Representation Theory

Arpon Basu

Last updated June 6, 2024

Contents

This report is based on Steinberg's book [Ste11] on the Representation Theory of finite groups. We thank him for making Representation Theory so accessible.

§1. Group Representations

Definition 1.1 (Representations)**.** Let G be a group. A group homomorphism $\varphi : G \mapsto \mathrm{GL}(V)$ is called a representation of g, where V is a finite-dimensional vector space. We also define $\deg(\varphi) := \dim(V)$.

Remark. Throughout this report, unless otherwise stated, we will always be working with finite-dimensional representations, i.e. we will always take V to be finite-dimensional $\mathbb{C}$-vector space.

For any $g \in G$, we abbreviate $\varphi(g)$ as φ_g.
We want our notion of representations to be invariant under basis changes of our vector space. Motivated by this, we define:

Definition 1.2 (Equivalence)**.** Let V, W be vector spaces, and let $T : V \mapsto W$ be a vector space isomorphism. Two representations $\varphi : G \mapsto \mathrm{GL}(V)$ and $\psi : G \mapsto \mathrm{GL}(W)$ are said to be equivalent if the following diagram commutes for every $g \in G$:

$$\begin{array}{ccc} V & \xrightarrow{\varphi_g} & V \\ {\scriptstyle T}\downarrow & & \downarrow{\scriptstyle T} \\ W & \xrightarrow{\psi_g} & W \end{array}$$

In other words, φ_g and ψ_g are similar linear transformations, since $\psi_g = T\varphi_g T^{-1}$ for all $g \in G$.

We now give a very important example of a representation:

Proposition 1. $\mathfrak{S}_n$, namely the symmetric group of n elements, has a degree n representation.

Proof. It is easy to see that $\psi : \mathfrak{S}_n \mapsto \mathrm{GL}_n(\mathbb{C})$ is a representation, where for any $\sigma \in \mathfrak{S}_n$, we define $\psi_\sigma(e_i) := e_{\sigma(i)}$. ■

Remark. Note that since ψ_σ is a linear transformation of $\mathbb{C}^n$, it is enough to specify ψ_σ on a basis of $\mathbb{C}^n$. Indeed, for any $v = \sum_{i=1}^n v_i e_i \in \mathbb{C}^n$, we now have $\psi_\sigma(v) = \sum_{i=1}^n v_i e_{\sigma(i)}$. Similarly, if a set S generates G, then it is enough to specify ψ_s for $s \in S$, to specify the whole representation. To summarize, it is enough to specify the action of the generators of G on some basis of V to specify a representation $\psi : G \mapsto \mathrm{GL}(V)$.

The above proposition extends to any finite group G:

Proposition 2 (Regular Representation)**.** A finite group G of n elements has a degree n representation.

Proof. We shall give an injective group homomorphism $\tau : G \mapsto \mathfrak{S}_n$. Composed with $\psi : \mathfrak{S}_n \mapsto \mathrm{GL}_n(\mathbb{C})$, we obtain a representation $\psi \circ \tau : G \mapsto \mathrm{GL}_n(\mathbb{C})$. Indeed, let $\iota : G \to [n]$ be a bijection. Note that for any $g \in G$, $\pi_g : G \mapsto G, \pi_g(h) := gh$ is a group automorphism, and then we can define τ as $\tau_g := \iota \circ \pi_g \circ \iota^{-1}$. ■

Remark. The above representation is known as a *regular representation* of G.

We now give some more definitions pertaining to representations:

Definition 1.3 (Invariant Subspaces)**.** Let $\psi : G \mapsto \mathrm{GL}(V)$ be a representation, and let W be a subspace of V. We say that W is G-invariant (under ψ) if $\psi_g w \in W$ for all $g \in G, w \in W$.
Furthermore, note that if W is a G-invariant subspace, then $\psi|_W : G \mapsto \mathrm{GL}(W)$ is also a representation. We call $\psi|_W$ a *subrepresentation* of ψ.

Example. A few illustrations are as follows:

1. Note that for any representation $\psi : G \mapsto \mathrm{GL}(V)$, 0 and V are always G-invariant.
2. Consider the representation of $\mathfrak{S}_5$ as in Proposition 1, and let W be the subspace of $\mathrm{GL}_5(\mathbb{C})$ generated by $e_1 + e_2 + e_3 + e_4 + e_5 = \begin{bmatrix}1 & 1 & 1 & 1 & 1\end{bmatrix}^{\mathsf{T}}$. Note that for any $\sigma \in \mathfrak{S}_5$,
$$\psi_\sigma \left(\sum_{i=1}^{5} \lambda e_i \right) = \sum_{i=1}^{5} \lambda e_{\sigma(i)} = \sum_{i=1}^{5} \lambda e_i$$
Thus W is $\mathfrak{S}_5$-invariant.

We also define the direct sum of representations.

Definition 1.4 (Direct Sum of Representations)**.** Given representations $\psi^{(1)} : G \mapsto \mathrm{GL}(V_1)$, $\psi^{(2)} : G \mapsto \mathrm{GL}(V_2)$, we define the direct sum of these representations to be:
$$\psi^{(1)} \oplus \psi^{(2)} : G \mapsto \mathrm{GL}(V_1 \oplus V_2)$$
where $(\psi^{(1)} \oplus \psi^{(2)})_g(v_1, v_2) := (\psi^{(1)}_g v_1, \psi^{(2)}_g v_2)$. We also denote $\underbrace{\psi \oplus \cdots \oplus \psi}_{m \text{ times}}$ as $m\psi$.
In other words, if $\psi^{(1)}_g$ is the matrix M_1, and $\psi^{(2)}_g$ is the matrix M_2, then $(\psi^{(1)} \oplus \psi^{(2)})_g$ is the block matrix $\begin{bmatrix} M_1 & 0 \\ 0 & M_2 \end{bmatrix}$.
Furthermore, note that if $V = W_1 \oplus W_2$, then any representation $\psi : G \mapsto \mathrm{GL}(V)$ decomposes as $\psi = \psi|_{W_1} \oplus \psi|_{W_2}$.

Since we eventually want to decompose all representations as a direct sum of simpler representations, we define some necessary notions:

Definition 1.5 (Irreducible Representations)**.** A representation $\psi : G \mapsto \mathrm{GL}(V)$ is called irreducible if the only G-invariant subspaces are 0 and V.

Example. A few illustrations are in order:

1. Consider the *trivial* representation $\psi : G \mapsto \mathrm{GL}_1(\mathbb{C}) \cong \mathbb{C}^*$, where $\psi_g = 1$ for all $g \in G$. It is easy to see that the trivial representation is irreducible. Indeed, any degree 1 representation has to be irreducible.
2. Consider the dihedral group D_n, and recall that $D_n = \langle r, s | r^n = s^2 = 1, (rs)^2 = 1 \rangle$, where r represents an anticlockwise rotation by $2\pi/n$, and s represents a reflection about the x-axis. Consider the representation $\psi : D_n \mapsto \mathrm{GL}_2(\mathbb{C})$, where
$$r \mapsto \begin{bmatrix} \cos(2\pi/n) & -\sin(2\pi/n) \\ \sin(2\pi/n) & \cos(2\pi/n) \end{bmatrix}, s \mapsto \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

ψ is actually an irreducible representation: Indeed, assume for the sake of contradiction that ψ is not irreducible. Then $\mathbb{C}^2 = W \oplus U$, where W, U are 1-dimensional D_n-invariant subspaces. Let $W = \langle v \rangle$ be generated by v. Then note that v must be an eigenvector of both ψ_r and ψ_s. However, ψ_r, ψ_s don't share any eigenvector, and thus ψ is irreducible.

3. For $n \geq 2$, the representation in Proposition 1 is *not* irreducible.

As hinted before, we shall seek to establish some analogies of representation theory with group theory and linear algebra as follows:

Group Theory	Linear Algebra	Representation Theory
Subgroup	Subspace	G-invariant subspace
Simple group	One-dimensional Subspace	Irreducible Representation

Indeed, the analogy between vector spaces and representations is not too surprising in light of the fact that if $\psi : 0 \mapsto \mathrm{GL}(V)$ is a representation, then ψ_0 is the identity matrix, and consequently, $\psi_0(V) = V$, i.e. vector spaces can be thought of as special cases of representations.
To strengthen the above analogies, we also make the following definitions:

Definition 1.6 (Completely Reducible)**.** A representation ψ is called completely reducible if there exist irreducible representations $\psi^{(1)}, \ldots, \psi^{(r)}$ such that $\psi = \psi^{(1)} \oplus \cdots \oplus \psi^{(r)}$.

Definition 1.7 (Decomposable)**.** A representation $\psi : G \mapsto \mathrm{GL}(V)$ is called decomposable if $V = V_1 \oplus V_2$, where V_1, V_2 are non-zero G-invariant subspaces. ψ is called indecomposable if it is not decomposable.

It is important to note, yet not too difficult to see, that the aforementioned notions are identical for equivalent representations, i.e.

Proposition 3. Let φ, ψ be two equivalent representations. Then φ is decomposable, irreducible, or completely reducible if and only if ψ is decomposable, irreducible, or completely reducible respectively.

Let $\mathrm{U}(V)$ be the group of unitary linear transformations of an inner product space V [1], i.e. if $U \in \mathrm{U}(V)$, then for any two vectors $v_1, v_2 \in V$, $\langle v_1, v_2 \rangle = \langle Uv_1, Uv_2 \rangle$.

Definition 1.8. A group homomorphism $\psi : G \mapsto \mathrm{U}(V) \hookrightarrow \mathrm{GL}(V)$ is called a unitary representation.

Example. A few examples are in order:

1. Note that $\mathrm{U}_1(\mathbb{C}) = \{z \in \mathbb{C} : z\overline{z} = 1\} \cong S^1$. Thus, for example, $\psi : \mathbb{R} \mapsto S^1, x \mapsto e^{2i\pi x}$ is a unitary representation of $\mathbb{R}$.
2. In general, homomorphisms $\psi : G \mapsto S^1$ are 1-dimensional unitary representations.

The reason we care about unitary representations is because they satisfy they are always irreducible or decomposable:

[1] V is a vector space equipped with an inner product, i.e. V is a Hilbert space

Proposition 4. Let $\psi : G \mapsto \mathrm{U}(V)$ be a unitary representation. Then ψ is either irreducible or decomposable.

Proof. Suppose ψ is not irreducible. Then we must have a proper subspace W which is G-invariant. If we can show that $W^\perp$ is G-invariant, then we would be done, since $V = W \oplus W^\perp$. To that extent, let $g \in G, w \in W, v \in W^\perp$ be arbitrary. Then

$$\langle \psi_g v, w \rangle = \langle v, \psi_g^* w \rangle = \langle v, \psi_g^{-1} w \rangle$$

Since $\psi_g : W \mapsto W$ is a full-rank linear transformation, it is bijective, and consequently, there is a $w' \in W$ such that $\psi_g w' = w$. Thus

$$\langle \psi_g v, w \rangle = \langle v, w' \rangle = 0$$

where the last equality follows from the fact that $v \in W^\perp, w' \in W$. Since w was arbitrary, we get $\psi_g v \in W^\perp$, as desired. ■

Finally, we prove that all representations of finite groups are equivalent to some unitary representation.

Theorem 1.1. Every finite-dimensional representation of a finite group G is equivalent to a unitary representation.

Proof. Let $\psi : G \mapsto \mathrm{GL}_n(\mathbb{C})$ be a representation. Consider the matrix:

$$B := \frac{1}{|G|} \sum_{g \in G} \psi_g^* \psi_g$$

Note that B is a positive definite Hermitian matrix: Indeed, for any $v \in V$,

$$v^* B v = \frac{1}{|G|} \sum_{g \in G} v^* \psi_g^* \psi_g v = \frac{1}{|G|} \sum_{g \in G} \|\psi_g v\|^2$$

The above expression is non-negative everywhere and is 0 only when $\psi_g v = 0$ for all g, which happens only when $v = 0$ since ψ_g's are invertible matrices.
Since B is a positive-definite Hermitian matrix, there exists a $T \in \mathrm{GL}_n(\mathbb{C})$ such that $B = T^*T$. Now, consider the vector space isomorphism $\mathbb{C}^n \mapsto \mathbb{C}^n$ given by $v \mapsto Tv$. Note that ψ will now be transformed to the equivalent representation $T\psi T^{-1}$. Thus, if we can show that $T\psi_g T^{-1}$ is unitary for all $g \in G$, we're done. To that end, note that $(T\psi_g T^{-1})^* = (T^{-1})^* \psi_g^* T^* = (T^*)^{-1} \psi_g^* T^*$, and thus

$$(T\psi_g T^{-1})^* \cdot (T\psi_g T^{-1}) = (T^*)^{-1} \psi_g^* T^* T \psi_g T^{-1} = (T^*)^{-1} \psi_g^* B \psi_g T^{-1}$$

Now,

$$\psi_g^* B \psi_g = \frac{1}{|G|} \sum_{h \in G} \psi_g^* \psi_h^* \psi_h \psi_g = \frac{1}{|G|} \sum_{h \in G} \psi_{hg}^* \psi_{hg}$$

where the last equality follows from the fact that ψ is a homomorphism. Now, for any $g \in G$, $h \mapsto hg$ is a group automorphism. Thus $\sum_{h \in G} \psi_{hg}^* \psi_{hg} = \sum_{h \in G} \psi_h^* \psi_h$, and consequently,

$$(T\psi_g T^{-1})^* \cdot (T\psi_g T^{-1}) = (T^*)^{-1} B T^{-1} = (T^*)^{-1} T^* T T^{-1} = I$$

Thus, $T\psi_g T^{-1}$ is unitary, as desired. ■

Corollary 1.2. If ψ is a representation of a finite group, then ψ is either irreducible or decomposable.

