following relation:*

$$\sum_{i=1}^{h} {n_i}^2 = g, \text{ where } |G| = g \tag{170}$$

2. If $s \in G$ and $s \neq 1$, then we have

$$\sum_{i=1}^{h} n_i \chi_i(s) = 0 \tag{171}$$

Proof. By Corollary 3.22, we have for all $s \in G$:

$$r_G(s) = \sum_{i=1}^{h} n_i \chi_i(s) \tag{172}$$

Let $s = 1$, then equation (81) becomes:

$$g = r_G(1) = \sum_{i=1}^{h} n_i \chi_i(1) = \sum_{i=1}^{h} {n_i}^2 \tag{173}$$

This completes the proof of the first part of the corollary.

For the second case, clearly, if $s \neq 1$, then $\chi_i(s)$ for all i is equal to 0, hence

$$\sum_{i=1}^{h} n_i \chi_i(s) = 0 \tag{174}$$

□

Remark 4.31. A representation of G is irreducible if and only if the following holds:

$${n_1}^2 + ... + {n_k}^2 = g \tag{175}$$

Proof. Suppose we have constructed mutually nonisomorphic irreducible representations of degrees $n_1, ..., n_k$ of $W_1, ..., W_k$, then for each $1 \leq i \leq k$, we have

$$n_i \chi_i(1) = n_i^2 \tag{176}$$

Hence if $\sum_i {n_i}^2 = g$, all W_is are irreducible. □

Definition 4.32 (**class function**). A function f on G is called a *class function* if f satisfies:

$$f(tst^{-1}) = f(s) \text{ for all } s, t \in G \tag{177}$$

Proposition 4.33. *Let f be a class function on G, and let $\tau : G \to \mathcal{UH}$ be a unitary representation of G. Let τ_f be the linear mapping of $\mathcal{H}$ onto itself:*

$$\tau_f = \sum_{t \in G} f(t)\tau(t) \tag{178}$$

If $\mathcal{H}$ is irreducible of degree n and character χ, then τ_f is a homothety of ratio λ:

$$\lambda = \frac{1}{n} \sum_{t \in G} f(t)\chi(t) = \frac{g}{n}(f|\chi^*) \tag{179}$$

Proof. Note that we have

$$\tau(s)^{-1}\tau_f\tau(s) = \tau(s)^{-1}(\sum_{t \in G} f(t)\tau(t))\tau(s) \tag{180}$$

$$= \sum_{t \in G} f(t)\tau(s)^{-1}\tau(t)\tau(s) \tag{181}$$

$$= \sum_{t \in G} f(t)\tau(s^{-1}ts) \tag{182}$$

$$\tag{183}$$

Let $u = s^{-1}ts$, then we have $t = sus^{-1}$, hence we have:

$$\tau(s)^{-1}\tau_f\tau(s) = \sum_{t \in G} f(t)\tau(s^{-1}ts) = \sum_{u \in G} f(sus^{-1})\tau(u) \tag{184}$$

Since f is a class function on G, i.e., $f(tst^{-1}) = f(s)$ for all $s, t \in G$, we have

$$\sum_{u \in G} f(sus^{-1})\tau(u) = \sum_{u \in G} f(u)\tau(u) = \tau_f \tag{185}$$

Hence we have

$$\tau(s)^{-1}\tau_f\tau(s) = \tau_f \tag{186}$$

$$\tau_f\tau(s) = \tau_f\tau(s) \tag{187}$$

Then by the second part of Schur's lemma, we have that τ_f is a homothety with scalar λ. Hence the trace of τ_f is given by $n\lambda$.

We have:

$$\sum_{t \in G} f(t) \operatorname{Tr}(\tau(t)) = \sum_{t \in G} f(t)\chi(t) \tag{188}$$

Hence

$$n\lambda = \sum_{t \in G} f(t)\chi(t) = g \cdot (f|\chi^*) \tag{189}$$

Therefore we have

$$\lambda = \frac{g}{n} \cdot (f|\chi^*) \tag{190}$$

This completes the proof. □

Theorem 4.34. *The characters $\chi_1, ..., \chi_h$ form an orthonormal basis of $\mathcal{H}$.*

Proof. We have already shown that the χ_is form an orthonormal system in H. Hence it suffices to show that the χ_is generate H.

$$\tau(f)\,|0\rangle = \sum_{t\in G} f(t)\tau(t)\,|0\rangle = \sum_{t\in G} f(t)\,|t\rangle \tag{191}$$

□

Theorem 4.35. *The number of irreducible representations of G (up to isomorphism) is equal to the number of classes of G.*

Proof. Let $C_1, ..., C_k$ be distinct classes of G.

The dimension of the space H of class functions is equal to k.

As we have seen before in the previous theorem, this dimension k is equal to the number of irreducible representations of H, as required. □

Proposition 4.36. *Let $s \in G$, and let $c(s)$ be the number of elements in the conjugacy class of s. Then we have:*

1.

$$\sum_{i=1}^{h} \chi_i(s)^* \chi_i(s) = \frac{g}{c(s)} \tag{192}$$

2. For $t \in G$ not conjugate to s, we have

$$\sum_{i=1}^{h} \chi_i(s)^* \chi_i(s) = 0 \tag{193}$$

Proof. Let f_s be the function equal to 1 on the class of s and equal to 0 elsewhere. We claim that f_s is a class function. Indeed...

