Representation Theory of Finite Groups

Amit Rajaraman

Last updated July 11, 2022

Contents

§-1. Notation

Given a set X, S_X is the set of all bijections from X to itself.

§0. Preliminaries

We define precisely those things that the author of these notes did not know at the time of reading. If there are things in these notes you do not know that are not defined anywhere within the notes, too bad!

0.1. Algebra

Definition 0.1. Given a group G, $\hat{G}$ denotes the set of all group homomorphisms from $G \to \mathbb{C}^*$. This is a group under point-wise operations and is called the *dual group* of G.

Proposition 0.1. If G_1, G_2 are groups and $G = G_1 \times G_2$, then $\hat{G} \cong \hat{G_1} \times \hat{G_2}$.

Proof. Let $\varphi \in \hat{G}$. Define the homomorphism $\Phi : \hat{G} \to \hat{G_1} \times \hat{G_2}$ by $\varphi \mapsto (\varphi_1, \varphi_2)$, where

$$\varphi_1(g_1) = \varphi(g_1, 1) \text{ and } \varphi_2(g_2) = \varphi(2, g_2).$$

Let us show that Φ is injective by showing that precisely one $\varphi \in \hat{G}$ maps to $(1, 1)$. Indeed, this would imply that $\varphi(g_1, 1) = \varphi(1, g_2) = 1$ for all $g_1 \in G_2, g_2 \in G_2$. As φ is a homomorphism, $\varphi(g_1, g_2) = 1$ as well.
For surjectivity, let $(\rho_1, \rho_2) \in \hat{G_1} \times \hat{G_2}$. Consider $\varphi : G \to \mathbb{C}^*$ defined by $\varphi(g_1, g_2) = \rho_1(g_1)\rho_2(g_2)$. It is not difficult to show that $\varphi \in \hat{G}$ since ρ_1, ρ_2 are homomorphisms ■

Proposition 0.2. If $G = \mathbb{Z}/n\mathbb{Z}$, then $\hat{G} \sim G$.

Proof. Let $\varphi : G \to \mathbb{C}^*$ be a homomorphism. Observe that φ is determined by $\varphi(\overline{1})$. Further, since $n\overline{m} = 0$ for any $\overline{m} \in G$, $\varphi(\overline{m})^n = \varphi(0)$, so every $\varphi(g)$ is an nth root of unity. As a result, there are at most n elements in $\hat{G}$ corresponding to which of the n roots of unity $\overline{1}$ is mapped to – each such homomorphism $\varphi^{(k)}$ is of the form $\varphi(\overline{m}) = \omega_n^{km}$ for some k. It is easily checked that all of these do in fact correspond to homomorphisms.
Further, this group is cyclic because $\varphi^{(k)} = (\varphi^{(1)})^k$. ■

Theorem 0.3. For any finite abelian group G, $\hat{G} \sim G$.

This follows directly using the classification theorem of finite groups and the previous two propositions.

0.2. Linear Algebra

Proposition 0.4. Let $W \leq V$ be vector spaces and $T \in \mathrm{GL}(V)$. Then, T is W-invariant iff $T(W) = W$.

Definition 0.2. Let V be a finite dimensional inner product space and $T \in \mathrm{End}(V)$. The *adjoint* of T is the unique linear operator T^* such that for any $v, w \in V$,

$$\langle Tv, w\rangle = \langle v, T^*w\rangle.$$

Proposition 0.5. Let V be an inner product space and $T \in \mathrm{End}(V)$. Suppose that $W \leq V$ be T-invariant. Then, $W^\perp$ is T^*-invariant.

Proof. Let $w \in W^\perp$. Then for any $v \in W$, we have

$$0 = \langle Tv, w\rangle = \langle v, T^*w\rangle,$$

so $T^*w \in W^\perp$ and the desideratum follows. ■

Definition 0.3. Let V be an inner product space and $U \in \mathrm{GL}(V)$. U is said to be *unitary* if

$$\langle v, w\rangle = \langle Uv, Uw\rangle$$

for all $v, w \in V$.

In other words,

$$\langle v, U^*Uw\rangle = \langle v, w\rangle.$$

However, the identity map is its own adjoint, so $U^* = U^{-1}$.
The subset $U(V) \subseteq \mathrm{GL}(V)$ of all unitary operators forms a subgroup.

Definition 0.4. A matrix $U \in \mathrm{GL}_n(\mathbb{C})$ is said to be *unitary* if $U^*U = I_n$.