Remark. Consider the following finite-dimensional representation:

$$\psi : \mathbb{Z} \mapsto \mathrm{GL}_2(\mathbb{C}), x \mapsto \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}$$

Clearly, the image of ψ doesn't lie in $\mathrm{U}_2(\mathbb{C})$. Furthermore, note that when $x \neq 0$, ψ_x is not diagonalizable: Consequently, ψ can't be equivalent to a unitary representation, since unitary matrices are diagonalizable. Thus, infinite groups can have representations that aren't equivalent to any unitary representation. Furthermore, note that the subspace generated by $\begin{bmatrix} 1 & 0 \end{bmatrix}^{\mathsf{T}}$ is a $\mathbb{Z}$-invariant subspace, and thus ψ is not irreducible. At the same time, ψ is not decomposable either: Indeed, if it were decomposable, then it would be a direct sum of two one-dimensional representations. However, the direct sum of two one-dimensional representations would be a diagonal matrix, and thus ψ can't be equivalent to it since ψ_x is not diagonalizable for $x \neq 0$.

We can finally prove the decomposition theorem we have been hinting at until now.

Theorem 1.3 (Maschke's Theorem)**.** Every representation of a finite group is completely reducible.

Proof. Let $\psi : G \mapsto \mathrm{GL}_n(\mathbb{C})$ be a representation. We induct on n.
If $n = 1$, ψ is irreducible, so we have nothing to prove. Thus, assuming the statement is true for all $n \leq k$, we want to prove it for $n = k + 1$. If ψ is irreducible, we have nothing to prove. Otherwise, by Corollary 1.2, ψ is decomposable, so $\mathbb{C}^{k+1} = V_1 \oplus V_2$, where $\dim(V_1), \dim(V_2) \leq k$, and V_1, V_2 are G-invariant. By induction hypothesis, we have $V_1 = A_1 \oplus \cdots \oplus A_r, V_2 = B_1 \oplus \cdots \oplus B_s$, where A_i, B_j are G-invariant, and $\psi|_{A_i}, \psi|_{B_j}$ are irreducible, for all $i \in [r], j \in [s]$. Consequently,

$$\psi = \bigoplus_{i \in [r]} \psi|_{A_i} \oplus \bigoplus_{j \in [s]} \psi|_{B_j}$$

is the desired decomposition of ψ. ∎

Remark. Thus, if ψ is the representation of a finite group, then

$$\psi \sim \begin{bmatrix} \psi^{(1)} & 0 & \dots & 0 \\ 0 & \psi^{(2)} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \psi^{(m)} \end{bmatrix}$$

where $\psi^{(i)}$ is irreducible for all $i \in [m]$.

§2. Character Theory

Theorem 1.3 makes it clear that to study representations of finite groups, it is enough to study irreducible representations. To do that, we shall equip the space of irreducible representations with further structure, and motivated by that, we define:

Definition 2.1 (Homomorphisms of Representations)**.** Let $\psi^{(1)} : G \mapsto \mathrm{GL}(V), \psi^{(2)} : G \mapsto \mathrm{GL}(W)$ be two representations. We say that a linear map $T : V \mapsto W$ is a homomorphism from $\psi^{(1)}$ to $\psi^{(2)}$ if the following diagram commutes for every $g \in G$:

$$\begin{array}{ccc} V & \xrightarrow{\psi_g^{(1)}} & V \\ {\scriptstyle T}\downarrow & & \downarrow{\scriptstyle T} \\ W & \xrightarrow{\psi_g^{(2)}} & W \end{array}$$

Remark. If T is a bijective linear map, then $\psi^{(1)}, \psi^{(2)}$ are equivalent, i.e. isomorphic.

The set of all homomorphisms from φ to ψ is denoted as $\mathrm{Hom}_G(\varphi, \psi)$. Note that $\mathrm{Hom}_G(\varphi, \psi) \subseteq \mathrm{Hom}_G(V, W)$.
Once we introduce homomorphisms, we immediately have kernels and images, and some useful interpretations of those things.

Proposition 5. Let $T : V \mapsto W$ be a homomorphism of representations on a group G. Then $\ker(T)$ is a G-invariant subspace of V, while $\mathrm{im}(T)$ is a G-invariant subspace of W.

Proof. Let $\psi^{(1)} : G \mapsto \mathrm{GL}(V)$, and $\psi^{(2)} : G \mapsto \mathrm{GL}(W)$ be the aforementioned representations. Let $v \in \ker(T) \subseteq V$. Then $T(v) = 0$, and thus $\psi_g^{(2)}(T(v)) = 0$. But $\psi_g^{(2)}(T(v)) = T(\psi_g^{(1)}(v))$, implying that $\psi_g^{(1)}(v) \in \ker(T)$, thus showing that $\ker(T)$ is a G-invariant subspace.
Similarly, let $w \in \mathrm{im}(T)$, and let $v \in V$ be such that $Tv = w$. Then:

$$\psi_g^{(2)}(w) = \psi_g^{(2)}(T(v)) = T(\psi_g^{(1)}(v)) \in \mathrm{im}(T)$$

Thus $\mathrm{im}(T)$ is a G-invariant subspace of W. ∎

Toward our goal of characterizing all representations, we equip $\mathrm{Hom}_G(\varphi, \rho)$ with some additional structure, namely, that of a vector space.

Proposition 6. Let $\varphi : G \mapsto \mathrm{GL}(V), \rho : G \mapsto \mathrm{GL}(W)$ be representations.
Then $\mathrm{Hom}_G(\varphi, \rho)$ is a subspace of $\mathrm{Hom}_G(V, W)$.

Proof. Let $T_1, T_2 \in \mathrm{Hom}_G(\varphi, \rho), c_1, c_2 \in \mathbb{C}, v \in V$. Then

$$(c_1T_1 + c_2T_2) \circ \varphi_g(v) = c_1T_1\varphi_g(v) + c_2T_2\varphi_g(v) = \rho_g(c_1T_1v) + \rho_g(c_2T_2v) = \rho_g((c_1T_1 + c_2T_2)v)$$

∎

We are now in a position to state a fundamental observation due to Schur, which severely restricts homomorphisms between irreducible representations.

Lemma 2.1 (Schur's Lemma)**.** Let φ, ρ be irreducible representations of G. Let $T \in \mathrm{Hom}_G(\varphi, \rho)$. Then either T is invertible, or $T = 0$. Consequently,

1. If $\varphi \not\sim \rho$, then $\mathrm{Hom}_G(\varphi, \rho) = 0$.
2. $\mathrm{Hom}_G(\varphi, \varphi) = \{\lambda I : \lambda \in \mathbb{C}\}$.
3. If $\varphi \sim \rho$, then $\dim \mathrm{Hom}_G(\varphi, \rho) = 1$.

Proof. Since $\ker(T)$ is an G-invariant subspace of the irreducible representation φ, $\ker(T) = 0$ or V. If $\ker(T) = V$, then $T = 0$. If $\ker(T) = 0$, then T is injective. Now, we also have that $\mathrm{im}(T) = 0, W$. However, since V is not singleton, $\mathrm{im}(T) \neq 0$. Thus $\mathrm{im}(T) = W$, i.e. T is bijective, i.e. T is invertible.
Clearly, if $\mathrm{Hom}_G(\varphi, \rho)$ contains any invertible element, then φ and ρ are equivalent. Consequently, if $\varphi \not\sim \rho$, then $\mathrm{Hom}_G(\varphi, \rho) = 0$, since any non-zero element of $\mathrm{Hom}_G(\varphi, \rho)$ must be invertible.
Suppose $T \in \mathrm{Hom}_G(\varphi, \varphi)$, and let $T \neq 0$. Since T is a complex matrix, it must have an eigenvalue, say $\lambda \in \mathbb{C}$. Then $\lambda I - T \in \mathrm{Hom}_G(\varphi, \varphi)$ (since $\mathrm{Hom}_G(\varphi, \varphi)$ is a vector space). But since $\lambda I - T$ is not invertible, it must be 0.
Similarly, $\mathrm{Hom}_G(\varphi, \rho) = \{\lambda T : \lambda \in \mathbb{C}\}$ where T is an isomorphism between φ and ρ, which is clearly one-dimensional. ■

We can finally describe the irreducible representations of an abelian group!

Theorem 2.2 (Irreducible Representations of Abelian Groups)**.** Let G be an abelian group. Then any irreducible representation has degree 1, i.e. if $\varphi : G \mapsto \mathrm{GL}(V)$ is irreducible, then $\dim(V) = 1$.

Proof. Fix some $h \in G$, and set $T = \varphi_h$. Then for any $g \in G$,

$$T\varphi_g = \varphi_h\varphi_g = \varphi_{hg} = \varphi_{gh} = \varphi_g\varphi_h = \varphi_g T$$

Thus $T \in \mathrm{Hom}_G(\varphi, \varphi)$, and consequently, $T = \lambda_h I$ for some $\lambda_h \in \mathbb{C}$. Then for any non-zero vector v,

$$T(\mu v) = \varphi_h \mu v = \lambda_h \mu v \in \langle v \rangle$$

Consequently, $\langle v \rangle$ is a G-invariant subspace for φ_h. Since h was arbitrary, $\langle v \rangle$ is a G-invariant subspace for φ. Since φ is irreducible, we must have $\langle v \rangle = V$, implying that $\dim(V) = 1$, as desired. ■

We now start moving towards irreducible representations of non-abelian groups. All groups henceforth will be assumed to be finite.

2.1. Orthogonality Relations

Let G be a finite group, and let $\mathbb{C}^G := \{f \mid f : G \mapsto \mathbb{C}\}$ be the set of *all* functions (not necessarily homomorphisms) from G to $\mathbb{C}$. $\mathbb{C}^G$ is also known as the *group algebra* of the group G. We also denote $\mathbb{C}^G$ as $L(G)$.
Clearly, $\mathbb{C}^G$ is a $\mathbb{C}$-vector space, and given $f_1, f_2 \in \mathbb{C}^G$, we define their inner product to be:

$$\langle f_1, f_2 \rangle := \frac{1}{|G|} \sum_{g \in G} \overline{f_1(g)} f_2(g)$$

Having had success with looking at unitary representations earlier, we try to replicate similar methods here. In particular, we shall now have the occasion to use the averaging trick again to describe a projection from $\mathrm{Hom}(V, W)$ to $\mathrm{Hom}_G(\varphi, \rho)$.

Lemma 2.3. Let $\varphi : G \mapsto \mathrm{GL}(V)$, $\rho : G \mapsto \mathrm{GL}(W)$ be representations, and let $T : V \mapsto W$ be an arbitrary linear map. Define:

$$T^{\#} := \frac{1}{|G|} \sum_{g \in G} \rho_{g^{-1}} T \varphi_g$$

Then the map $P : \mathrm{Hom}(V, W) \mapsto \mathrm{Hom}_G(\varphi, \rho)$ given by $P(T) := T^{\#}$ is an idempotent surjective linear map. In particular, if $T \in \mathrm{Hom}_G(\varphi, \rho)$, then $T^{\#} = T$. In other words, P is a projection map from $\mathrm{Hom}(V, W)$ to $\mathrm{Hom}_G(\varphi, \rho)$.

Proof. Note that we first have to verify that $T^{\#} \in \mathrm{Hom}_G(\varphi, \rho)$ for any $T \in \mathrm{Hom}(V, W)$. We do that by direct computation, by noting that:

$$T^{\#} \varphi_g = \frac{1}{|G|} \sum_{h \in G} \rho_{h^{-1}} T \varphi_h \varphi_g = \rho_g \cdot \frac{1}{|G|} \sum_{h \in G} \rho_{g^{-1}} \rho_{h^{-1}} T \varphi_{hg} = \rho_g \cdot \frac{1}{|G|} \sum_{h \in G} \rho_{(hg)^{-1}} T \varphi_{hg} = \rho_g T^{\#}$$

Furthermore, if $T \in \mathrm{Hom}_G(\varphi, \rho)$, then

$$T^{\#} = \frac{1}{|G|} \sum_{g \in G} \rho_{g^{-1}} T \varphi_g = \frac{1}{|G|} \sum_{g \in G} \rho_{g^{-1}} \rho_g T = T$$

Thus the map P is idempotent. Furthermore, since for any $T \in \mathrm{Hom}_G(\varphi, \rho)$, we have $P(T) = T$, P is surjective too. The linearity of P is also easy to see. ■

In the case φ, ρ are unitary representations, we can explicitly calculate the map P. Indeed, if $V = \mathbb{C}^n, W = \mathbb{C}^m$, $\mathrm{Hom}(V, W)$ can be identified with $\mathbb{C}^{m \times n}$. Also, let E^{rs} denote the $m \times n$ matrix whose $(r, s)^{\text{th}}$ entry is 1, and all other entries are 0. Then the matrices $\{E^{rs}\}_{r \in [m], s \in [n]}$ form a basis of $\mathbb{C}^{m \times n}$ as a $\mathbb{C}$-vector space.
Thus, for the following lemma, we shall treat $\mathrm{Hom}_G(\varphi, \rho)$ as a subspace of $\mathbb{C}^{m \times n}$.

Lemma 2.4. Let $\varphi : G \mapsto \mathrm{U}_n(\mathbb{C})$, $\rho : G \mapsto \mathrm{U}_m(\mathbb{C})$ be unitary representations. Let $A = E^{ki} \in \mathbb{C}^{m \times n}$. Then $A^{\#}_{\ell j} = \langle \rho_{k\ell}, \varphi_{ij} \rangle$, where $\rho_{k\ell}$ refers to the function $\rho_{k\ell} : G \mapsto \mathbb{C}$, $\rho_{k\ell}(g) := (\rho_g)_{k\ell}$.

Proof. The proof is by direct computation. Firstly, note that since ρ is a unitary representation, $\rho_{g^{-1}} = \rho_g^{-1} = \rho_g^*$. Then

$$A^{\#}_{\ell j} = \frac{1}{|G|} \sum_{g \in G} (\rho_g^* E^{ki} \varphi_g)_{\ell j}$$

Now,

$$(E^{ki} \varphi_g)_{rs} = \sum_t E^{ki}_{rt} (\varphi_g)_{ts} = \sum_t \delta_{kr} \delta_{it} (\varphi_g)_{ts} = \delta_{kr} (\varphi_g)_{is}$$

Then

$$(\rho_g^* E^{ki} \varphi_g)_{\ell j} = \sum_t (\rho_g^*)_{\ell t} \delta_{kt} (\varphi_g)_{ij} = (\rho_g^*)_{\ell k} (\varphi_g)_{ij} = \overline{(\rho_g)_{k\ell}} (\varphi_g)_{ij}$$

The result then follows from the definition of the inner product on $\mathbb{C}^G$. ■

We now restate Schur's lemma (Lemma 2.1) in terms of the $T^{\#}$ notation for further use later on.