Hence we have:

$$f_s = \sum_{i=1}^{h} \lambda_i \chi_i \tag{194}$$

where

$$\lambda_i = (f_s|\chi_i) = \frac{c(s)}{g}\chi_i(s)^* \tag{195}$$

Then for each $t \in G$, we have:

$$f_s(t) = \frac{c(s)}{g} \sum_{i=1}^{h} \chi_i s^* \chi_i(t) \tag{196}$$

Let $t = s$, we obtain:

$$\sum_{i=1}^{h} \chi_i(s)^* \chi_i(s) = \frac{g}{c(s)} \tag{197}$$

which proves part 1 of the proposition.

Let t not be a conjugate of s, then we have

$$\sum_{i=1}^{h} \chi_i(s)^* \chi_i(s) = 0 \tag{198}$$

which proves part 2 of the proposition. □

5 Subgroups, products, induced representations

Theorem 5.1. *The following two statements are equivalent:*

1. *G is a abelian.*
2. *All the irreducible representations of G have degree 1.*

Proof. First note that given an abelian group G, since $gag^{-1} = a$ for all a and g in G, $Cl(a) = \{a\}$ for all a in G, the number of classes of G is equal to the order of G.

Assume $\tau : G \to \mathcal{U}(\mathcal{H})$ is an irreducible representation of G:

$$\mathcal{H} = W_1 \oplus ... \oplus W_h \tag{199}$$

Let g be the order of G, and let $(n_1, ..., n_h)$ be the dimensions of the W_is, respectively. By theorem 4.35, h is the number of of classes of G.

Since G is abelian, $h = g$:

$$h = g = n_1^2 + ... + n_h^2 \tag{200}$$

Therefore $n_i = 1$ for all i. □

Corollary 5.2. *Let A be an abelian subgroup of G, let a be the order of A and g be the order of G. Then each irreducible representation of G has dimension* $\leq \frac{g}{a}$.

Proof. Let $\tau : G \to \mathcal{U}(\mathcal{H})$ be an irreducible representation of G. Since we are given the abelian subgroup A, we can define a subrepresentation of A as $\tau_A : A \to \mathcal{U}(W)$, where $W \subset \mathcal{H}$ is a Hilbert subspace stable under G.

By theorem 5.1, $dim(W) = 1$. Let $s \in G$, define $\mathcal{H}'$ to be the Hilbert subspace of $\mathcal{H}$ generated by the images $\tau(s)W$.

Note that $\mathcal{H}'$ is stable under G. Since τ is an irreducible representation of G, we must have $\mathcal{H}' = \mathcal{H}$.

Hence for $s \in G$, $t \in A$:

$$\tau(st)W = \tau(s)\tau(t)W = \tau(s)W \tag{201}$$

(for $t \in A$, $\sigma(t)W = W$)

Hence the number of distinct $\tau(s)W$ is at most $\frac{g}{a}$.

$$dim(\mathcal{H}) \leq \frac{g}{a} \tag{202}$$

since $\mathcal{H}$ is the direct sum sum of the $\sigma(s)W$. □

Definition 5.3 (Tensor product of representations)**.** Let $\sigma : G_1 \to \mathcal{U}(\mathcal{H}_1)$ and $\tau : G_2 \to \mathcal{U}(\mathcal{H}_2)$ be two linear representations of groups G_1 and G_2 in $\mathcal{H}_1$ and $\mathcal{H}_2$ respectively.

Define the linear representation $\sigma \otimes \tau$ to be the *tensor product* of representations σ and τ as follows:

$$(\sigma \otimes \tau)(s_1, s_2) = \sigma(s_1) \otimes \tau(s_2) \tag{203}$$

where $s_1 \in G_1$ and $s_2 \in G_2$.

Lemma 5.4. *If χ_1 is the character of σ, and χ_2 is the character of τ, then the character χ of $\sigma \otimes \tau$ is given by:*

$$\chi(s_1, s_2) = \chi_1(s_1) \cdot \chi_2(s_2) \tag{204}$$

Proof. Let A_{ij} be the matrix of $\sigma(s_1)$, and B_{ij} be the matrix of $\tau(s_2)$. Then:

$$\chi_1(s_1) = \sum_i a_{ii} \tag{205}$$

$$\chi_2(s_2) = \sum_i b_{ii} \tag{206}$$

Therefore:

$$\chi_1(s_1)\chi_2(s_2) = \sum_i a_{ii} \sum_j b_{jj} \tag{207}$$

The matrix of $\sigma \otimes \tau$ has trace:

$$\mathrm{Tr}(\sigma \otimes \tau) = \sum_{i,j} a_{ii} b_{jj} \tag{208}$$

Since

$$\sum_i a_{ii} \sum_j b_{jj} = \sum_{i,j} a_{ii} b_{jj} \tag{209}$$

$\chi(s_1, s_2) = \chi_1(s_1) \cdot \chi_2(s_2)$, as required. □

Remark 5.5. When G_1 and G_2 are equal to the same group G, the representation $\sigma \otimes \tau$ defined above is a representation of $G \times G$.

Remark 5.6. When restricted to the diagonal subgroup of $G \times G$, i.e., the set of elements given by $H = \{(g, g) | g \in G\}$ has the representation denoted by $\sigma \otimes \tau$. But it is necessary to distinguish these two representations.

Theorem 5.7. *1. If σ and τ are irreducible, then $\sigma \otimes \tau$ is an irreducible representation of $G_1 \times G_2$.*

2. Each irreducible representation of $G_1 \times G_2$ is isomorphic to a representation $\sigma \otimes \tau$, where σ is an irreducible representation of G_1, and τ is an irreducible representation of G_2.