The set of all unitary matrices is denoted $U_n(\mathbb{C})$ and is a subgroup of $\mathrm{GL}_n(\mathbb{C})$.

Proposition 0.6. Let V be an inner product space and $T \in U(V)$. Suppose that $W \leq V$ is T-invariant. Then, $W^\perp$ is also T-invariant.

Proof. Recalling Proposition 0.5, we have that $W^\perp$ is T^{-1}-invariant. It then follows by Proposition 0.4 that $W^\perp$ is T-invariant as well ($T^{-1}(W^\perp) = W^\perp$ so $T(W^\perp) = W^\perp$). ■

Definition 0.5 (Minimal Polynomial)**.** Let $T \in \mathrm{End}(V)$. The *minimal polynomial* of T is the unique monic polynomial $m(X) \in \mathbb{C}[X]$ of minimal degree such that $m(T)$ is the zero operator.

Definition 0.6 (Diagonalisable)**.** Let $T \in \mathrm{End}(V)$. T is said to be *diagonalisable* if there exists a basis B of V consisting of eigenvectors of T.

For the rest of this section, we use T to denote an element of $\mathrm{End}(V)$ and $m(X)$ its minimal polynomial.

Proposition 0.7. Let $T \in \mathrm{End}(V)$, $m(X)$ be its minimal polynomial, and $p(X) \in \mathbb{C}[X]$ be any polynomial such that $p(T) = 0$. Then $p(\lambda) = 0$ for any eigenvalue $\lambda \in \mathbb{C}$ of T. In particular, all the eigenvalues of T (in $\mathbb{C}$) are roots of the minimal polynomial.

Proof. Suppose

$$p(X) = a_0 + a_1 X + \cdots + a_r X^r.$$

If λ is an eigenvalue of T and v ($\neq 0$) a corresponding eigenvector, then $T^k v = \lambda^k v$. So,

$$\begin{aligned} 0 = p(T)v &= \left(a_0 + a_1 T + \cdots + a_r T^r\right) v \\ &= \left(a_0 + a_1\lambda + a_2\lambda^2 + \cdots + a_r\lambda^r\right) v = p(\lambda)v. \end{aligned}$$

As $v \neq 0$, $p(\lambda) = 0$. ∎

As the minimal polynomial divides the characteristic polynomial, this says that the minimal polynomial and characteristic polynomial have precisely the same roots.

Theorem 0.8. Let $T \in \mathrm{End}(V)$ and $m(X)$ be its minimal polynomial. T is diagonalisable if and only if $m(X)$ has distinct roots.

Proof. First, suppose that T is diagonalisable.
Let $\lambda_1, \ldots, \lambda_r$ be the distinct eigenvalues of T. Consider

$$p(X) = (X - \lambda_1)(X - \lambda_2)\cdots(X - \lambda_r).$$

It is clear from the previous proposition that $p(X) \mid m(X)$. If we manage to show that $m(X) \mid p(X)$, then $m(X) = p(X)$ and we are done. To show this, it suffices to show that $p(T) = 0$, and to show this it suffices to show that $p(T)$ annihilates some basis of V. Towards this, let B be an eigenbasis of V with respect to T (since T is diagonalisable, this exists). Any $v \in B$ is annihilated by some $T - \lambda_i$. Since all the $(T - \lambda_i)$ commute, it follows that $p(T)$ vanishes on B, and thus V.

Now, suppose that $m(X)$ has distinct roots, and let it be equal to $(X - \lambda_1)\cdots(X - \lambda_r)$ for distinct $\lambda_i \in \mathbb{C}$. Let E_λ denote the eigenspace of λ. We wish to show that $V = \bigoplus_{i=1}^r E_{\lambda_i}$. Recall that eigenvectors corresponding to different eigenspaces are linearly independent. As a result, it suffices to show that $V = +_{i=1}^r E_{\lambda_i}$. For each $i \in [r]$, let

$$g_i(X) = \prod_{j \neq i} (X - \lambda_j)$$

and

$$f_i(X) = \frac{g_i(X)}{g_i(\lambda_i)}.$$

Observe that

$$1 = \sum_{i=1}^r f_i(X).$$

Indeed, they are polynomials of degree at most $r - 1$ that agree at the r points $(\lambda_i)_{i=1}^r$. As a result, for any $v \in V$,

$$v = \sum_{i=1}^r f_i(T)v.$$

If we manage to show that $f_i(T)v \in E_{\lambda_i}$, we are done. This is not too difficult to see as

$$(T - \lambda_i) f_i(T)v = \frac{1}{g_i(\lambda_i)} m(T)v = 0.$$ ∎

We now give a couple of general definitions that will come into use later in the notes.