Lemma 2.5. Let $\varphi : G \mapsto \mathrm{GL}(V)$, $\rho : G \mapsto \mathrm{GL}(W)$ be irreducible representations, and let $T : V \mapsto W$ be an arbitrary linear map. Then:

1. If $\varphi \not\sim \rho$, then $T^{\#} = 0$.
2. If $\varphi = \rho$, then $T^{\#} = (\mathrm{tr}(T)/\deg(\varphi))I$.

Proof. If $\varphi \not\sim \rho$, then $\mathrm{Hom}_G(\varphi, \rho) = 0$. Since $T^{\#} \in \mathrm{Hom}_G(\varphi, \rho)$, we get that $T^{\#} = 0$.
If $\varphi = \rho$, then $T^{\#} = \lambda I$ for some λ. To calculate λ, note that $\mathrm{tr}(T^{\#}) = n\lambda$, where $n = \dim(V) = \deg(\varphi)$. At the same time,

$$\mathrm{tr}(T^{\#}) = \frac{1}{|G|}\sum_{g\in G}\mathrm{tr}(\varphi_{g^{-1}}T\varphi_g) = \frac{1}{|G|}\sum_{g\in G}\mathrm{tr}(T\varphi_g\varphi_{g^{-1}}) = \mathrm{tr}(T)$$

Thus $T^{\#} = (\mathrm{tr}(T)/\deg(\varphi))I$, as desired. ∎

The results stated above are sufficient to prove the so-called Schur Orthogonality Relations, a very important result in representation theory.

Theorem 2.6 (Schur Orthogonality Relations)**.** Let $\varphi : G \mapsto \mathrm{U}(V)$, $\rho : G \mapsto \mathrm{U}(W)$ be inequivalent irreducible unitary representations. Then:

1. $\langle \rho_{k\ell}, \varphi_{ij}\rangle = 0$.
2. $\langle \varphi_{k\ell}, \varphi_{ij}\rangle = (1/\deg(\varphi))\delta_{ik}\delta_{j\ell}$.

Proof. Note that $\langle \rho_{k\ell}, \varphi_{ij}\rangle = A^{\#}_{\ell j}$ for some $A^{\#} \in \mathrm{Hom}_G(\varphi, \rho)$. But $\mathrm{Hom}_G(\varphi, \rho) = 0$. The other result also follows from Lemma 2.4 and the second part of Lemma 2.5. ∎

Corollary 2.7. If φ is an irreducible unitary representation of G of degree d, then $\{\sqrt{d}\varphi_{ij} : i, j \in [d]\}$ is an orthonormal set.

The above corollary immediately allows us to classify all equivalence classes of irreducible representations of G.

Theorem 2.8 (Equivalence Classes of Irreducible Representations)**.** Let G be a finite group. Then there are only finitely many equivalence classes of irreducible representations, say $\varphi^{(1)}, \ldots, \varphi^{(s)}$. Furthermore, if we write $d_i := \deg(\varphi^{(i)})$, then the set

$$\{\sqrt{d_k}\varphi^{(k)}_{ij} : k \in [s], i, j \in [d_k]\}$$

is an orthonormal subset of $\mathbb{C}^G$, and consequently, $s \leq d_1^2 + \cdots + d_s^2 \leq |G|$.

Proof. By Theorem 1.1, WLOG we can assume that all the equivalence classes of representations are being represented by unitary representations. If $\varphi^{(1)}, \varphi^{(2)}, \ldots$ are inequivalent unitary representations, then $\varphi^{(1)}_{11}, \varphi^{(2)}_{11}$ form an orthogonal system by Theorem 2.6. Since $\mathbb{C}^G$ is finite-dimensional, we get that the number of inequivalent representations is finite and thus denote them as $\varphi^{(1)}, \ldots, \varphi^{(s)}$. Finally, since the dimension of $\mathbb{C}^G$ is $|G|$, and since $\{\sqrt{d_k}\varphi^{(k)}_{ij} : k \in [s], i, j \in [d_k]\}$ is an orthonormal system (and hence linearly independent), we get that $d_1^2 + \cdots + d_s^2 \leq |G|$, as desired. ∎

We now introduce characters to prove the uniqueness of the decomposition obtained in Maschke's theorem.

2.2. Characters

Characters are a remarkably economical way of encapsulating a lot of information about a representation.

Definition 2.2. Let $\varphi : G \mapsto \mathrm{GL}(V)$ be a representation. The character of φ, denoted χ_φ, is a function $\chi_\varphi : G \mapsto \mathbb{C}$, where $\chi_\varphi(g) := \mathrm{tr}(\varphi_g)$.

The first thing that we need to verify is that the characters of isomorphic representations should be the same. Indeed,

Proposition 7. If $\varphi \sim \psi$, $\chi_\varphi = \chi_\psi$.

Proof. If $\varphi \sim \psi$, then there is an invertible linear transform T such that $\psi_g = T\varphi_g T^{-1}$ for all $g \in G$, and

$$\operatorname{tr}(\chi_g) = \operatorname{tr}(T\varphi_g T^{-1}) = \operatorname{tr}(\varphi_g T^{-1} \cdot T) = \operatorname{tr}(\varphi_g)$$

as desired. ■

Another useful fact is as follows:

Proposition 8. $\chi_\varphi(1) = \deg(\varphi)$.

Proof. Note that $\varphi_{1_G} = I$ since φ is a homomorphism. Consequently, $\chi_\varphi(1) = \deg(\varphi)$. ■

Also note that if φ is a degree 1 representation, then $\varphi_g \in \mathbb{C}$, and thus $\chi_\varphi(g) = \varphi_g$. Thus, henceforth, we shall not distinguish between a degree 1 representation and its character. In particular, that implies the following proposition.

Proposition 9. Let φ be a degree 1 representation, and let χ be its character. Then $\chi : G \mapsto \mathbb{C}^\times$ is a group homomorphism.

Remark. Note that characters are not multiplicative *in general*: Indeed,

$$\chi_\varphi(g_1 g_2) = \operatorname{tr}(\varphi_{g_1 g_2}) = \operatorname{tr}(\varphi_{g_1}\varphi_{g_2}) \neq \operatorname{tr}(\varphi_{g_1})\operatorname{tr}(\varphi_{g_2}) = \chi_\varphi(g_1)\chi_\varphi(g_2)$$

We also note the following fact:

Proposition 10. Let $\varphi = \rho \oplus \psi$. Then $\chi_\varphi = \chi_\rho + \chi_\psi$.

Proof. Note that

$$\varphi_g = \begin{bmatrix} \rho_g & 0 \\ 0 & \psi_g \end{bmatrix}$$

Thus, $\chi_\varphi(g) = \operatorname{tr}(\varphi_g) = \operatorname{tr}(\rho_g) + \operatorname{tr}(\psi_g) = \chi_\rho(g) + \chi_\psi(g)$, as desired. ■

Now, the fact that $\operatorname{tr}(A) = \operatorname{tr}(PAP^{-1})$, which we used to show that characters of isomorphic representations are the same, can also be used to give a decomposition of the group in terms of the character. On the surface of it, it seems like the character, associating just one number to a whole matrix, loses a lot of information. However, as we shall see now, the character manages to 'retain' a significant bit of information.

Proposition 11. Let $\varphi : G \mapsto \mathrm{GL}(V)$ be a representation. Then for any $g, h \in G$,

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

Proof. Note that

$$\chi_\varphi(hgh^{-1}) = \operatorname{tr}(\varphi_{hgh^{-1}}) = \operatorname{tr}(\varphi_h\varphi_g\varphi_{h^{-1}}) = \operatorname{tr}(\varphi_h\varphi_g\varphi_h^{-1}) = \operatorname{tr}(\varphi_g\varphi_h^{-1}\varphi_h) = \chi_\varphi(g)$$

■

Motivated by this proposition, we make the following definition:

Definition 2.3 (Class Function)**.** A function $f : G \mapsto \mathbb{C}$ is called a class function if $f(g) = f(hgh^{-1})$ for any $g, h \in G$.

Recall that for any group, we say that g_1, g_2 are conjugate if there exists some $h \in G$ such that $g_1 = hg_2h^{-1}$. Conjugacy is an equivalence relation, and the equivalence classes of a group under conjugacy are called conjugacy classes.
To quickly refresh our memory of conjugacy classes from group theory, let's look at the following examples:

1. Consider the group $\mathfrak{S}_3$: Firstly, note that for any group G, the identity element 1_G forms a singleton conjugacy class, since $g^{-1}1_Gg = 1_G$ [2]. Next, note that all order 2 elements of $\mathfrak{S}_3$ are conjugate to each other: Indeed, $(ac) = \sigma^{-1}(bc)\sigma$, where $\sigma = abc \mapsto cab$, and similar conjugacy relations can be obtained between (bc) and (ab) too. Finally, the two remaining elements of $\mathfrak{S}_3$, both of which are order 3, are conjugate to each other: Indeed, $(bca) = (bc)^{-1}(cab)(bc)$. Thus, the conjugacy classes of $\mathfrak{S}_3$ are $\big\{\{1\}, \{(ab), (bc), (ca)\}, \{(bca), (cab)\}\big\}$.

2. Let Q_8 be the group of quaternions, i.e. Q_8 is generated by $\widehat{i}, \widehat{j}, \widehat{k}$, where $\widehat{i}^2 = \widehat{j}^2 = \widehat{k}^2 = \widehat{i}\widehat{j}\widehat{k} = -1$. Note that $Q_8 = \{\pm 1, \pm\widehat{i}, \pm\widehat{j}, \pm\widehat{k}\}$, and $Z(Q_8) = \{\pm 1\}$. Thus, $\{1\}, \{-1\}$ are two conjugacy classes. Furthermore, $t, -t$ are conjugate for $t \in \{\widehat{i}, \widehat{j}, \widehat{k}\}$: For example, note that $-\widehat{i} = \widehat{k}^{-1}\widehat{i}\widehat{k} = -\widehat{k}\widehat{i}\widehat{k} = -\widehat{k} \cdot (-\widehat{k}\widehat{i}) = \widehat{k}^2\widehat{i} = -\widehat{i}$. Thus the conjugacy classes of Q_8 are $\Big\{\{1\}, \{-1\}, \{\pm\widehat{i}\}, \{\pm\widehat{j}\}, \{\pm\widehat{k}\}\Big\}$.

3. Recall the dihedral groups from Item 2, i.e. $D_n := \langle r, s | r^n = s^2 = (rs)^2 = 1\rangle$. To calculate the conjugacy classes of D_n, we make cases:

   (a) Suppose n is odd: Note that s is conjugate to sr^2: Indeed, $r \cdot sr^2 \cdot r^{-1} = rsr = s$. Similarly, $sr^2 \sim sr^4$ (we use $\sim$ to denote conjugacy), and so on, until $sr^{n-1} \sim sr \sim sr^3 \sim sr^5 \sim \cdots$, i.e. $\{s, sr, \ldots, sr^{n-1}\}$ all belong to the same conjugacy class. At the same time, note that $r \sim r{-}1$: Indeed, $srs^{-1} = srs = ssr^{-1} = r^{-1}$. Similarly, $r^k \sim r^{-k}$ for all k. Moreover, for any k, we have $r^j \cdot r^k \cdot r^{-j} = r^k, sr^j \cdot r^k r^{-j} s^{-1} = sr^k s = r^{-k}$. Thus, $\{r^k, r^{-k}\}$ form a conjugacy class. Consequently, the conjugacy classes of D_n, for odd n are $\Big\{\{1\}, \{r, r^{-1}\}, \ldots, \{r^{(n-1)/2}, r^{-(n-1)/2}\}, \{s, sr, \ldots, sr^{n-1}\}\Big\}$.

   (b) Suppose n is even: Note that $\{1\}, \{r, r^{-1}\}, \ldots, \{r^{n/2}, r^{-n/2}\}$ [3] continue to remain conjugacy classes for the same reasons as above. However, the conjugacy class $\{s, sr, \ldots, sr^{n-1}\}$ now splits into two parts, namely $\{s, sr^2, \ldots, sr^{n-2}\}, \{sr, sr^3, \ldots, sr^{n-1}\}$. Consequently, the conjugacy classes of D_n, for even n are $\Big\{\{1\}, \{r, r^{-1}\}, \ldots, \{r^{n/2}, r^{-n/2}\}, \{s, sr^2, \ldots, sr^{n-2}\}, \{sr, sr^3, \ldots, sr^{n-1}\}\Big\}$.

Consequently, *class functions are constant on conjugacy classes*.
We denote the set of all class functions in $L(G) = \mathbb{C}^G$ as $Z(L(G))$ [4].

Proposition 12. $Z(L(G))$ is a subspace of $\mathbb{C}^G$.

[2] In general, all elements of $Z(G)$ form singleton conjugacy classes, because they commute with everything else
[3] note that $r^{n/2} = r^{-n/2}$
[4] the notation $Z(\cdot)$ is indicative of it being the 'center' of something: A priori, that is a bit confusing since $L(G)$ is an abelian group (and thus the center of $L(G)$ as a group is $L(G)$ itself). However, we shall later equip $L(G)$ with a non-commutative multiplication operator, and $Z(L(G))$ will turn out to be the center of that (non-commutative) ring

Proof. Let $f_1, f_2 \in Z(L(G))$. Then

$$(c_1f_1 + c_2f_2)(hgh^{-1}) = c_1f_1(hgh^{-1}) + c_2f_2(hgh^{-1}) = c_1f_1(g) + c_2f_2(g) = (c_1f_1 + c_2f_2)(g)$$

■

We shall now describe a basis for $Z(L(G))$ and hence compute its dimension.
Let $\mathrm{Cl}(G)$ be the set of conjugacy classes of G. For every $C \in \mathrm{Cl}(G)$, define $\delta_C : G \mapsto \mathbb{C}$, where $\delta_C := \mathbb{1}_C$, i.e.

$$\delta_C(x) := \begin{cases} 1, & x \in C \\ 0, & \text{otherwise} \end{cases}$$

Lemma 2.9. $\{\delta_C : C \in \mathrm{Cl}(G)\}$ is a basis for $Z(L(G))$. Thus $\dim Z(L(G)) = |\mathrm{Cl}(G)|$.