Proof. Let g_1 be the order of G_1, g_2 be the order of G_2, and g be the order of $G_1 \times G_2$.

We first prove the first part of the theorem. Note that if σ and τ are irreducible, by theorem 4.31:

$$\frac{1}{g_1} \sum_{s_1} |\chi_1(s_1)|^2 = 1 \tag{210}$$

$$\frac{1}{g_2} \sum_{s_2} |\chi_2(s_2)|^2 = 1 \tag{211}$$

Then by lemma 5.4:

$$\frac{1}{g_1} \sum_{s_1} |\chi_1(s_1)|^2 \frac{1}{g_2} \sum_{s_2} |\chi_2(s_2)|^2 = \frac{1}{g_1 g_2} \sum_{s_1} |\chi_1(s_1)|^2 \sum_{s_2} |\chi_2(s_2)|^2 \tag{212}$$

$$= \frac{1}{g} \sum_{s_1, s_2} |\chi(s_1, s_2)|^2 = 1 \tag{213}$$

By the converse of remark 4.31, $\sigma \otimes \tau$ is an irreducible representation of $G_1 \times G_2$, as required.

Now we prove the second part of the theorem. We first claim that each class function f is orthogonal to the characters of the form $\chi_1(s_1)\chi_2(s_2)$.

Hence it suffices to show that each class function f on $G_1 \times G_2$ is zero.

Suppose then we have:

$$\sum_{s_1,s_2} f(s_1,s_2)\chi_1(s_1)^*\chi_2(s_2)^* = 0 \tag{214}$$

Fixing χ_2, let's define

$$g(s_1) = \sum_{s_2} f(s_1,s_2)\chi_2(s_2)^* \tag{215}$$

Then we have for all χ_1:

$$\sum_{s_1} g(s_1)\chi_1(s_1)^* = 0 \tag{216}$$

Note that g is a class function. Therefore this implies that $g = 0$.

Similarly, the same statement holds for for χ_2 when fixing χ_1, therefore we conclude that $f(s_1, s_2) = 0$. □

(TODO: complete proof)

Remark 5.8 (Alternate Proof). We prove the second part of **Theorem 5.7** by computing the sum of the squares of the degrees of the representations $\sigma \otimes \tau$, then we check that the equation

$$\sum_{i=1}^{n} n_i^2 = g \tag{217}$$

is satisfied, where the n_is are the degrees of the irreducible representations.

Definition 5.9 (System of Representatives)**.** If we choose an element from each left coset of H, we obtain a subset R of G called a *system of representatives* of G/H, each s in G can be written uniquely $s = rt$, where $r \in R$ and $t \in H$.

Definition 5.10 (Induced Representations)**.** Let $\sigma : G \to \mathcal{U}(\mathcal{H})$ be a unitary representation of G, and let $\sigma_H : H \to \mathcal{U}(W)$ be the subrepresentation restricted to the subgroup H, and W a Hilbert subspace of $\mathcal{H}$ stable under G.

$$\sigma(st)W = \sigma(s)\sigma(t)W = \sigma(s)(\sigma(t)W) = \sigma(s)W \tag{218}$$

If ψ is a left coset of of H, we can define a subspace W_ψ to be $\sigma(s)W$ for any $s \in \psi$. It is clear that the W_ψ are permuted among themselves by the $\sigma(s)$, $s \in G$. Therefore the sum $\sum_{\psi \in G/H} W_\psi$ is a suprepresentation of V.

We say that the representation σ of G in V is *induced* by the representation σ_H of H in W if V is equal to the sum of the W_ψ ($\psi \in G/H$) and if this sum is direct, i.e., $V = \oplus_{\psi \in G/H} W_\psi$.

Remark 5.11. Each $x \in V$ can be written uniquely as $\sum_{\psi \in G/H} x_\psi$, with $x_\psi \in W_\psi$ for each ψ.

Remark 5.12. If R is a system of representatives of G/H, the vector space V is the direct sum of the $\sigma(r)W$, with $r \in R$.

In particular, we have:

$$dim(V) = \sum_{r \in R} dim(\sigma(r)W) = (G : H) \cdot dim(W) \tag{219}$$

Lemma 5.13. *Suppose that $(\mathcal{H}, \sigma)$ is induced by (W, θ). Let $\sigma' : G \to \mathcal{U}(\mathcal{H}')$ be a linear representation of G, and let $f : W \to \mathcal{H}'$ be a linear map such that*

$$f(\theta(t)w) = \sigma'(t)f(w) \text{ for all } t \in H \text{ and } w \in W \tag{220}$$

Then there exists a unique linear map $F : \mathcal{H} \to \mathcal{H}'$ which extends f and satisfies for all $s \in G$:

$$F(\sigma(s)) = \sigma'(s)F \tag{221}$$

Proof. If $x \in \sigma(s)W$, then $\sigma(s)^{-1}x \in W$.

If F satisfies the above stated conditions, then:

$$F(x) = F(\sigma(s)\sigma(s)^{-1}x) \tag{222}$$
$$= \sigma'(s)F(\sigma(s)^{-1}x) \tag{223}$$
$$= \sigma'(s)f(\sigma(s)^{-1}x) \tag{224}$$
$$\tag{225}$$

Note that this equation proves the uniqueness of F because it determines F on $\sigma(s)W$, and therefore on V as well because V is the sum of $\sigma(s)W$.