Definition 0.7 (Center)**.** Let R be a ring. The *center* of R is denoted $Z(R)$ and defined as

$$Z(R) = \{r \in R : rs = sr \text{ for all } s \in R\}.$$

One can show that $Z(R)$ is a commutative subring of R.

0.3. Number Theory

Definition 0.8 (Algebraic integer)**.** $\alpha \in \mathbb{C}$ is said to be an *algebraic integer* if it is a root of a monic polynomial with integer coefficients. That is, there exists $n > 0$ and integers $a_0, \ldots, a_{n-1}$ such that $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$. The set of all algebraic integers is denoted $\mathbb{A}$.

The monic requirement is important. For example, $1/2$ is a root of $2z - 1$ which is not monic, and is in fact not an algebraic integer.

Example (Closure under negation and conjugation)**.** If $\alpha \in \mathbb{A}$, and p is a monic polynomial of degree n with $p(\alpha) = 0$, then considering the polynomial $z \mapsto (-1)^n p(-z)$ shows that $-\alpha \in \mathbb{A}$ as well. Since p has real coefficients, we also have that $\overline{\alpha} \in \mathbb{A}$.

Proposition 0.9. $\mathbb{A} \cap \mathbb{Q} = \mathbb{Z}$.

Proof. Let $r = p/q \in \mathbb{Q}$ be an algebraic integer with $p \in \mathbb{Z}$, $q \in \mathbb{N}$, and $\gcd(p, q) = 1$. Let $a_0, \ldots, a_{n-1} \in \mathbb{Z}$ with $r^n + a_{n-1}r^{n-1} + \cdots + a_0 = 0$. Multiplying with q^n gives $p^n + a_{n-1}qp^{n-1} + \cdots + a_0 q^n = 0$. Note that all of these terms but the first are divisible by q. Consequently, even the first term must be divisible by q. That is, $q \mid p^n$. Since $\gcd(p, q) = 1$, this implies that $q = 1$, proving the required. ∎

Example. Let A be a square integer matrix. The eigenvalues of A are precisely the roots of $\det(zI - A)$, which is a monic polynomial. As a result, any eigenvalue of an integer matrix is an algebraic integer.

It turns out that the above in fact characterizes all algebraic integers.

Proposition 0.10. $\alpha \in \mathbb{C}$ is an algebraic integer iff it is an eigenvalue of a square integer matrix A.

Proof. We have already seen that the backward implication is true.
Let $\alpha \in \mathbb{A}$ and $a_{n-1}, \ldots, a_0$ such that $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0$. Then, $\alpha^n = -a_{n-1}\alpha^{n-1} - \cdots - a_0$ and we get

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

completing the proof. ■

Proposition 0.11. $\mathbb{A}$ is a subring of $\mathbb{C}$.

Proof. It is easy to see that $0 \in \mathbb{A}$, and we already saw that it is closed under additive inverses. Let $\alpha, \beta \in \mathbb{A}$. ■

§1. Introduction

1.1. Basic Definitions

1.1.1. Representations

Definition 1.1 (Representation)**.** A *representation* of a group G is a homomorphism $\varphi : G \to \mathrm{GL}(V)$ for some finite-dimensional vector space V over $\mathbb{C}$. The *degree* of φ is the dimension of V.

Henceforth, V (or any other symbol for a vector space) is used to denote a non-trivial vector space over $\mathbb{C}$.
The map $\varphi(g)$ is typically denoted φ_g, and $\varphi_g(v)$ as $\varphi_g v$.
Note that since φ is a homomorphism, it is determined by its values on any generating set of G.
Recall that given a group G and set X, a group action of G on X is merely a function $G \to S_X$. Representations can thus be pictured as a special case of a group action where the image of any element is not just a bijection, it is linear.