Proof. Let $f \in Z(L(G))$. Choose $c \in C$ for every $C \in \mathrm{Cl}(G)$. Then note that

$$f = \sum_{C \in \mathrm{Cl}(G)} f(c)\delta_C$$

Note that the above definition is consistent, since $f(c) = f(c')$ for any $c, c' \in C$, since $f \in Z(L(G))$ is a class function. Thus $\{\delta_C : C \in \mathrm{Cl}(G)\}$ span $Z(L(G))$. Furthermore, if

$$\sum_{C \in \mathrm{Cl}(G)} \alpha_C \cdot \delta_C = 0$$

then $\alpha_C = 0$ for all $C \in \mathrm{Cl}(G)$: Indeed, for any $x \in G$, inputting x in the above expression yields $\alpha_{C_x} = 0$, where $x \in C_x \in \mathrm{Cl}(G)$. Thus, varying x over G yields the desired result. ■

We now describe another spanning set for $Z(L(G))$, which will finally connect representations to class functions.

Theorem 2.10 (First Orthogonality Relation)**.** Let φ, ρ be irreducible representations of G. Then:

$$\langle \chi_\varphi, \chi_\rho \rangle = \begin{cases} 1, & \text{if } \varphi \sim \rho \\ 0, & \text{if } \varphi \not\sim \rho \end{cases}$$

Consequently, *any* group G has at most $|\mathrm{Cl}(G)|$ inequivalent irreducible representations.

Proof. By Theorem 1.1, φ, ρ are equivalent to some unitary representation(s). Since characters of equivalent representations are the same, WLOG we may assume φ, ρ are unitary. Let $\deg(\varphi) = n, \deg(\rho) = m$. Then

$$\langle \chi_\rho, \chi_\varphi \rangle = \sum_{g \in G} \chi_\varphi(g) \cdot \overline{\chi_\rho(g)} = \sum_{g \in G} \mathrm{tr}(\varphi_g) \cdot \overline{\mathrm{tr}(\rho_g)} = \sum_{g \in G} \sum_{i=1}^{n} \sum_{j=1}^{m} (\varphi_g)_{ii} \cdot \overline{(\rho_g)_{jj}}$$

$$= \sum_{i=1}^{n} \sum_{j=1}^{m} \sum_{g \in G} (\varphi_g)_{ii} \cdot \overline{(\rho_g)_{jj}} = \sum_{i=1}^{n} \sum_{j=1}^{m} \langle \varphi_{ii}, \rho_{jj} \rangle$$

By Theorem 2.6, if $\varphi \not\sim \rho$, the above expression is 0. On the other hand, if $\varphi \sim \rho$, then $\langle \varphi_{ii}, \rho_{jj} \rangle = (1/\deg(\varphi)) \cdot \delta_{ij}^2 = (1/\deg(\varphi)) \cdot \delta_{ij}$. Thus

$$\sum_{i=1}^{n} \sum_{j=1}^{m} \langle \varphi_{ii}, \rho_{jj} \rangle = \sum_{i=1}^{n} \sum_{j=1}^{n} \frac{\delta_{ij}}{n} = 1$$

as desired. ■

We can finally prove the uniqueness of Maschke's decomposition:

Theorem 2.11 (Uniqueness of Maschke's decomposition)**.** Let $\varphi^{(1)}, \dots, \varphi^{(s)}$ be a complete set of representatives of the equivalence classes of irreducible representations of G. Let ρ be any representation of G. Then by Theorem 1.3, we have

$$\rho \sim m_1\varphi^{(1)} \oplus \cdots \oplus m_s\varphi^{(s)}$$

Then $m_i = \langle \chi_{\varphi^{(i)}}, \chi_\rho \rangle$. Consequently, the decomposition of ρ into irreducible constituents is unique.

Proof. By Proposition 10,

$$\chi_\rho = m_1\chi_{\varphi^{(1)}} + \cdots + m_s\chi_{\varphi^{(s)}}$$

Thus,

$$\langle \chi_\rho, \chi_{\varphi^{(s)}} \rangle = \sum_{i=1}^{s} m_i \langle \chi_{\varphi^{(i)}}, \chi_{\varphi^{(s)}} \rangle \overset{\text{Theorem 2.10}}{=} m_s$$

■

Corollary 2.12. A representation ρ is irreducible iff $\langle \chi_\rho, \chi_\rho \rangle = 1$.

Proof. Let

$$\rho \sim m_1\varphi^{(1)} \oplus \cdots \oplus m_s\varphi^{(s)}$$

be the Maschke decomposition of ρ. Then by Theorem 2.10, we have $\langle \chi_\rho, \chi_\rho \rangle = \sum_{i=1}^{s} m_i^2$. Consequently, if ρ is not irreducible, $\langle \chi_\rho, \chi_\rho \rangle > 1$. Conversely, if ρ is irreducible, then $\rho \sim \varphi^{(s)}$ for some s, and $\langle \chi_\rho, \chi_\rho \rangle = 1$. ■

2.3. Regular Representations

Recall regular representations (Proposition 2); we shall now develop regular representations from another viewpoint.
Given any finite set X, we can synthetically 'build' a $\mathbb{C}$-vector space which has X as its basis: Indeed, define:

$$\mathbb{C}X := \left\{ \sum_{x \in X} c_x x : c_x \in \mathbb{C} \right\}$$

Addition and scalar multiplication are obvious: Indeed,

$$\sum_{x \in X} a_x x + \sum_{x \in X} b_x x := \sum_{x \in X} (a_x + b_x) x$$

$$\lambda \cdot \sum_{x \in X} a_x x := \sum_{x \in X} (\lambda a_x) x$$

Finally,

$$\left\langle \sum_{x \in X} a_x x, \sum_{x \in X} b_x x \right\rangle := \sum_{x \in X} \overline{a}_x b_x$$

Remark. Note that unlike in the case of $\mathbb{C}^G$, the dot product for $\mathbb{C}X$ (or $\mathbb{C}G$) does not involve scaling by $1/|G|$.

Definition 2.4 (Regular Representations)**.** Let G be a finite group. The regular representation of G is defined to be the homomorphism $L : G \mapsto \mathrm{GL}(\mathbb{C}G)$, where

$$L_g \sum_{h\in G} c_h h := \sum_{h\in G} c_h gh = \sum_{x\in G} c_{g^{-1}x} x$$

Remark. The 'L' stands for 'Left', since g gets *left* multiplied with h.
We remark that L is not only a representation but a unitary representation.

Proposition 13. L is a unitary representation.

Proof. We must first prove that L is a representation, i.e. L is a group homomorphism. To that extent,

$$L_{g_1} L_{g_2} h = g_1(g_2 h) = (g_1 g_2)h = L_{g_1 g_2} h$$

Thus, L is a representation. To show that L is unitary, we have to show that $\langle L_g v, L_g w\rangle = \langle v, w\rangle$ for all $v, w \in \mathbb{C}G, g \in G$. Indeed,

$$\left\langle L_g \sum_{h\in G} c_h h, L_g \sum_{h\in G} k_h h \right\rangle = \left\langle \sum_{h\in G} c_h gh, \sum_{h\in G} k_h gh \right\rangle = \left\langle \sum_{x\in G} c_{g^{-1}x} x, \sum_{x\in G} k_{g^{-1}x} x \right\rangle = \sum_{x\in G} \overline{c}_{g^{-1}x} \cdot k_{g^{-1}x}$$

Since $x \mapsto g^{-1}x$ is an automorphism of G,

$$\sum_{x\in G} \overline{c}_{g^{-1}x} \cdot k_{g^{-1}x} = \sum_{x\in G} \overline{c}_x \cdot k_x = \left\langle \sum_{h\in G} c_h h, \sum_{h\in G} k_h h \right\rangle$$

as desired. Since L_g is unitary, it is also invertible, and thus $L : G \mapsto \mathrm{GL}(\mathbb{C}G)$ is a unitary representation. ■

It turns out that L has a particularly simple character.

Proposition 14. The character of L is given by:

$$\chi_L(g) = \begin{cases} |G|, & \text{if } g = 1 \\ 0, & \text{otherwise} \end{cases}$$

Proof. Fix any g, and consider L_g as a matrix, whose rows and columns are indexed by elements of G. Note that $(L_g)_{h_1 h_2} = 1$ if and only if $L_g(h_1) = h_2$, i.e. $gh_1 = h_2$. Thus, note that $(L_g)_{hh} = 1$ if and only if $g = 1$.
Thus, if $g = 1$, then L_g is the identity matrix, with trace $|G|$. If $g \neq 1$, then no diagonal entry is 1, and the trace is 0. ■

Now that we have calculated the character of G, we can calculate the Maschke decomposition of L. It has a particularly nice form.

Theorem 2.13. Let $\varphi^{(1)}, \ldots, \varphi^{(s)}$ be the (representatives of) the inequivalent irreducible representations of G. Let $d_i := \deg(\varphi^{(i)})$. Then

$$L \sim d_1 \varphi^{(1)} \oplus \cdots \oplus d_s \varphi^{(s)}$$

Proof. Note that

$$\langle \chi_L, \chi_{\varphi^{(i)}} \rangle = \chi_{\varphi^{(i)}}(1) = \deg(\varphi^{(i)}) = d_i$$

Thus, by Theorem 2.11,

$$L \sim d_1\varphi^{(1)} \oplus \cdots \oplus d_s\varphi^{(s)}$$

■

Corollary 2.14. We have $|G| = d_1^2 + \cdots + d_s^2$.

Proof. We have

$$\chi_L = \sum_{i=1}^{s} d_i \chi_{\varphi^{(i)}} \implies |G| = \chi_L(1) = \sum_{i=1}^{s} d_i \chi_{\varphi^{(i)}}(1) = \sum_{i=1}^{s} d_i^2$$

■

Corollary 2.15. Write

$$\mathcal{B} := \left\{ \sqrt{d_k}\varphi_{ij}^{(k)} : k \in [s], i, j \in [d_k] \right\}$$

From Theorem 2.8, we know that $\mathcal{B}$ is an orthonormal spanning set of $\mathbb{C}^G$. It is in fact an orthonormal *basis* of $\mathbb{C}^G$.

Proof. This follows from the fact that

$$d_1^2 + \cdots + d_s^2 = |G|$$

■

For convenience, we shall henceforth refer to $\chi_{\varphi^{(i)}}$ as χ_i.

Theorem 2.16. The set $\chi_1, \ldots, \chi_s$ is an orthonormal basis for $Z(L(G))$.

Proof. By Theorem 2.10, we know that $\chi_1, \ldots, \chi_s$ are an orthonormal, and hence linearly independent, set. We must now show that they span $Z(L(G))$. Now, by Corollary 2.15, $\left\{ \sqrt{d_k}\varphi_{ij}^{(k)} : k \in [s], i, j \in [d_k] \right\}$ spans $\mathbb{C}^G \supset Z(L(G))$, and thus, for any $f \in Z(L(G))$, we have:

$$f = \sum_{i,j,k} c_{ij}^{(k)} \varphi_{ij}^{(k)}$$

for some constants $c_{ij}^{(k)}$. Now, since f is a class function,

$$f(x) = \frac{1}{|G|} \cdot \sum_{g \in G} f(g^{-1}xg) = \frac{1}{|G|} \sum_{g \in G} \sum_{i,j,k} c_{ij}^{(k)} \varphi_{ij}^{(k)}(g^{-1}xg) = \sum_{i,j,k} c_{ij}^{(k)} \cdot \left(\frac{1}{|G|} \cdot \sum_{g \in G} \varphi_{ij}^{(k)}(g^{-1}xg) \right)$$

$$= \sum_{i,j,k} c_{ij}^{(k)} \cdot \left(\frac{1}{|G|} \cdot \sum_{g \in G} \varphi_{g^{-1}}^{(k)} \varphi_x^{(k)} \varphi_g^{(k)} \right)_{ij} = \sum_{i,j,k} c_{ij}^{(k)} \cdot \left((\varphi_x^{(k)})^{\#} \right)_{ij} \overset{\text{Lemma 2.5}}{=} \sum_{i,j,k} c_{ij}^{(k)} \cdot \left(\frac{\operatorname{tr}(\varphi_x^{(k)})}{d_k} I \right)_{ij}$$

$$= \sum_{i,j,k} c_{ij}^{(k)} \cdot \frac{\chi_k(x)}{d_k} \delta_{ij} = \sum_{i,k} c_{ii}^{(k)} \cdot \frac{\chi_k(x)}{d_k}$$

Thus,

$$f = \sum_k \frac{1}{d_k} \left(\sum_i c_{ii}^{(k)} \right) \cdot \chi_k$$

Thus, f actually lies in the span of $\chi_1, \ldots, \chi_s$. Consequently, $\chi_1, \ldots, \chi_s$ form an orthonormal *basis* for $Z(L(G))$. ■

Corollary 2.17. $s = \dim(Z(L(G))) = |\operatorname{Cl}(G)|$, i.e., the number of inequivalent irreducible representations of a group G is equal to the number of conjugacy classes.

Corollary 2.18. A finite abelian group G has $|G|$ inequivalent irreducible representations.

Proof. Note that every element of an abelian group forms a singleton conjugacy class. ■

Lemma 2.19 (Irreducible Representations of $\mathbb{Z}/n\mathbb{Z}$)**.** Let $\omega = e^{2i\pi/n}$. Define $\chi_k : \mathbb{Z}/n\mathbb{Z} \mapsto \mathbb{C}^*$ as:

$$\chi_k(\overline{m}) := \omega^{km}$$

Then $\chi_0, \ldots, \chi_{n-1}$ are representatives of all the inequivalent irreducible representations of $\mathbb{Z}/n\mathbb{Z}$.