Now let $x \in W_\psi$, and choose $s \in \psi$. We define $F(x)$ by:

$$F(x) = \sigma'(s)f(\sigma(s)^{-1}x) \tag{226}$$

Note that the definition of $F(x)$ does not depend on the choice of $s \in \psi$. If we replace s by st, then we have:

$$\sigma'(st)f(\sigma(st)^{-1}x) = \sigma'(s)\sigma'(t)f(\sigma_H(t)^{-1}\sigma(s)^{-1}x) \tag{227}$$
$$= \sigma'(s)(\sigma_H(t)\sigma_H(t)^{-1}\sigma(s)^{-1}x) \tag{228}$$
$$= \sigma'(s)f(\sigma(s)^{-1}x) \tag{229}$$

Therefore since V is the direct sum of the W_ψ, there exists a unique linear map $F : V \to V'$ which satisfies

$$F(\sigma(s)) = \sigma'(s)F \text{ for all } s \in G \tag{230}$$

□

Example 5.14 (Regular Representation). Let $\mathcal{H}$ be the regular representation space of G, then the Hilbert space $\mathcal{H}$ has a basis $|t\rangle_{t\in G}$ such that

$$\sigma(s)\,|t\rangle = |st\rangle \text{ for } s \in G, t \in G \tag{231}$$

Let W be the Hilbert subspace of $\mathcal{H}$ with basis $|t\rangle_{t\in H}$. Then representation θ of H in W is the regular representation of H, and it is clear the σ is induced by θ.

Example 5.15. If $(\mathcal{H}, \sigma)$ is induced by (W, θ), and if W_1 is a stable subspace of W, the subspace $V_1 = \sum_{r\in R} \sigma(r)W_1$ of V is stable under G, and the representation of G in V_1 is induced by the representation of H in W_1.

Example 5.16. If σ_1 is induced by θ_1 and σ_2 is induced by θ_2, then $\sigma_1 \oplus \sigma_2$ is induced by $\theta_1 \oplus \theta_2$.

Theorem 5.17. *Let (W, σ_H) be a linear representation of H. There exists a linear representation (V, σ) of G which is induced by (W, σ_H), and it is unique up to isomorphism.*

Proof. By **Example 5.16**, we may assume that θ is irreducible. θ is isomorphic to a subrepresentation of the regular representation of H, which can be induced to the regular representation of G. By **Example 5.14**, θ can be induced as well.

Now we prove the uniqueness of σ up to isomorphism.

Assume the contrary and let (V, σ) and (V', σ') be two representations induced by (W, θ).

By **Lemma 5.13**, there exists $F : V \to V'$ which satisfies $F(\sigma(s)) = \sigma'(s) \circ F$ for all $s \in G$. Since V' and V has the same dimension, namely, $(G : H) \cdot dim(W)$, we conclude that F is an isomorphism, which completes the proof. □

Theorem 5.18. *Let h be the order of H and let R be a system of representatives of G/H. For each $u \in G$, we have:*

$$\chi_\sigma(u) = \sum_{r\in R \ r^{-1}ur\in H} \chi_\theta(r^{-1}ur) = \frac{1}{h} \sum_{s\in G \ s^{-1}us\in H} \chi_\theta(s^{-1}us) \tag{232}$$

In particular, $\chi_\sigma(u)$ is a linear combination of the values of χ_θ on the intersection of H with the conjugacy class of u in G.

Proof. First note that for $r \in R$, the space V is the direct sum of the $\sigma(r)W$.

To determine $\chi_\sigma(u) = Tr_V(\sigma(u))$, we can use a basis of V which is a union of bases of the $\sigma_r W$.

We claim that the indices r such that r_u give zero diagonal terms, and the others give the trace of $\sigma(u)$ on the $\sigma(r)W$.

Hence we obtain the following:

$$\chi_\sigma(u) = \sum_{r\in R_u} Tr_{\sigma(r)W}(\sigma(u, r)) \tag{233}$$

where R_u denotes the set of $r \in R$ such that $r_u = r$, and $\sigma(u, r)$ denotes the restriction of $\sigma(u)$ to $\sigma(r)W$.

Note that r belongs to R_u if and only if ur can be written as rt with $t \in H$, i.e., $r^{-1}ur$ belongs to H.

Hence it suffices to compute $Tr_{\sigma(r)W}(\sigma(u,r))$, for $r \in R_u$. Note that $\sigma(r)$ defines an isomorphism of W onto $\sigma(r)W$, hence we have:

$$\sigma(r) \circ \theta_t = \sigma(u,r) \circ \sigma(r) \tag{234}$$

with $t = r^{-1}ur \in H$.

Note that we have:

$$\chi_\theta(t) = \chi_\theta(r^{-1}ur) \tag{235}$$

Therefore we obtain the following:

$$\chi_\sigma(u) = \sum_{r \in R_u} \chi_\theta(r^{-1}ur) \tag{236}$$

This equation is obtained by noticing that all elements s of G in the left coset rH ($r \in R_u$) satisfy $\chi_\theta(s^{-1}us) = \chi_\theta(r^{-1}ur)$. □

Theorem 5.19 (Frobenius Reciprocity Formula)**.** *The Frobenius Reciprocity Formula is given as follows:*

$$(f_H|\chi_\theta)_H = (f|\chi_\sigma)_G \tag{237}$$

where f is a class function on G, and f_H is the restriction of f to H.