Example. Let X be a set X and consider the *linearisation* $\mathbb{C}X$ of X, defined as the vector space with elements of the form $\sum_{x\in X} c_x x$, where each $c_x \in \mathbb{C}$, addition defined by

$$\sum_{x\in X} c_x x + \sum_{x\in X} d_x x = \sum_{x\in X} (c_x + d_x)x,$$

and scalar multiplication by

$$c \sum_{x\in X} c_x x = \sum_{x\in X} (cc_x)x.$$

It is clear that $\mathbb{C}X$ has basis X.
Observe that any group action of a group G on X extends to an action on $\mathbb{C}X$ as a representation! Indeed, we define

$$g \cdot \left(\sum_{x\in X} c_x x \right) = \sum_{x\in X} c_x (g \cdot x).$$

If V is a 1-dimensional vector space over $\mathbb{C}$, then $\mathrm{GL}(V) \cong \mathbb{C}$. In such a case, to stay sane, we usually write z instead of φ to denote a representation[1], so each z_g is a complex.
The trivial representation of a group G is the homomorphism $z : G \to \mathbb{C}^*$ given by $z_g = 1$ for all $g \in G$.

Example. Let $n \in \mathbb{N}$. Recall that $\mathrm{GL}(\mathbb{C}^*) \cong \mathrm{GL}(\mathbb{C})$, so any degree-one representation may be considered as a function $z : \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}^*$. However, recall from Proposition 0.2 that any representation is of the form defined by $z(\overline{m}) = \omega_n^{km}$ for some fixed $k \in \mathbb{N}$. It turns out that these are the "only" representations of a finite cyclic group (where "only" is defined in an appropriate sense, as we shall see later).

Observe that the above mentioned representations are incredibly restrictive, and we are barely using the fact that the representation is to $\mathbb{C}^*$.

[1] one could say that in such a scenario, z is used to *represent a representation*.

Example. Now, consider the degree-one representations $z : G \to \mathbb{C}^*$ of a non-Abelian group G. Recall the (Abelian) *commutator subgroup* $[G, G]$ of G consisting of elements of the form $xy - yx$. Because $\mathbb{C}^*$ is Abelian, $[G, G] \subseteq \ker z$. Consequently, z factors through the quotient as

$$\begin{array}{ccc} G & \xrightarrow{z} & \mathbb{C}^* \\ \downarrow & \nearrow_{\widetilde{z}} & \\ G/[G,G] & & \end{array}$$

As a result, when studying degree-one representations, it suffices to assume that the group is non-Abelian.

Why are representations useful? Consider the problem of, given a group G and $x, y \in G$, finding $x \in G$ such that $gxg^{-1} = y$. It might then be easier to find M such that $M\varphi_x M^{-1} = \varphi_y$ since testing matrix similarity is a well-studied problem. A g in the preimage of M may then be a good candidate for the required.

1.1.2. Equivalence

Let $\varphi : G \to \mathrm{GL}(V)$ be a degree-n representation. Let B, B' be two bases of V, and consider the two corresponding isomorphisms $T, T' : V \to \mathbb{C}^n$ mapping the basis elements of B, B' to the standard basis vectors of $\mathbb{C}^n$. We would then like that the two representations $\psi, \psi' : G \to \mathbb{C}^n$ defined by

$$\psi_g = T\varphi_g T^{-1} \text{ and } \psi'_g T'\varphi_g (T')^{-1}$$

are the same in some sense. Towards this, we define the following.

Definition 1.2. Two representations $\varphi : G \to \mathrm{GL}(V)$ and $\psi : G \to \mathrm{GL}(W)$ are said to be *equivalent* if there exists an isomorphism (an *equivalence*) $T : V \to W$ such that $\psi_g = T\varphi_g T^{-1}$ for all $g \in G$. If this is the case, we write $\varphi \sim \psi$.

Note that T must be independent of g!
The above definition can be represented as saying that there exists an equivalence $T : V \to W$ such that the following commutes for all $g \in G$.

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

Observe that V, W must be isomorphic, that is, φ, ψ are of the same degree.

Proposition 1.1. Let G be a group and $z, z^* : G \to \mathbb{C}^*$ be degree-one representations. Then, $z \sim z^*$ iff $z = z^*$.

Proof. Let $z \sim z^*$ and $T : \mathbb{C}^* \to \mathbb{C}^*$ be an equivalence. Then, for any $g \in G$,

$$\begin{aligned} z^*_g v &= T z_g T^{-1} v \\ &= z_g T T^{-1} v && (T \text{ is linear}) \\ &= z_g v, \end{aligned}$$

so $z = z'$. ∎

From Theorem 0.3 and Section 1.1.1, we get the following.

Corollary 1.2. Any finite group G has exactly $|G/[G, G]|$ inequivalent degree-one representations.

Recall Definition 0.1.