Proof. Recall that the irreducible representations of a finite abelian group are degree 1, and thus WLOG we identify them with their characters. Also, note that

$$\langle \chi_k, \chi_k \rangle = \frac{1}{n} \sum_{m=0}^{n-1} \omega^{2km} = 1$$

and thus all the χ_*'s are irreducible. Finally, it is clear that χ_*'s are different as functions, and hence correspond to inequivalent representations. Since an abelian group has exactly n inequivalent irreducible representations, it follows that $\chi_0, \ldots, \chi_{n-1}$ are representatives of all the inequivalent irreducible representations of $\mathbb{Z}/n\mathbb{Z}$. ■

2.3.1. Irreducible Representations of finite abelian groups

Let G be a finite abelian group. Then by the structure theorem for finite abelian groups,

$$G = \bigoplus_{j=1}^{u} \mathbb{Z}/n_j\mathbb{Z}$$

where $n_1, \ldots, n_u$ are prime powers (not necessarily distinct). Recall that to specify any representation of a group G, it suffices to specify the images of the generators of G. Now, G is generated by $e_j := (0, 0, \ldots, 1, \ldots, 0) \in \oplus_{j=1}^{u} \mathbb{Z}/n_j\mathbb{Z}$, where the '1' varies over all the u positions. Now, if ρ is an irreducible representation of G, it is easy to see that $\rho(e_j) = \exp(2i\pi k_j/n_j)$, where $0 \leq k_j < n_j$. Consequently, for any $(n_1, \ldots, n_u) \in G$, we have:

$$\rho((\overline{m_1}, \ldots, \overline{m_u})) = \exp\left(2i\pi \left(\frac{m_1 k_1}{n_1} + \cdots + \frac{m_u k_u}{n_u} \right) \right)$$

Thus, for every $(k_1, \ldots, k_u) \in \{0, \ldots, n_1 - 1\} \times \cdots \times \{0, \ldots, n_u - 1\}$, we obtain a representation of G. By Corollary 2.12, it is easy to verify that they are irreducible. It is also easy to see that they are distinct (i.e. inequivalent). Since

$$\left| \{0, \ldots, n_1 - 1\} \times \cdots \times \{0, \ldots, n_u - 1\} \right| = n_1 \cdots n_u = n$$

, by Corollary 2.18, these are the representatives of all the inequivalent irreducible representations of G.

Theorem 2.20 (Irreducible Representations of finite abelian groups)**.** Let G be a finite abelian group, and let

$$G = \bigoplus_{j=1}^{u} \mathbb{Z}/n_j\mathbb{Z}$$

be the decomposition of G into cyclic groups, as given by the structure theorem. Write $\omega_j := \exp(2i\pi/n_j)$. Define $\chi_{k_1,\dots,k_u} : G \mapsto \mathbb{C}^*$ as:

$$\chi_{k_1,\dots,k_u}(\overline{m_1},\dots,\overline{m_u}) := \prod_{j=1}^{u} \omega_j^{k_j m_j} = \prod_{j=1}^{u} \chi_{k_j}(\overline{m_j})$$

Then $\left\{\chi_{k_1,\dots,k_u}\right\}_{(k_1,\dots,k_u)\in\{0,\dots,n_1-1\}\times\cdots\times\{0,\dots,n_u-1\}}$ are representatives of all the inequivalent irreducible representations of G.

The characters of the group $(\mathbb{Z}/2\mathbb{Z})^n \cong \mathbb{F}_2^n$ are very important in computer science. Indeed, for any $(k_1,\dots,k_n) \in \{0,1\}^n$, we have a character $\chi_{k_1,\dots,k_n} : \mathbb{F}_2^n \mapsto \mathbb{C}$ as:

$$\chi_{k_1,\dots,k_n}(m_1,\dots,m_n) = (-1)^{\sum_{j=1}^{n} k_j m_j}$$

We restate this slightly differently: Note that there is a correspondence between elements of $\{0,1\}^n$ and subsets of n, where $(k_1,\dots,k_n) \in \{0,1\}^n$ corresponds to $\left\{i \in [n] : k_i = 1\right\}$. Thus, let $S \subseteq [n]$. Also, rewrite the group $((\mathbb{Z}/2\mathbb{Z})^n, +, (0,\dots,0))$ in a multiplicative form, as $(\{-1,1\}^n, \cdot, (1,\dots,1))$. Then it is easy to see that the new character function becomes:

$$\chi_S(x_1,\dots,x_n) := \prod_{i\in S} x_i$$

where $(x_1,\dots,x_n) \in \{-1,1\}^n$.
Since $G = \{-1,1\}^n$ is abelian, $\{\chi_S\}_{S\subseteq[n]}$ form a basis for $\mathbb{C}^G$, i.e. any function $f : \{-1,1\}^n \mapsto \mathbb{C}$ can be uniquely written as $f = \sum_{S\subseteq[n]} \alpha_S \chi_S$. The coefficients α_S are known as the *Fourier coefficients* of f.
We shall deal with Fourier expansions in detail in the upcoming chapters.

2.4. Character Tables

Definition 2.5. Let G be any group, and write $|\operatorname{Cl}(G)| =: s$. Then the character table of G is a $s \times s$ matrix X, with $X_{ij} := \chi_i(C_j)$, where χ_i is the i^{th} irreducible representation, and C_j is the j^{th} conjugacy class.

One very surprising fact is that X^*X is a diagonal matrix:

Theorem 2.21 (Second Orthogonality Relation)**.** Let C, C' be conjugacy classes of a group G, and suppose $g \in C, h \in C'$. Then

$$\sum_{i=1}^{s} \overline{\chi_i(g)} \cdot \chi_i(h) = \frac{|G|}{|C|} \cdot \mathbb{1}_{C=C'}$$

Consequently, X^*X is a diagonal matrix.

Proof. Note that $\{\delta_C\}_{C\in \mathrm{Cl}(G)}$ and $\{\chi_i\}_{i\in[s]}$ are orthonormal bases for $Z(L(G))$. Expressing them in terms of each other gets what we want. Indeed,

$$\delta_C = \sum_{i=1}^{s} \langle \chi_i, \delta_C \rangle \chi_i$$

Thus,

$$\delta_C(h) = \sum_{i=1}^{s} \frac{1}{|G|} \sum_{x\in G} \overline{\chi_i(x)} \cdot \delta_C(x)\chi_i(h) = \sum_{i=1}^{s} \frac{1}{|G|} \sum_{x\in C} \overline{\chi_i(x)} \cdot \chi_i(h) = \sum_{i=1}^{s} \frac{1}{|G|} \sum_{x\in C} \overline{\chi_i(g)} \cdot \chi_i(h) = \frac{|C|}{|G|} \sum_{i=1}^{s} \overline{\chi_i(g)} \cdot \chi_i(h)$$

Thus,

$$\sum_{i=1}^{s} \overline{\chi_i(g)} \cdot \chi_i(h) = \frac{|G|}{|C|} \cdot \delta_C(h) = \frac{|G|}{|C|} \cdot \mathbb{1}_{C=C'}$$

■

Remark. Although the columns of X are orthogonal, the rows of X need not be orthogonal, as we shall see soon.

2.5. Computing Character Tables

We shall compute the character tables for some groups of interest.

2.5.1. The Quaternion Group

Recall the quaternion group Q_8 from Item 2. It has 5 conjugacy classes, namely $\{1\}, \{-1\}, \{\pm\widehat{i}\}, \{\pm\widehat{j}\}, \{\pm\widehat{k}\}$. Thus, $s = 5$, and we have $d_1^2 + \cdots + d_5^2 = 8$. The only way 5 positive integers' squares can sum to 8 is if $d_1, \ldots, d_5 = 1, 1, 1, 1, 2$. Thus Q_8 has 4 inequivalent irreducible degree 1 representations, and one irreducible degree 2 representation.
Thus, suppose $\rho : Q_8 \mapsto \mathbb{C}^*$ is a homomorphism. Let $\alpha = \rho(\widehat{i}), \beta = \rho(\widehat{j}), \gamma = \rho(\widehat{k}), \delta = \rho(-1)$. Since ρ is a homomorphism, we must have $\alpha^2 = \beta^2 = \gamma^2 = \alpha\beta\gamma = \delta$ (since $\widehat{i}, \widehat{j}, \widehat{k}$, who generate Q_8, satisfy these relations among themselves). Now, we must also have $\delta^2 = 1$, i.e. $\delta = \pm 1$. If $\delta = -1$, a little trial and error shows that no α, β, γ can satisfy the above relations. Thus, $\delta = 1$, which shows that $\alpha, \beta, \gamma = \pm 1$. A little fiddling then reveals the 4 irreducible representations to be:

$$\begin{array}{c} \\ \chi_1 \\ \chi_2 \\ \chi_3 \\ \chi_4 \\ \chi_5 \end{array} \begin{array}{c} \begin{array}{ccccc} \{1\} & \{-1\} & \{\pm\widehat{i}\} & \{\pm\widehat{j}\} & \{\pm\widehat{k}\} \end{array} \\ \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 \\ * & * & * & * & * \end{pmatrix} \end{array}$$

The irreducibility of the above representations may be checked by Corollary 2.12. We now have to find an irreducible degree 2 representation of Q_8. Consequently, we need matrices $A, B, C, D \in \mathrm{GL}_2(\mathbb{C})$ such that $A^2 = B^2 = C^2 = ABC = D, D^2 = I$. Also note that without loss of generality we can choose $A, B, C, D \in \mathrm{U}_2(\mathbb{C})$ since any representation is equivalent to a unitary one. As it turns out, the unitary representation(s) of Q_8 have a connection with the so-called *Pauli matrices*: Indeed,

$$\widehat{i} \mapsto \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix} = -i\sigma_x, \widehat{j} \mapsto \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = -i\sigma_y, \widehat{k} \mapsto \begin{bmatrix} -i & 0 \\ 0 & i \end{bmatrix} = -i\sigma_z$$

gives a group homomorphism $Q_8 \mapsto \mathrm{U}_2(\mathbb{C})$, where $\sigma_x, \sigma_y, \sigma_z$ are the Pauli matrices. The above matrices also yield that:

$$\rho(-1) = \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix}^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$$

Thus, we can finally complete the character table as:

$$\begin{array}{c} \\ \chi_1 \\ \chi_2 \\ \chi_3 \\ \chi_4 \\ \chi_5 \end{array} \begin{array}{c} \begin{array}{ccccc} \{1\} & \{-1\} & \{\pm\widehat{i}\} & \{\pm\widehat{j}\} & \{\pm\widehat{k}\} \end{array} \\ \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 \\ 2 & -2 & 0 & 0 & 0 \end{pmatrix} \end{array}$$

Note that we could have found the last row of the character table without calculating the degree 2 representation explicitly: Indeed, first note that if ρ is an irreducible degree 2 representation of Q_8, then $\rho(1) = I \in \mathrm{GL}_2(\mathbb{C})$, and thus $\chi_5(1) = \mathrm{tr}(I) = 2$. Thus, let the last row of the character table be $\begin{bmatrix} 2 & x_1 & x_2 & x_3 & x_4 \end{bmatrix}$. By the orthogonality relations, we have $2x_1 + 4 = 0, 2x_2 = 0, 2x_3 = 0, 2x_4 = 0$, which yields the desired result.

2.5.2. The Dihedral Group

Recall the dihedral groups from Item 2, Item 3. We shall now calculate the irreducible representations of D_n.
Firstly, note that the degree 1 representation $\rho : D_n \mapsto \mathbb{C}^*$, $\rho(g) := 1$ is always an irreducible representation. It is also easy to verify that $\rho(r) := 1, \rho(s) := -1$ is also an irreducible representation.
Also, recall from Item 2, the representation:

$$r \mapsto \begin{bmatrix} \cos(2\pi k/n) & -\sin(2\pi k/n) \\ \sin(2\pi k/n) & \cos(2\pi k/n) \end{bmatrix}, s \mapsto \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

is irreducible for $1 \leq k \leq \lfloor (n-1)/2 \rfloor$ [5].
Thus, we already have $2 + \lfloor (n-1)/2 \rfloor$ representations for D_n. Now, recall from Item 3 that if n is odd, then it has $2 + \lfloor (n-1)/2 \rfloor$ conjugacy classes, and thus for odd n we have described all irreducible representations.
For even n, we have $n/2 + 3$ conjugacy classes, which means that we're still missing 2 irreducible representations. From Corollary 2.14, we obtain that the remaining representations must be of degree 1 each. Indeed, if n is even, then note that $r \mapsto -1, s \mapsto 1; r \mapsto -1, s \mapsto -1$ are also inequivalent irreducible representations.
Thus, if $n = 2\ell + 1$, then the character table of D_n is:

$$\begin{array}{c} \\ \chi_1 \\ \chi_2 \\ \chi_3 \\ \vdots \\ \chi_{\ell+2} \end{array} \begin{array}{c} \begin{array}{ccccccc} \{1\} & \{r, r^{-1}\} & \{r^2, r^{-2}\} & \cdots & \{r^\ell, r^{-\ell}\} & \{s, sr, \ldots, sr^{2\ell}\} \end{array} \\ \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ 1 & 1 & 1 & \cdots & 1 & -1 \\ 2 & 2\cos(2\pi/n) & 2\cos(4\pi/n) & \cdots & 2\cos(2\ell\pi/n) & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 2 & 2\cos(2\ell\pi/n) & 2\cos(4\ell\pi/n) & \cdots & 2\cos(2\ell^2\pi/n) & 0 \end{pmatrix} \end{array}$$

And if $n = 2\ell$, then the character table of D_n is:

$$\begin{array}{c} \\ \chi_1 \\ \chi_2 \\ \chi_3 \\ \chi_4 \\ \chi_5 \\ \vdots \\ \chi_{\ell+3} \end{array} \begin{array}{c} \begin{array}{ccccccc} \{1\} & \{r, r^{-1}\} & \{r^2, r^{-2}\} & \cdots & \{r^\ell\} & \{s, sr^2, \ldots, sr^{2\ell-2}\} & \{sr, sr^3, \ldots, sr^{2\ell-1}\} \end{array} \\ \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 & 1 & 1 \\ 1 & 1 & 1 & \cdots & 1 & -1 & -1 \\ 1 & -1 & -1 & \cdots & -1 & 1 & -1 \\ 1 & -1 & -1 & \cdots & -1 & -1 & 1 \\ 2 & 2\cos(2\pi/n) & 2\cos(4\pi/n) & \cdots & 2\cos(2\ell\pi/n) & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 2 & 2\cos(2(\ell-1)\pi/n) & 2\cos(4(\ell-1)\pi/n) & \cdots & 2\cos(2(\ell-1)\ell\pi/n) & 0 & 0 \end{pmatrix} \end{array}$$

Remark. The character tables of D_4 and Q_8 are isomorphic to each other, even though D_4 and Q_8 are not isomorphic as groups.