Proof.

$$(f|\chi_\sigma)_G = \frac{1}{|G|}\sum_{t\in G} f(t)\chi_\sigma(t^{-1}) \tag{238}$$

$$= \frac{1}{|G|}\sum_{t\in G}(\frac{1}{|H|}\sum_{s\in G, s^{-1}ts\in H} f_H(s^{-1}ts))\chi_\sigma(t^{-1}) \tag{239}$$

$$= \frac{1}{|G|}\frac{1}{|H|}\sum_{t\in G}\sum_{s\in G} f_H(s^{-1}ts)\chi_\sigma((s^{-1}ts)^{-1}) \tag{240}$$

$$= \frac{1}{|G|}\frac{1}{|H|}\sum_{t\in G}\sum_{s\in G} f_H(t)\chi_\sigma(t^{-1}) \tag{241}$$

$$= \frac{1}{|H|}\sum_{t\in G} f_H(t)\chi_\sigma(t^{-1}) \tag{242}$$

$$= \frac{1}{|H|}\sum_{t\in H} f_H(t)\chi_\sigma(t^{-1}) \tag{243}$$

$$= \frac{1}{|H|}\sum_{t\in H} f_H(t)\chi_\theta(t^{-1}) \tag{244}$$

$$= (f_H|\chi_\theta)_H \tag{245}$$

$$\tag{246}$$

□

6 Examples

In this section, we compute the character tables for the groups S_3, D_4, prove the explicit isomorphism between the Pauli group on one qubit $\mathcal{P}_1$ and D_4, and give the explicit irreducible representation of the standard representation of S_3. Before computing the character tables, we first give two useful theorems in computing character tables:

Theorem 6.1 (Row Orthogonality Theorem)**.** *If τ_1 and τ_2 are two inequivalent irreducible linear representations, and let χ_1 and χ_2 be their characters respectively, then:*

$$\sum_{s\in G}\chi_1(s)\overline{\chi_2(s)} = 0 \tag{247}$$

and

$$\sum_{s\in G}\chi_1(s)\overline{\chi_1(s)} = |G| \tag{248}$$

($|G|$ denotes the order of group G).

Theorem 6.2 (Column Orthogonality Theorem)**.** *For any conjugacy classes c_1 and c_2, pick $g_1 \in c_1$, $g_2 \in c_2$, we have:*

$$\sum_{\chi}\chi(g_1)\chi(g_2^{-1}) = 0 \tag{249}$$

where χ varies over the characters of irreducible linear representations of G.

For a single conjugacy class c and $g \in c$, we have the following:

$$\sum_{\chi}\chi(g)\chi(g^{-1}) = \frac{|G|}{|C|} \tag{250}$$

Example 6.3 (Character Table for S_3). The group S_3 has three equivalence classes determined by the cycle type; in particular, the 1-cycle which is also just the identity element $\{1\}$, the 2-cycle which has order 3 $\{(12),(13),(23)\}$, and the 3-cycle which has order 2 $\{(132),(123)\}$.

Recall from theorem 4.35 that the number of irreducible representations of G (up to isomorphism) is equal to the number of classes of G.

Therefore from theorem 4.35 and remark 4.31 we conclude that there are 3 irreducible representations, and their dimensions are 1,1,2.

Note that both the trivial representation and the alternating representation are irreducible since they are of dimension 1, therefore up to now we have the following character table:

	1-cycle (identity)	2-cycle	3-cycle
trivial representation	1	1	1
alternating representation	1	-1	1
some representation with degree 2	x	y	z

Then applying Theorem 6.1 (172) to the variable x, we have

$$1^2 + 1^2 + x^2 = 6 \tag{251}$$

Hence $x = 2$.

Then applying Theorem 6.1 (172) to the variable x, we have

$$1^2 + (-1)^2 + y^2 = 2 \tag{252}$$

Hence $y = 0$.

Then by applying Theorem 6.1 (171) to the identity element and $g \in 3 - cycle$, we have:

$$1^2 + 1^2 + 2z = 0 \tag{253}$$

Hence $z = -1$. (Note that we cannot use equation (172) here because both 1 and -1 have square equal to 1)

Therefore we obtain the following character table:

	1-cycle (identity)	2-cycle	3-cycle
trivial representation	1	1	1
alternating representation	1	-1	1
some representation with degree 2	2	0	-1

Example 6.4 (Ismorphism between the Pauli Group on one qubit and D_4). The Pauli Group on one qubit is represented by:

$$G = \langle X, J, Z | X^2 = J^2 = Z^2 = 1, [J, X] = [J, Z] = 1, [X, Z] = J \rangle \tag{254}$$