[5] by examining their characters, it is easy to check that they are inequivalent. Conversely, for $k \geq \lfloor n/2 \rfloor$, examining their characters shows them to be equivalent to the aforementioned representations

2.6. Dimension Theorem

As we have already seen before, the orthogonality relations severely restrict how representations and characters of a group can behave. As it turns out, we can extract further mileage.

Definition 2.6 (Algebraic Integers)**.** A complex number $\alpha \in \mathbb{C}$ is said to be an algebraic integer if it is the root of a monic polynomial with integer coefficients.
We denote by $\mathbb{A}$ the set of algebraic integers.

Thus, $\sqrt{2}$ is an algebraic integer, while $1/2$ is not an algebraic integer. As it turns out, the only rational algebraic integers are the actual integers:

Lemma 2.22. $\mathbb{A} \cap \mathbb{Q} = \mathbb{Z}$.

Proof. By the rational root theorem, if a rational number is a root of a polynomial with integer coefficients, then the denominator (in the reduced form) of the rational number must divide 1, i.e., it must equal ± 1. But that implies that the rational number is actually an integer. ■

We shall now prove that $\mathbb{A}$ is actually a subring of $\mathbb{C}$. To do that, we need the following lemma:

Lemma 2.23. $\lambda \in \mathbb{A}$ iff there exists a matrix $A \in \mathbb{Z}^{n\times n}$ such that λ is an eigenvalue of A, i.e. there exists a $v \in \mathbb{C}^n \setminus \{0\}$ such that $Av = \lambda v$.

Proof. Note that the eigenvalues of a matrix with integral entries are also algebraic integers, since $\det(A - xI)$ is a monic polynomial in x with integral coefficients.
Conversely, suppose $\lambda \in \mathbb{A}$. Then $\lambda^n + a_{n-1}\lambda^{n-1} + \cdots + a_0 = 0$ for some integers $a_0, \ldots, a_{n-1} \in \mathbb{Z}$. Then:

$$\begin{bmatrix} 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 \\ -a_0 & -a_1 & -a_2 & -a_3 & \cdots & -a_{n-1} \end{bmatrix} \cdot \begin{bmatrix} 1 \\ \lambda \\ \lambda^2 \\ \vdots \\ \lambda^{n-2} \\ \lambda^{n-1} \end{bmatrix} = \lambda \cdot \begin{bmatrix} 1 \\ \lambda \\ \lambda^2 \\ \vdots \\ \lambda^{n-2} \\ \lambda^{n-1} \end{bmatrix}$$

■

Remark. Also, note that if $\alpha \in \mathbb{A}$, then $\overline{\alpha} \in \mathbb{A}$: Indeed, if $Av = \alpha v$ for some $A \in \mathbb{Z}^{n\times n}$, then $A\overline{v} = \overline{\alpha v}$.

Theorem 2.24. $\mathbb{A}$ is a subring of $\mathbb{C}$.

Proof. Suppose $\lambda_1, \lambda_2 \in \mathbb{A}$, with λ_1 being an eigenvalue of $A_1 \in \mathbb{Z}^{n_1\times n_1}$, and λ_2 being an eigenvalue of $A_2 \in \mathbb{Z}^{n_2\times n_2}$. Then $\lambda_1\lambda_2$ is an eigenvalue of $A_1 \otimes A_2 \in \mathbb{Z}^{n_1n_2\times n_1n_2}$ (in particular, if $\lambda \in \mathbb{A}$, then $-\lambda \in \mathbb{A}$ since $-1 \in \mathbb{A}$), and $\lambda_1 + \lambda_2$ is an eigenvalue of $A_1 \oplus A_2 := A_1 \otimes I_{n_2} + I_{n_1} \otimes A_2$. ■

Remark. If the corresponding eigenvectors of λ_1, λ_2 are v_1, v_2 respectively, then $v_1 \otimes v_2$ is the eigenvector for $\lambda_1\lambda_2$, since $(A_1 \otimes A_2)(v_1 \otimes v_2) = (A_1v_1) \otimes (A_2v_2) = \lambda_1v_1 \otimes \lambda_2v_2 = \lambda_1\lambda_2(v_1 \otimes v_2)$. $v_1 \otimes v_2$ is also the eigenvector for $\lambda_1 + \lambda_2$, since $(A_1 \otimes I_{n_2} + I_{n_1} \otimes A_2)(v_1 \otimes v_2) = (A_1v_1) \otimes (I_{n_2}v_2) + (I_{n_1}v_1) \otimes (A_2v_2) = \lambda_1v_1 \otimes v_2 + \lambda_2v_1 \otimes v_2$, as desired.

We finally link algebraic integers to representation theory.

Lemma 2.25. Let $\varphi : G \mapsto \mathrm{GL}_m(\mathbb{C})$ be a representation of a finite group G (with $|G| = n$), and let χ be the corresponding character. Then $\chi(g)$ is the sum of m n^{th}-roots of unity, and consequently $\chi(g)$ is an algebraic integer for all $g \in G$, since the roots of unity are algebraic integers.

Proof. Note that for any g, $\chi_\varphi(g)$ is the trace of $\varphi(g)$. Also recall that the trace of a matrix is the sum of its eigenvalues. Furthermore, since $|G| = n$, $g^n = 1$ for all $g \in G$, and thus $\varphi(g)^n = I$. Now, WLOG we can assume φ to be unitary, in which case $\varphi(g)$ is unitary and hence diagonalizable, and thus the eigenvalues of $\varphi(g)$ are the n^{th} roots of unity since $\varphi(g)^n = I$. Thus we're done. ∎

We shall now establish a series of lemmata which will lead us to the so-called dimension theorem, which says that the degree of an irreducible representation must divide the order of the group.
Let G be a group of order n, and let $\{C_1, \dots, C_s\}$ be the conjugacy classes of G, with $C_1 = \{1\}$. Let n_i be the size of C_i. Let φ be an irreducible representation of G, and write $d := \deg(\varphi), \chi_i := \chi_\varphi(C_i), T_i := \sum_{x \in C_i} \varphi_x$.

Lemma 2.26. $T_i = (n_i \chi_i / d) \cdot I$.

Proof. We will show that $T_i \in \mathrm{Hom}(\varphi, \varphi)$, which will imply (by Lemma 2.1) that $T_i = \lambda I$ for some $\lambda \in \mathbb{C}$. But then:

$$d\lambda = \mathrm{tr}(\lambda I) = \mathrm{tr}(T_i) = \sum_{x \in C_i} \mathrm{tr}(\varphi_x) = \sum_{x \in C_i} \chi_\varphi(x) = \sum_{x \in C_i} \chi_i = n_i \chi_i \implies \lambda = n_i \chi_i / d$$

as desired. Now, towards proving that $T_i \in \mathrm{Hom}(\varphi, \varphi)$, note that

$$\varphi_g T \varphi_{g^{-1}} = \sum_{x \in C_i} \varphi_g \varphi_x \varphi_{g^{-1}} = \sum_{x \in C_i} \varphi_{gxg^{-1}} = T_i$$

where the last line follows since C_i is a conjugacy class, and hence $gC_ig^{-1} = C_i$ for any g. ∎

Lemma 2.27. There exists $(a_{ijk}) \in \mathbb{Z}^{s \times s \times s}$ such that for any i, j, k, $T_iT_j = \sum_{k=1}^{s} a_{ijk} T_k$.

Proof. Note that

$$T_iT_j = \sum_{x \in C_i, y \in C_j} \varphi_{xy} = \sum_{g \in G} b_{ijg} \varphi_g$$

where b_{ijg} is the number of ways to write $g \in G$ as xy with $x \in C_i, y \in C_j$. Note that if we can prove $b_{ijg_1} = b_{ijg_2}$ for $g_1, g_2 \in G$ of the same conjugacy class, then we'd be done (with $a_{ijk} = n_k b_{ijg}$ for any $g \in C_k$). But note that if g_1, g_2 are conjugate, say as $g_1 = gg_2g^{-1}$ for some $g \in G$, then for every representation $g_2 = xy$, we can write $g_1 = gxyg^{-1} = (gxg^{-1})(gyg^{-1})$. Note that $gxg^{-1} \in C_i, gyg^{-1} \in C_j$, and thus we have an injection (clearly, if $(x_1, y_1) \neq (x_2, y_2)$, then $(gx_1g^{-1}, gy_1g^{-1}) \neq (gx_2g^{-1}, gy_2g^{-1})$) from the set of representations of g_2 as an element of C_iC_j to the set of representations of g_1 as an element of C_iC_j. We can easily obtain a reverse injection too, showing that these two sets are in bijection, and hence have the same cardinality. ∎

Lemma 2.28. $n_i \chi_i / d$ is an algebraic integer for all $i \in [s]$.

Proof. By Lemma 2.26, Lemma 2.27,

$$\frac{n_j\chi_j}{d}\cdot\frac{n_i\chi_i}{d}=\sum_{k=1}^{s}a_{ijk}\frac{n_k\chi_k}{d}$$

Thus if we define $A_i := (a_{ijk})_{j,k} \in \mathbb{Z}^{s\times s}$, and $v := (n_i\chi_i/d)_i$, then $A_iv = (n_i\chi_i/d)v$, and thus $n_i\chi_i/d \in \mathbb{A}$ by Lemma 2.23. ∎

We can finally prove the promised 'Dimension Theorem'.

Theorem 2.29. Let φ be an irreducible representation of degree d of a group G. Then $d \mid |G|$.

Proof. By Theorem 2.10, we have:

$$1=\langle\chi_\varphi,\chi_\varphi\rangle=\frac{1}{|G|}\sum_{g\in G}\overline{\chi_\varphi(g)}\chi_\varphi(g)\implies\frac{|G|}{d}=\sum_{g\in G}\overline{\chi_\varphi(g)}\frac{\chi_\varphi(g)}{d}$$

But

$$\sum_{g\in G}\overline{\chi_\varphi(g)}\frac{\chi_\varphi(g)}{d}=\sum_{i=1}^{s}\overline{\chi_i}\frac{n_i\chi_i}{d}$$

By Lemma 2.28, $\frac{n_i\chi_i}{d}\in\mathbb{A}$. Furthermore, since $\chi_i\in\mathbb{A}$, $\overline{\chi_i}\in\mathbb{A}$. Thus, since $\mathbb{A}$ is a ring, $|G|/d\in\mathbb{A}$. But $|G|/d$ is also a rational number, and thus $|G|/d\in\mathbb{Z}$, i.e. $d\mid|G|$. ∎

While the dimension theorem is undoubtedly a great theorem in representation theory, one sees its greatest power when it is used to prove group-theoretic statements which seem little to have to do with representation theory.

Theorem 2.30. Any group of order p^2, where p is a prime, is abelian.

Proof. Let $d_1,\dots,d_s$ be the degrees of the inequivalent irreducible representations of the group. Note that the trivial representation (which sends every element of the group to $1\in\mathrm{GL}_1(\mathbb{C})$) is irreducible, and has degree 1. Thus, WLOG $d_1=1$. Thus, $d_2^2+\cdots+d_s^2=p^2-1$. On the other hand, by the dimension theorem, $d_i\mid p^2\implies d_i=1,p,p^2$. However, if $d_i\geq p$, then $d_i^2\geq p^2>p^2-1$, which can't be the case. Thus, $d_i=1$ for all i. But that means that G is abelian. ∎

Turns out that one can extract even more information about representations from abstract properties of groups, which in turn help us characterize and classify the groups themselves.
Let G be a group. Recall the *commutator subgroup* of G was defined to be $G':=\langle xyx^{-1}y^{-1}\mid x,y\in G\rangle$. From standard group theory, we know that G' is normal in G, the quotient G/G' is abelian, and if N is any normal subgroup of G such that G/N is abelian, then $G'\leq N$, i.e. G' is the smallest normal subgroup of G which makes the quotient G/G' abelian.

Theorem 2.31. Any group G has $|G/G'|$ many inequivalent degree 1 representations.

Proof. Let $\rho:G\mapsto\mathbb{C}^\times$ be a degree 1 representation of G. We will show that ρ 'factors through' G'. Now, $\mathbb{C}^\times\geq\mathrm{im}(\rho)\cong G/\ker(\rho)$, and thus $G/\ker(\rho)$ is abelian. Consequently, $G'\leq\ker(\rho)$. Now, consider the map $\psi:G/G'\mapsto\mathbb{C}^\times$ defined as $\psi(gG'):=\rho(g)$. We claim that ψ is well-defined, since if $gG'=hG'$, then $g=hg'$ for some $g'\in G$, and thus $\rho(g)=\rho(h)\rho(g')=\rho(h)$, since $\rho(g')=1$, since $G'\leq\ker(\rho)$. It is also easy to verify that ψ is a homomorphism, and thus ψ is a representation of G/G'.

Conversely, for any representation $\psi : G/G' \mapsto \mathbb{C}^\times$, $\psi \circ \pi : G \mapsto \mathbb{C}^\times$ is a representation of G, where $\pi : G \mapsto G/G'$ is the canonical projection. Thus, the degree 1 representations of G are in bijection with the degree 1 representations of G/G'. But G/G' is abelian, and thus only has degree 1 representations, and we're done. ■

Remark. Note that degree 1 representations are always irreducible.

Theorem 2.32. Any group of order pq, where $p < q$ are primes such that $p \nmid (q-1)$, is abelian.