Note that

$$G = \{1, X, Z, XZ, J, XJ, JZ, XJZ\} \tag{255}$$

We prove that the map σ defined by:

$$\sigma(J) = r^2 \tag{256}$$

$$\sigma(X) = s \tag{257}$$

$$\sigma(Z) = rs \tag{258}$$

is a homomorphism with respect to

$$D_4 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\} \tag{259}$$

In fact, this can be proven by applying σ to each element of G:

$$\sigma(1) = 1 \tag{260}$$

$$\sigma(X) = s \tag{261}$$

$$\sigma(XZ) = srs = r \tag{262}$$

$$\sigma(J) = r^2 \tag{263}$$

$$\sigma(XJ) = sr^2 \tag{264}$$

$$\sigma(JZ) = r^3 s \tag{265}$$

$$\sigma(Z) = rs \tag{266}$$

$$\sigma(XJZ) = sr^2 rs = sr^3 s = r^3 \tag{267}$$

Now we define the map $\tau : D_4 \to G$ defined by:

$$\tau(r) = XZ \tag{268}$$

$$\tau(s) = X \tag{269}$$

We prove that this is a homomorphism on G. In fact,

$$\tau(1) = 1 \tag{270}$$

$$\tau(r) = XZ \tag{271}$$
$$\tau(r^2) = XZXZ = J \tag{272}$$
$$\tau(r^3) = JXZ = XJZ \tag{273}$$
$$\tau(s) = X \tag{274}$$
$$\tau(sr) = Z \tag{275}$$
$$\tau(sr^2) = ZXZ = XJ \tag{276}$$
$$\tau(sr^3) = ZXZXZ = ZJ \tag{277}$$

Since both σ and τ are homomorphisms, we have completed the proof that there exists an isomorphism between D_4 and the Pauli Group on one qubit. □

Remark 6.5. We show σ and τ are homomorphisms on the entire group $\mathcal{P}_1$ by checking explicitly on the generators of $\mathcal{P}_1$.

Indeed,

$$\sigma(J)\sigma(X) = r^2 s = \sigma(JX) \tag{278}$$
$$\sigma(J)\sigma(Z) = r^3 s = \sigma(JZ) \tag{279}$$
$$\sigma(X)\sigma(Z) = srs = \sigma(XZ) \tag{280}$$
$$\tau(r)\sigma(s) = XZX = \tau(rs) \tag{281}$$

6.1 Representations of D_n

Example 6.6 (Representation for D_n). D_n is the group of rotations and reflections of the plane which preserve a regular polygon with n vertices. It contains n rotations, and n reflections. (the order of D_n is $2n$) Denote r as the rotation through an angle $\frac{2\pi}{n}$, and let s be one of its reflections, then we have:

$$r^n = 1, s^2 = 1, srs = r^{-1} \tag{282}$$

Each element of D_n can be written uniquely, either in the form r^k, where $0 \leq k \leq n-1$, or of the form sr^k, where $0 \leq k \leq n-1$.

Irreducible Representations of the group D_n (n even ≥ 2) Note that there are 4 irreducible representations of dimension/degree 1. They are obtained by letting ± 1 corresponding to r^k and sr^k in all possible ways. Let the four representations be τ_1, τ_2, τ_3, and τ_4, and let the characters of these representations be χ_1, χ_2, χ_3, and χ_4 respectively. Then up to now we have the following character table:

	r^k	sr^k
χ_1	1	1
χ_2	1	-1
χ_3	$(-1)^k$	$(-1)^k$
χ_4	$(-1)^k$	$(-1)^{k+1}$

Now we consider irreducible representations of degree 2. We claim that σ_h defined in the following way is indeed a representation:

$$\sigma_h(r^k) = \begin{pmatrix} w^{hk} & 0 \\ 0 & w^{-hk} \end{pmatrix} \tag{283}$$

$$\sigma_h(sr^k) = \begin{pmatrix} 0 & w^{-hk} \\ w^{hk} & 0 \end{pmatrix} \tag{284}$$

where $w = e^{\frac{2\pi i}{n}}$ and h an arbitrary integer.

Note that σ_h and σ_{n-h} are isomorphic. Therefore we may assume $0 \leq n \leq \frac{n}{2}$.

Note that when $h = 0$ and $h = \frac{n}{2}$, we have the corresponding representations having characters $\chi_1 + \chi_2$ and $\chi_3 + \chi_4$ respectively.

We claim that when $0 < n < \frac{n}{2}$, the representation σ_h is irreducible.

Proof. Since $w^h \neq w^{-h}$, the only lines stable under $\sigma_h(r^k)$ are the coordinate axes, namely the basis vectors $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ and $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$. Note that these basis vectors are not stable under $\sigma_h(sr^k)$. The same argument shows that $\sigma_h(r^k)$ and $\sigma_h(sr^k)$ are pairwise nonisomorphic. □

The characters of $\sigma_h(r^k)$ and $\sigma_h(sr^k)$ are given by the following:

$$\chi_h(r^k) = w^{hk} + w^{-hk} = 2\cos\frac{2\pi hk}{n} \tag{285}$$

$$\chi_h(sr^k) = 0 \tag{286}$$

We claim that τ_1, τ_2, τ_3, τ_4, and σ_h for $0 < h < \frac{n}{2}$ are the only irreducible representations for D_n.

Proof. Recall Remark 4.32, we compute the sum of squares of the representations.

$$\sum n_i^2 = 4 \times 1^2 + (\frac{n}{2} - 1) \times 2^2 = 2n \tag{287}$$

which is equal to the order of D_n. □

Remark 6.7. The representation σ_h is induced by the representation of C_n with character χ_h.