Proof. Once again, we have $pq = d_1^2 + \cdots + d_s^2$. By the dimension theorem, $d_i = 1, p, q, pq$. However, since $q > p$, $d_i = 1, p$. Now, let m be the number of inequivalent irreducible degree 1 representations. Then $pq = m + (s-m)p^2$. Thus, $p \mid m$. At the same time, m equals the cardinality of a quotient of our group, and thus $m \mid pq$. Thus, $m = p, pq$. However, if $m = p$, then we have $q = 1 + (s-p)p$, which is a contradiction, since $p \nmid (q-1)$. ■

§3. Fourier Analysis on Finite Abelian Groups

We explore the connections of Fourier analysis on finite groups with representation theory.
Let $f : \mathbb{Z} \mapsto \mathbb{C}$ be a periodic function, i.e. there is some $n \in \mathbb{N}$ for which $f(x+n) = f(x)$ for all $x \in \mathbb{Z}$. Then note that we can identify f with a function $f : \mathbb{Z}_n \mapsto \mathbb{C}$. Furthermore, since $\mathbb{Z}_n$ is abelian, $Z(L(\mathbb{Z}_n)) = L(\mathbb{Z}_n)$, and thus the characters of $\mathbb{Z}_n$ form an orthonormal basis for $Z(L(\mathbb{Z}_n)) = L(\mathbb{Z}_n)$, i.e. we can write:

$$f = \langle \chi_0, f \rangle \chi_0 + \cdots + \langle \chi_{n-1}, f \rangle \chi_{n-1}$$

The coefficients $\langle \chi_m, f \rangle$ are precisely the Fourier coefficients. We now present the definition for general finite abelian groups.

Definition 3.1 (Fourier Transforms for abelian groups)**.** Let $G = \{g_1, \ldots, g_n\}$ be a finite abelian group, and let $\chi_1, \ldots, \chi_n$ be some n inequivalent irreducible characters of G. Note that we are fixing an ordering on G and the characters for this.
Let $f : G \mapsto \mathbb{C}$. Then the Fourier transform of f, denoted as $\widehat{f} : G \mapsto \mathbb{C}$, is given by:

$$\widehat{f}(g_i) := n\langle \chi_i, f \rangle = \sum_{g \in G} \overline{\chi_i(g)} f(g)$$

Remark. A few remarks are due:

1. The Fourier transform is a linear transform $L(G) \mapsto L(G)$.
2. (**Fourier Inversion Formula**) The Fourier transform is invertible, i.e.

$$f = \frac{1}{n} \sum_{i=1}^{n} \widehat{f}(g_i) \chi_i$$

   Since the Fourier transform is invertible, it is injective. Since the Fourier transform is an injective linear map from a finite-dimensional vector space $L(G)$ to itself, it is invertible, even as a linear transform.
3. For the group $\mathbb{Z}/n\mathbb{Z}$,

$$\widehat{f}(m) = \sum_{k=0}^{n-1} e^{-2i\pi mk/n} f(k)$$

$$f(m) = \frac{1}{n} \sum_{k=0}^{n-1} e^{2i\pi mk/n} \widehat{f}(k)$$

   Note that for the group $\mathbb{Z}/n\mathbb{Z}$, there is a canonical ordering $0 < 1 < \cdots < n-1$ of the group, and a corresponding canonical order of the characters.
4. (**Plancherel's Formula**) For any $a, b \in L(G)$, we have

$$\langle a, b \rangle = \frac{1}{n} \langle \widehat{a}, \widehat{b} \rangle$$

   Indeed, by the Fourier Inversion Formula,

$$\langle a, b \rangle = \frac{1}{n^2} \sum_{i,j} \widehat{a}(g_i) \widehat{b}(g_j) \langle \chi_i, \chi_j \rangle = \frac{1}{n^2} \sum_{i,j} \widehat{a}(g_i) \widehat{b}(g_j) \delta_{ij} = \frac{1}{n} \langle \widehat{a}, \widehat{b} \rangle$$

We also introduce the convolution product:

Definition 3.2. Let G be a finite group, and let $f_1, f_2 \in L(G)$. Then

$$(f_1 * f_2)(x) := \sum_{y \in G} f_1(xy^{-1}) f_2(y)$$

We wish to use $*$ as an operator. For that, we first prove its associativity:

Proposition 15 (Associativity of $*$)**.** Let G be any group, and let $f_1, f_2, f_3 \in L(G)$ be arbitrary. Then

$$f_1 * (f_2 * f_3) = (f_1 * f_2) * f_3$$

Proof. Note that

$$(f_1 * (f_2 * f_3))(x) = \sum_{y \in G} f_1(xy^{-1}) \cdot (f_2 * f_3)(y) = \sum_{y \in G} f_1(xy^{-1}) \cdot \sum_{z \in G} f_2(yz^{-1}) f_3(z)$$

$$= \sum_{z \in G} \left(\sum_{y \in G} f_1(xy^{-1}) f_2(yz^{-1}) \right) \cdot f_3(z) = \sum_{z \in G} \left(\sum_{a \in G} f_1(a) f_2(a^{-1}xz^{-1}) \right) \cdot f_3(z) = \sum_{z \in G} (f_1 * f_2)(xz^{-1}) f_3(z)$$

$$= ((f_1 * f_2) * f_3)(x)$$

■

Denote by δ_g the function $\delta_g : G \mapsto \mathbb{C}$, $\delta_g(h) := \mathbb{1}_{g=h}$. Then:

Proposition 16. $\delta_g * \delta_h = \delta_{gh}$.

Proof.

$$(\delta_g * \delta_h)(x) = \sum_{y \in G} \delta_g(xy^{-1}) \delta_h(y) = \delta_g(xh^{-1}) = \delta_{gh}(x)$$

■

Remark. The above proposition also immediately highlights that $*$ is not a commutative operation for general groups G.

Proposition 17. $\widehat{\chi}_i = n\delta_{g_i}$.

Proof. Note that:

$$\widehat{\chi}_i(g_j) = n\langle \chi_j, \chi_i \rangle = \delta_{ij} n$$

■

The reason the convolution product is so interesting is that it turns $L(G)$ into a *non-commutative* ring. [6]

[6] note that there is another way to turn $L(G)$ into a ring, namely, by addition and pointwise multiplication of functions.

Lemma 3.1. $(L(G), +, *, 0, \delta_1)$ is a ring.

Proof. Note that $*$ is a bonafide multiplication operator since it is associative. Thus, to verify the ring structure, we just need to verify the distributivity of $*$ over $+$ and confirm that δ_1 is indeed the multiplicative identity.
The distributivity is easy to verify. To note that δ_1 is the identity, note that for any $f \in L(G)$, we have:

$$f = \sum_{g \in G} f(g)\delta_g$$

Thus,

$$f * \delta_1 = \sum_{g \in G} f(g)\delta_g * \delta_1 = \sum_{g \in G} f(g)\delta_g = f$$

$$\delta_1 * f = \sum_{g \in G} f(g)\delta_1 * \delta_g = \sum_{g \in G} f(g)\delta_g = f$$

■

We can finally explain the notation $Z(L(G))$:

Lemma 3.2. $Z(L(G))$ is the center of the ring $L(G)$, i.e.

$$Z(L(G)) = \{f \in L(G) : f * a = a * f \text{ for all } a \in L(G)\}$$

Proof. Suppose f is a class function. Then

$$(f * a)(x) = \sum_{y \in G} f(xy^{-1})a(y)$$

Substitute $y = xz^{-1}$: As z varies over G, y also varies over G. Thus,

$$\sum_{y \in G} f(xy^{-1})a(y) = \sum_{z \in G} a(xz^{-1})f(xzx^{-1})$$

Since f is a class function, $f(xzx^{-1}) = f(z)$. Substituting this above yields that $f * a = a * f$, as desired.
Conversely, suppose $f * a = a * f$ for all $a \in L(G)$. Set $a = \delta_g$ for some $g \in G$. Then:

$$(f * \delta_g)(x) = \sum_{y \in G} f(xy^{-1})\delta_g(y) = f(xg^{-1})$$

$$(\delta_g * f)(x) = \sum_{y \in G} \delta_g(xy^{-1})f(y) = f(g^{-1}x)$$

Set $x = gh$ for any $h \in G$. Then $f(h) = f(ghg^{-1})$ for all $g, h \in G$. Thus f is a class function. ■

Corollary 3.3. $L(G)$ is a commutative ring if and only if G is an abelian group.

Proof. Note that $\dim(Z(L(G))) = |\operatorname{Cl}(G)|$. If G is abelian, then $|\operatorname{Cl}(G)| = |G|$, and we have $Z(L(G)) = L(G)$, i.e. $L(G)$ is a commutative ring. Conversely, if G is not abelian, then $Z(L(G)) \subsetneq L(G)$, i.e. $L(G)$ is not commutative. ■

As mentioned above, there is another possible ring structure to $L(G)$, namely, $(L(G), +, \cdot, 0, \mathbf{1})$, where $\mathbf{1}(x) := 1$ for all $x \in G$, and the multiplication is the usual pointwise multiplication:

$$(f \cdot g)(x) := f(x)g(x)$$

Note that $(L(G), +, \cdot, 0, \mathbf{1})$ is a commutative ring. One very surprising facet of Fourier analysis is the following result:

Theorem 3.4. The map $f \mapsto \widehat{f}$ induces a ring isomorphism from $(L(G), +, *, 0, \delta_1)$ to $(L(G), +, \cdot, 0, \mathbf{1})$. Equivalently, $\widehat{f_1 * f_2} = \widehat{f_1} \cdot \widehat{f_2}$ for all $f_1, f_2 \in L(G)$.

Remark. One may be puzzled as to how a non-commutative ring such as $(L(G), +, *, 0, \delta_1)$ is isomorphic to a commutative ring such as $(L(G), +, \cdot, 0, \mathbf{1})$. However, note that we have only defined the Fourier transform for abelian groups, and for abelian groups, the ring $(L(G), +, *, 0, \delta_1)$ is commutative.

Proof. Note that:

$$\widehat{f_1 * f_2}(g_i) = n\langle \chi_i, f_1 * f_2 \rangle = \sum_{g \in G} \overline{\chi_i(g)}(f_1 * f_2)(g) = \sum_{g \in G} \overline{\chi_i(g)} \sum_{h \in G} f_1(gh^{-1})f_2(h) = \sum_{h \in G} f_2(h) \sum_{g \in G} \overline{\chi_i(g)} f_1(gh^{-1})$$

Put $z = gh^{-1}$. As g varies over G, z also varies over G. Then:

$$\sum_{h \in G} f_2(h) \sum_{g \in G} \overline{\chi_i(g)} f_1(gh^{-1}) = \sum_{h \in G} f_2(h) \sum_{z \in G} \overline{\chi_i(zh)} f_1(z)$$

By Proposition 9, $\chi_i(zh) = \chi_i(z)\chi_i(h)$. Thus,

$$\sum_{h \in G} f_2(h) \sum_{z \in G} \overline{\chi_i(zh)} f_1(z) = \sum_{h \in G} \overline{\chi_i(h)} f_2(h) \sum_{z \in G} \overline{\chi_i(z)} f_1(z) = \sum_{z \in G} \overline{\chi_i(z)} f_1(z) \sum_{h \in G} \overline{\chi_i(h)} f_2(h)$$

$$= n\langle \chi_i, f_1 \rangle \cdot n\langle \chi_i, f_2 \rangle = \widehat{f_1}(g_i)\widehat{f_2}(g_i)$$

Finally, we also verify that $0 \mapsto 0, \delta_1 \mapsto \mathbf{1}$: The first assertion is clear, and

$$\widehat{\delta_1}(g_i) = \sum_{g \in G} \overline{\chi_i(g)} \delta_1(g) = \overline{\chi_i(1)} = 1$$

■

Remark. A few remarks are due:

1. One 'practical' relevance of the above theorem is as follows: Note that computing $f_1 * f_2$ is of great importance in real life: Indeed, suppose $\sum_{g \in G} f_1(g) = \sum_{g \in G} f_2(g) = 1$, with $f_1(g), f_2(g) \geq 0$ for all $g \in G$. Let X_i be a random variable on G with distribution f_i, $i \in \{1, 2\}$. Then $f_1 * f_2$ is the probability distribution of $X_1 + X_2$. Then the above theorem suggests an alternative (to the usual summation) to computing $f_1 * f_2$: We may first calculate $\widehat{f_1 * f_2} = \widehat{f_1} \cdot \widehat{f_2}$, and use the Fourier inversion formula to get $f_1 * f_2$. While this might seem needlessly complicated at first, as it turns out, algorithmically this is the way to go, because Fourier transforms are very efficiently calculated through Fast Fourier Transforms.

2. A parallel theory holds for the usual Fourier analysis on $\mathbb{R}$: Indeed, recall that for $\mathbb{Z}/n\mathbb{Z}$, we have:

$$(f_1 * f_2)(m) := \sum_{k=0}^{n-1} f_1(m-k)f_2(k)$$

$$\widehat{f}(m) := \sum_{k=0}^{n-1} e^{-2i\pi mk/n} f(k)$$

$$f(m) = \frac{1}{n}\sum_{k=0}^{n-1} e^{2i\pi mk/n}\widehat{f}(k)$$

$$f \mapsto \widehat{f} \text{ induces a vector-space automorphism } L(G) \xrightarrow{\sim} L(G)$$

Similarly, for $\mathbb{R}$, we define the so-called *Schwartz space*, i.e.:

$$\mathcal{S}(\mathbb{R}) := \{f \in C^\infty_{\mathbb{C}}(\mathbb{R}) : x^n \cdot f^{(m)}(x) \xrightarrow{x\to\pm\infty} 0 \ \forall n, m \geq 0\}$$

where recall that $C^\infty_{\mathbb{C}}(\mathbb{R})$ is the space of all smooth functions from $\mathbb{R}$ to $\mathbb{C}$, and $f^{(m)} := \frac{d^m f}{dx^m}$ is the m^{th} derivative of f, where the zeroth derivative of f is defined to be f itself. Then we have:

$$(f_1 * f_2)(x) := \int_{-\infty}^{\infty} f_1(x-y)f_2(y)dy$$

$$\widehat{f}(\xi) := \int_{-\infty}^{\infty} e^{-2i\pi\xi x} f(x)dx$$

$$f(x) = \int_{-\infty}^{\infty} e^{2i\pi x\xi}\widehat{f}(\xi)d\xi$$

$$f \mapsto \widehat{f} \text{ induces a vector-space automorphism } \mathcal{S}(\mathbb{R}) \xrightarrow{\sim} \mathcal{S}(\mathbb{R})$$

One can even equip $\mathcal{S}(\mathbb{R})$ with a suitable topology such that the map $f \mapsto \widehat{f}$ becomes a homeomorphism.

We will now use Fourier analysis for abelian groups to calculate eigenvalues of the Cayley graph.

3.1. Eigenvalues of the Cayley Graph

Definition 3.3 (Symmetric Subset)**.** Let G be a finite group. A subset $S \subseteq G$ is said to be symmetric if:

1. $1 \notin S$,
2. $g \in S \iff g^{-1} \in S$

Definition 3.4. Let G be a finite group, and let $S \subseteq G$ be a symmetric subset. Then the Cayley graph of G w.r.t S, denoted as $\mathrm{Cay}(G, S)$, is a graph with vertex set G, and two vertices g, h are adjacent if $gh^{-1} \in S$.

Remark. Since S is symmetric, $gh^{-1} \in S$ implies that $hg^{-1} \in S$, and thus the above graph is undirected.

We now link the spectrum of Cayley graphs to the representations of the underlying group.

Lemma 3.5. Let $G = \{g_1, \ldots, g_n\}$ be an abelian group, and let $\chi_1, \ldots, \chi_n$ be its inequivalent irreducible characters. Fix some $a \in L(G)$, and define the convolution operator $F : L(G) \mapsto L(G)$ as $F(b) := a * b$.
Then F is a linear operator, with eigenvectors $\chi_1, \ldots, \chi_n$, and eigenvalues $\widehat{a}(g_1), \ldots, \widehat{a}(g_n)$ respectively. Since $\chi_1, \ldots, \chi_n$ form an orthonormal system, we also have that F is a diagonalizable operator.

Proof. The linearity of F is clear. Now, $\widehat{a * \chi_i} = \widehat{a} \cdot \widehat{\chi_i} = \widehat{a} \cdot n\delta_{g_i}$. Also, $(\widehat{a} \cdot n\delta_{g_i})(x) = n\widehat{a}(x) \cdot \delta_{g_i}(x) = n\widehat{a}(g_i) \cdot \delta_{g_i}(x)$, and thus $\widehat{a} \cdot n\delta_{g_i} = n\widehat{a}(g_i) \cdot \delta_{g_i}$. Now, for any function f, we know that:

$$f = \frac{1}{n} \sum_{i=1}^{n} \widehat{f}(g_i)\chi_i$$

Thus,

$$a * \chi_i = \frac{1}{n} \sum_{j=1}^{n} (n\widehat{a}(g_i) \cdot \delta_{g_i})(g_j)\chi_j = \widehat{a}(g_i)\chi_i$$

as desired. ■

We can finally calculate the desired eigenvalues:

Theorem 3.6 (Spectrum of the Cayley graph of abelian groups)**.** Let $G = \{g_1, \ldots, g_n\}$ be an abelian group, and let $\chi_1, \ldots, \chi_n$ be its inequivalent irreducible characters. Let $S \subseteq G$ be a symmetric set, and let A be the adjacency matrix of $\mathrm{Cay}(G, S)$. Then:

1. The eigenvalues of A are, for $1 \leq i \leq n$,
$$\lambda_i = \sum_{i \in S} \chi_i(s)$$
2. The corresponding orthonormal basis of eigenvectors is given by $v_1, \ldots, v_n$, where
$$v_i := \begin{bmatrix} \chi_i(g_1) & \chi_i(g_2) & \cdots & \chi_i(g_n) \end{bmatrix}^{\mathsf{T}}$$
Note that
$$\begin{bmatrix} v_1^{\mathsf{T}} \\ v_2^{\mathsf{T}} \\ \vdots \\ v_n^{\mathsf{T}} \end{bmatrix}$$
is just the character table of G! Also, note that the eigenvectors don't depend on S.

Proof. Write δ_S for the function $\delta_S : G \mapsto \mathbb{C}$, where $\delta_S(s) = 1$ for all $s \in S$, and 0 otherwise.
Let $F : L(G) \mapsto L(G)$, $F(a) := \delta_S * a$. Also, let $\mathcal{B} = (\delta_{g_1}, \ldots, \delta_{g_n})$ be a basis for $L(G)$. We claim that $[F]_{\mathcal{B}}$, i.e. the matrix F expressed in the basis $\mathcal{B}$, is equal to the matrix A. Indeed,

$$F(\delta_{g_\alpha}) = \delta_S * \delta_{g_\alpha} = \left(\sum_{s \in S} \delta_s \right) * \delta_{g_\alpha} = \sum_{s \in S} \delta_s * \delta_{g_\alpha} = \sum_{s \in S} \delta_{sg_\alpha}$$

Now, note that the $(i,j)^{\text{th}}$ entry of $[F]_{\mathcal{B}}$ is the coefficient of δ_{g_i} in $F(\delta_{g_j})$, which is 1 if $g_i = sg_j$ for some $s \in S$, and 0 otherwise. In other words,

$$([F]_{\mathcal{B}})_{ij} = \mathbb{1}_{g_i = sg_j, s \in S} = \mathbb{1}_{g_i g_j^{-1} \in S} = A_{ij}$$

At this point, the eigenbasis part is done by Lemma 3.5. For the eigenvalues, note that:

$$\widehat{\delta_S}(g_i) = n\langle \chi_i, \delta_S \rangle = \sum_{g \in G} \overline{\chi_i(g)}\delta_S(g) = \sum_{g \in S} \overline{\chi_i(g)}$$

By Proposition 9, $\chi_i : G \mapsto \mathbb{C}^\times$ is a homomorphism. Furthermore, we can take the underlying representation of χ_i to be unitary, i.e. $\chi_i(g)\overline{\chi_i(g)} = 1$. Thus $\overline{\chi_i(g)} = \chi_i(g)^{-1} = \chi_i(g^{-1})$, and thus

$$\sum_{g \in S} \overline{\chi_i(g)} = \sum_{g^{-1} \in S} \chi_i(g) = \sum_{g \in S} \chi_i(g)$$

where the last equality follows since S is symmetric. ■

Remark. A few remarks are due:

1. Alon and Roichman [AR94] proved that for every $\delta \in (0,1)$, there exists a constant $c(\delta) > 0$ such that if S is a random subset of G (where G is *any* group, not necessarily abelian) of size $2c(\delta)\log n$ (we first sample $c(\delta)\log n$ elements from G uniformly and independently, and then we add their inverses to S. Note that we retain elements with multiplicity, i.e. S is a multiset. However, this is not a major issue.), then the expected value of the second largest eigenvalue of the normalized adjacency matrix of $\mathrm{Cay}(G,S)$ is at most $1-\delta$. Furthermore, for abelian groups, this result is optimal. Consequently, Cayley graphs of groups can be used to construct expanders.
2. Similar results can be shown for Cayley graphs of non-abelian groups G if the set S is conjugate, i.e. $g \in S \implies xgx^{-1} \in S$ for all $x \in G$.

§4. Fourier Analysis on Finite Non-Abelian Groups

Note that we can't extend the usual definition of Fourier transforms on abelian groups to non-abelian groups, since non-abelian groups don't have n inequivalent irreducible representations. Thus, we'll first try to re-interpret the Abelian case where a generalization becomes more apparent.
Let G be an abelian group, and let $f : G \mapsto \mathbb{C}$ be a function. Then define the map $T : L(G) \mapsto \mathbb{C}^n$, where

$$Tf := (n\langle\chi_1, f\rangle, n\langle\chi_2, f\rangle, \dots, n\langle\chi_n, f\rangle) = (\widehat{f}(g_1), \widehat{f}(g_2), \dots, \widehat{f}(g_n))$$

Clearly, T is linear. By the Fourier inversion formula, it is also invertible. Since T is an invertible linear map between two vector spaces, the vector spaces must be isomorphic, which is indeed the case since $L(G) = \mathbb{C}^G \cong \mathbb{C}^n$.
Now, since all irreducible representations of abelian groups are one-dimensional, the Fourier transform Tf has "one-dimensional components". However, for a non-abelian group, we won't have one-dimensional, but rather matrix-valued components. Putting it into words yields:

Definition 4.1 (Fourier Transforms on Non-Abelian Groups)**.** Let G be any finite group, and let $\varphi^{(1)}, \dots, \varphi^{(s)}$ be the inequivalent irreducible unitary representatives of all irreducible representations of G, and write $d_i := \deg(\varphi^{(i)})$. Then for any $f \in L(G)$, we define the Fourier transform of f to be:

$$T : L(G) \mapsto \mathbb{C}^{d_1 \times d_1} \times \cdots \times \mathbb{C}^{d_s \times d_s}$$

$$f \mapsto (\widehat{f}(\varphi^{(1)}), \widehat{f}(\varphi^{(2)}), \dots, \widehat{f}(\varphi^{(s)}))$$

where

$$\widehat{f}(\varphi^{(k)}) := \sum_{g \in G} \overline{\varphi_g^{(k)}} f(g)$$

More explicitly,

$$\widehat{f}(\varphi^{(k)})_{ij} = \sum_{g \in G} \overline{\varphi_{ij}^{(k)}(g)} f(g) = n\langle\varphi_{ij}^{(k)}, f\rangle \tag{4.1}$$

We now prove the Fourier inversion formula:

Theorem 4.1 (Fourier Inversion Formula)**.** Let $f : G \mapsto \mathbb{C}$ be a function. Then

$$f = \frac{1}{n} \sum_{i,j,k} d_k \widehat{f}(\varphi^{(k)})_{ij} \varphi_{ij}^{(k)}$$

Recall that $\varphi_{ij}^{(k)} : G \mapsto \mathbb{C}$ is the function such that $\varphi_{ij}^{(k)}(g) := (\varphi_g^{(k)})_{ij}$.

Proof. Recall from Corollary 2.15 that $\left\{\sqrt{d_k}\varphi_{ij}^{(k)} : k \in [s], i, j \in [d_k]\right\}$ is an orthonormal basis for $\mathbb{C}^G = L(G)$. Thus

$$f = \sum_{i,j,k} \langle\sqrt{d_k}\varphi_{ij}^{(k)}, f\rangle \sqrt{d_k}\varphi_{ij}^{(k)} = \frac{1}{n} \sum_{i,j,k} d_k n\langle\varphi_{ij}^{(k)}, f\rangle \varphi_{ij}^{(k)} \overset{\text{Eq. (4.1)}}{=} \frac{1}{n} \sum_{i,j,k} d_k \widehat{f}(\varphi^{(k)})_{ij} \varphi_{ij}^{(k)}$$

■

Corollary 4.2. If we regard both $L(G)$ and $\mathbb{C}^{d_1 \times d_1} \times \cdots \times \mathbb{C}^{d_s \times d_s}$ as $\mathbb{C}$-vector spaces, then T furnishes a vector space isomorphism between these two.

Proof. It is clear that T is linear. By Fourier inversion formula, it is also clear that T is injective. Now, note that

$$\dim_{\mathbb{C}}(\mathbb{C}^{d_1\times d_1}\times\cdots\times\mathbb{C}^{d_s\times d_s})=\sum_{i=1}^{n}d_i^2=|G|=\dim_{\mathbb{C}}(L(G))$$

Since T is an injective linear map between two finite-dimensional vector spaces of the same dimension, T is actually an isomorphism. ∎

We finish this chapter by proving a generalization of Theorem 3.4 for all finite groups.

Theorem 4.3 (Wedderburn's Theorem)**.** The Fourier transform

$$T:L(G)\mapsto\mathbb{C}^{d_1\times d_1}\times\cdots\times\mathbb{C}^{d_s\times d_s}$$

is a ring isomorphism between $(L(G),+,*,0,\delta_1)$ and the usual ring $\mathbb{C}^{d_1\times d_1}\times\cdots\times\mathbb{C}^{d_s\times d_s}$.

Proof. As with Theorem 3.4, the main statement to be shown is that $T(a*b)=Ta\cdot Tb$. Equivalently, we have to show $\widehat{a*b}(\varphi^{(k)})=\widehat{a}(\varphi^{(k)})\widehat{b}(\varphi^{(k)})$. Note that:

$$\widehat{a*b}(\varphi^{(k)})=\sum_{g\in G}\overline{\varphi_g^{(k)}}(a*b)(g)=\sum_{g\in G}\overline{\varphi_g^{(k)}}\sum_{h\in G}a(gh^{-1})b(h)=\sum_{h\in G}b(h)\sum_{g\in G}\overline{\varphi_g^{(k)}}a(gh^{-1})$$

Set $x=gh^{-1}$. Then

$$\sum_{h\in G}b(h)\sum_{g\in G}\overline{\varphi_g^{(k)}}a(gh^{-1})=\sum_{h\in G}b(h)\sum_{x\in G}\overline{\varphi_{xh}^{(k)}}a(x)=\sum_{h\in G}b(h)\sum_{x\in G}\overline{\varphi_x^{(k)}}\cdot\overline{\varphi_h^{(k)}}a(x)=\sum_{h\in G}\sum_{x\in G}a(x)\overline{\varphi_x^{(k)}}\cdot b(h)\overline{\varphi_h^{(k)}}$$

$$=\left(\sum_{x\in G}a(x)\overline{\varphi_x^{(k)}}\right)\cdot\left(\sum_{h\in G}b(h)\overline{\varphi_h^{(k)}}\right)=\widehat{a}(\varphi^{(k)})\widehat{b}(\varphi^{(k)})$$

Finally, we have to verify that δ_1 gets sent to the multiplicative identity of $\mathbb{C}^{d_1\times d_1}\times\cdots\times\mathbb{C}^{d_s\times d_s}$: Indeed,

$$\widehat{\delta_1}(\varphi^{(k)})=\sum_{g\in G}\overline{\varphi_g^{(k)}}\delta_1(g)=\overline{\varphi_1^{(k)}}=\mathrm{Id}\in\mathbb{C}^{d_k\times d_k}$$

∎

References

[AR94] Noga Alon and Yuval Roichman. Random cayley graphs and expanders. *Random Structures & Algorithms*, 5(2):271–284, 1994. URL: https://onlinelibrary.wiley.com/doi/abs/10.1002/rsa.3240050203, arXiv:https://onlinelibrary.wiley.com/doi/pdf/10.1002/rsa.3240050203, doi:10.1002/rsa.3240050203.

[Ste11] B. Steinberg. *Representation Theory of Finite Groups: An Introductory Approach*. Universitext. Springer New York, 2011. URL: https://books.google.co.in/books?id=hKHrk6cti8YC.