Example 6.8 (Character Table for D_4). First note that the group $D_4 = \langle r, s | r^4 = s^2 = 1, srs = r^{-1} \rangle$ has 5 conjugacy classes. They are given by

$$\{1\}, \{r^2\}, \{r, r^3\}, \{s, r^s\}, \{rs, r^3 s\} \tag{288}$$

There are 5 irreducible representations of D_4, they are given by:

$$\tau_1, \tau_2, \tau_3, \tau_4, \sigma_1 \tag{289}$$

We obtain the following character table:

	{1}	{r^2}	{r, r^3}	{s, r^s}	{rs, r$^3 s$}
τ_1	1	1	1	1	1
τ_2	1	1	1	-1	-1
τ_3	1	1	-1	1	-1
τ_4	1	1	-1	-1	1
σ_1	2	-2	0	0	0

(290)

	{1}	{J}	{XZ, XJZ}	{X, XJ}	{Z, JZ}
τ_1	1	1	1	1	1
τ_2	1	1	1	-1	-1
τ_3	1	1	-1	1	-1
τ_4	1	1	-1	-1	1
σ_1	2	-2	0	0	0

(291)

7 The regular representation of the one qubit pauli group

The term *quantum fourier transform* is generally used to refer to a particular unitary matrix on $\mathbb{C}^d$. This is a change of basis from a basis of group elements of $\mathbb{Z}_d$ to a basis of characters of $\mathbb{Z}_d$.

Definition 7.1.

The regular representation in its standard basis is a permutation matrix. There is a change of basis (multiple, actually) which takes this permutation matrix to a block matrix with irreps on the blocks. We call any such change of basis a *nonabelian Fourier transform.*

Recall the Pauli Group defined on one qubit:

$$G = \langle X, J, Z | X^2 = J^2 = Z^2 = 1, [J, X] = [J, Z] = 1, [X, Z] = J \rangle \quad (292)$$

Define the *left regular representation* ρ of G by $\rho(g)\,|h\rangle = |gh\rangle$

		$\rho(X)$	$\rho(J)$	$\rho(Z)$
000	1	100 (X)	010 (J)	001 (Z)
100	X	000 (1)	110 (XJ)	111 (XJZ)
001	Z	101 (XZ)	011 (JZ)	000 (1)
010	J	110 (XJ)	000 (1)	011 (JZ)
101	XZ	001 (Z)	111 (XJZ)	110 (XJ)
110	XJ	010 (J)	100 (X)	101 (XZ)
011	JZ	111 (XJZ)	001 (Z)	010 (J)
111	XJZ	011 (JZ)	101 (XZ)	100 (X)

(293)

We use an encoding $\beta : \{0,1\}^3 \to \mathcal{P}_1$ as $\beta(w) := J^{w_0} x^{w_1} z^{w_2}$

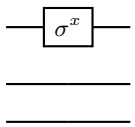
w	$\beta(w)$	$\rho(X)$	$\rho(J)$	$\rho(Z)$
000	1	010 (X)	010 (J)	001 (Z)
001	Z	011 (XZ)	101 (JZ)	000 (1)
010	X	000 (1)	110 (XJ)	111 (XJZ)
011	XZ	001 (Z)	111 (XJZ)	110 (XJ)
100	J	110 (XJ)	000 (1)	101 (JZ)
101	JZ	111 (XJZ)	001 (Z)	100 (J)
110	XJ	100 (J)	010 (X)	011 (XZ)
111	XJZ	101 (JZ)	101 (XZ)	010 (X)

(294)

(TODO: Give the bijection between three bit strings and the pauli group a definition block, so that we can refer to it for setting up the three qubit space. Add a remark about how if we pick a different bijection then $\rho(X)$ is the circuit with a CNOT in it.)

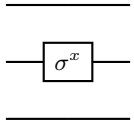
We reinterpret the representation hilbert space $\mathbb{C}^G$ as the three qubit space $(\mathbb{C}^2)^{\otimes 3}$.

We obtain the following circuit diagrams for $\rho(X)$, $\rho(J)$ and $\rho(Z)$:

$\rho(X) =$ 

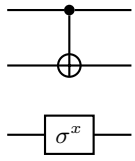
(295)

$$\rho(X) = X \otimes I \otimes I \tag{296}$$

$\rho(J) =$ 

(297)

$$\rho(J) = I \otimes X \otimes I \tag{298}$$

$\rho(Z) =$ 

(299)

We know there's a decomposition $\mathbb{C}^G = \bigoplus_\sigma \mathbb{C}_\sigma^{\otimes n_\sigma}$ with $n_i = \dim \sigma_i$. To start, we want to find four vectors which are simultaneous eigenvectors for all three of $\rho(x), \rho(z), \rho(J)$.

The eigenvectors of the logic gate σ^x are $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

The state $|+++\rangle$ is a simultaenous $+1$-eigenvector for all three operators. Written differently, $|+++\rangle = \frac{1}{\sqrt{8}} \sum_g |g\rangle$. Written this way, it is clearly stabilized by the regular representation.

We have a correspondence between our 4 characters and our 4 stable states. This one corresponds to the trivial character.

so for a character χ of degree 1, we can talk about the state

$$|\chi\rangle := \frac{1}{\sqrt{8}} \sum_g \chi(g) \, |g\rangle \, . \tag{300}$$

Recalling the character table from Equation 291, and letting χ_i refer to the character of irrep τ_i from that table, we have

$$|\chi_1\rangle = \frac{1}{\sqrt{8}} \sum_g |g\rangle = |+\rangle \otimes |+\rangle \otimes |+\rangle \,. \tag{301}$$

$$|\chi_2\rangle = \frac{1}{\sqrt{8}} \left(|1\rangle + |J\rangle + |XZ\rangle + |XJZ\rangle\right) - \frac{1}{\sqrt{8}} \left(|X\rangle + |XJ\rangle + |Z\rangle + |JZ\rangle\right) \tag{302}$$

$$= \frac{1}{\sqrt{8}} \left(|000\rangle + |010\rangle + |101\rangle + |111\rangle\right) - \frac{1}{\sqrt{8}} \left(|100\rangle + |110\rangle + |001\rangle + |011\rangle\right) \tag{303}$$

$$= |-\rangle \otimes |+\rangle \otimes |-\rangle \tag{304}$$

$$|\chi_3\rangle = \frac{1}{\sqrt{8}} \left(|1\rangle + |J\rangle + |X\rangle + |XJ\rangle\right) - \frac{1}{\sqrt{8}} \left(|XZ\rangle + |XJZ\rangle + |Z\rangle + |JZ\rangle\right) \tag{305}$$

$$= \frac{1}{\sqrt{8}} \left(|000\rangle + |010\rangle + |100\rangle + |110\rangle\right) - \frac{1}{\sqrt{8}} \left(|101\rangle + |111\rangle + |001\rangle + |011\rangle\right) \tag{306}$$

$$= |+\rangle \otimes |+\rangle \otimes |-\rangle \,. \tag{307}$$

$$|\chi_4\rangle = \frac{1}{\sqrt{8}} \left(|1\rangle + |J\rangle + |Z\rangle + |JZ\rangle\right) - \frac{1}{\sqrt{8}} \left(|XZ\rangle + |XJZ\rangle + |X\rangle + |XJ\rangle\right) \tag{308}$$

$$= \frac{1}{\sqrt{8}} \left(|000\rangle + |010\rangle + |001\rangle + |011\rangle\right) - \frac{1}{\sqrt{8}} \left(|101\rangle + |111\rangle + |100\rangle + |110\rangle\right) \tag{309}$$

$$= |-\rangle \otimes |+\rangle \otimes |+\rangle \,. \tag{310}$$

So we have a four-dimensional space of stable states. We want to project away from that. We'll be left with a four dimensional subspace which decomposes as a direct sum of two single qubits. By the $2+2 = 2\times 2$ trick, we'll reinterpret this as a tensor product of two qubits.

Four of the basis states of the nonabelian fourier transform decomposition are $H \otimes H \otimes H$ applied to a computational basis state. We might conclude that the unitary we're looking for is $H^{\otimes 3}$.

What happens if we conjugate our regular representation operators by this unitary?

$$H^{\otimes 3} \rho(X) H^{\otimes 3} = Z \otimes I \otimes I \tag{311}$$

$$H^{\otimes 3} \rho(J) H^{\otimes 3} = I \otimes Z \otimes I \tag{312}$$

$$H^{\otimes 3} \rho(Z) H^{\otimes 3} = Z \otimes I \otimes Z \tag{313}$$

$$\mathrm{CNOT} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X \tag{314}$$

$$(H \otimes H)\,\mathrm{CNOT}(H \otimes H) = |+\rangle\langle +| \otimes I + |-\rangle\langle -| \otimes Z \tag{315}$$

$$(H \otimes H)\,\mathrm{CNOT}(H \otimes H) = I \otimes |0\rangle\langle 0| + X \otimes |1\rangle\langle 1|\,. \tag{316}$$

$$(H \otimes H)\,\mathrm{CNOT}_{1,2}(H \otimes H) = \mathrm{CNOT}_{2,1} \tag{317}$$

7.1 Permutation Matrices

$$\rho(X) = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \tag{318}$$

$$\rho(J) = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix} \tag{319}$$

$$\rho(Z) = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \tag{320}$$

$$H^{\otimes 3}\rho(X)H^{\otimes 3} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \end{pmatrix} \tag{321}$$

$$H^{\otimes 3}\rho(J)H^{\otimes 3} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \end{pmatrix} \tag{322}$$

$$H^{\otimes 3}\rho(Z)H^{\otimes 3} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \end{pmatrix} \tag{323}$$

Q: what's the correct order for the bits? A1: J should be the first bit. Once we've ordered the bits correctly, hopefully things go as 000 001 010 011 100 101 110 111

Want a description of the remaining four states (which are the image under $H^{\otimes 3}$ of the states of the form $|1\rangle_J \otimes |\psi\rangle_{XZ}$.

The bell state

$$|\Psi\rangle := |00\rangle + |11\rangle \tag{324}$$

We say $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ is a *pure tensor* if $|\psi\rangle = |\psi\rangle_A \otimes |\psi\rangle_B$ for some vectors $|\psi\rangle_A \in \mathcal{H}_A$, $|\psi\rangle_B \in \mathcal{H}_B$.

Let $|\Psi\rangle = |\psi\rangle \otimes |\phi\rangle$.

Suppose towards a contradiciton that $|\Psi\rangle$ is a pure tensor with $|\Psi\rangle = |\psi\rangle \otimes |\phi\rangle$ and $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$ and $|\phi\rangle = c\,|0\rangle + d\,|1\rangle$.

Then $|\Psi\rangle = ac\,|00\rangle + bd\,|11\rangle + ad\,|01\rangle + bc\,|10\rangle$, so $ac = bd = 1$ and $ad = bc = 0$.

$|\Psi'\rangle := |00\rangle + |01\rangle + |10\rangle + |11\rangle$.

References

[DF04] David Steven Dummit and Richard M Foote. *Abstract algebra*. Vol. 3. Wiley Hoboken, 2004.

[Ser77] Jean-Pierre Serre. *Linear representations of finite groups*. Vol. 42. Springer, 1977.