Corollary 1.3. If G is an abelian group, its $|G|$ degree-one representations (up to equivalence) are just the elements of $\hat{G}$.

1.1.3. Irreducibility

Definition 1.3 (Invariant subspace)**.** Let $\varphi : G \to \mathrm{GL}(V)$ be a representation. A subspace $W \leq V$ is said to be *G-invariant* with respect to φ if for all $g \in G$ and $w \in W$, $\varphi_g(W) = W$.

Observe that if $W \leq V$ is G-invariant with respect to φ, then $\varphi|_W : G \to \mathrm{GL}(W)$ defined by $(\varphi|_W)_g(w) = \varphi_g(w)$ is a representation. In such a case, $\varphi|_W$ is said to be a *subrepresentation* of W.
Based on the direct sum of vector spaces, one can similarly define the direct sum of representations.

Definition 1.4 (Direct sum)**.** Let $\varphi^{(1)} : G \to \mathrm{GL}(V_1)$ and $\varphi^{(2)} : G \to \mathrm{GL}(V_2)$ be representations. Then, their (external) *direct sum* is the representation $\varphi^{(1)} \oplus \varphi^{(2)} : G \to \mathrm{GL}(V_1 \oplus V_2)$ defined by

$$\left(\varphi^{(1)} \oplus \varphi^{(2)}\right)_g (v_1, v_2) = (\varphi_g^{(1)}(v_1), \varphi_g^{(1)}(v_2))$$

for all $g \in G$ and $(v_1, v_2) \in V_1 \oplus V_2$.

The above is more natural to picture using matrices.
If $V_1 = \mathrm{GL}_m(\mathbb{C})$ and $V_2 = \mathrm{GL}_n(\mathbb{C})$ above, then each $\varphi_g^{(i)}$ can be expressed as a matrix. The matrix in $\mathrm{GL}_{m+n}(\mathbb{C})$ corresponding to their direct sum is then given by

$$\left(\varphi^{(1)} \oplus \varphi^{(2)}\right)_g = \begin{pmatrix} \varphi_g^{(1)} & \\ & \varphi_g^{(2)} \end{pmatrix},$$

where the empty cells are appropriately sized 0 matrices.

Recall the trivial representation of a group G. Observe then that the representation $\varphi : G \to \mathrm{GL}_n(\mathbb{C})$ given by $\rho_g = I_n$ for all $g \in G$ is equivalent to the direct sum of n copies of the trivial representation.

Proposition 1.4. If $V_1, V_2 \leq V$ are G-invariant subspaces with respect to φ and $V = V_1 \oplus V_2$, then φ is equivalent to $\varphi|_{V_1} \oplus \varphi|_{V_2}$.

Proof. Consider the map $T : V \to V_1 \oplus V_2$ defined by $T(v_1 + v_2) = (v_1, v_2)$ ($V_1 \oplus V_2$ here is the external direct sum).

Let $\psi = \varphi|_{V_1} \oplus \varphi|_{V_2}$. Then,

$$\begin{aligned}\psi_g(v_1, v_2) &= \left(\left(\varphi|_{V_1}\right)_g(v_1), \left(\varphi|_{V_2}\right)_g(v_2)\right) \\ &= (\varphi_g(v_1), \varphi_g(v_2)) \\ &= T(\varphi_g(v_1) + \varphi_g(v_2)) \\ &= T\varphi_g(v_1 + v_2) \\ &= T\varphi_g T^{-1}(v_1, v_2).\end{aligned}$$ ■

Above, let B_i be a basis of V_i for $i = 1, 2$. Because each V_i is G-invariant, $\varphi_g(B_i) \subseteq \mathbb{C}B_i$. The matrix representation of $\varphi \cong \varphi^{(1)} \oplus \varphi^{(2)}$ is then

$$[\varphi_g]_B = \begin{bmatrix} \left[\varphi_g^{(1)}\right]_{B_1} & \\ & \left[\varphi_g^{(2)}\right]_{B_2} \end{bmatrix}.$$

Thus, it is seen that representations may be broken down into smaller representations which operate on invariant subspaces. The following definition arises naturally.

Definition 1.5 (Irreducible representation)**.** A non-zero representation $\varphi : G \to \mathrm{GL}(V)$ is said to be *irreducible* if the only G-invariant subspaces of V are 0 and V.

Note however that if a represenation is reducible, it need not actually have a decomposition of the form described in Proposition 1.4. We shall see an example of this later in

Example. Let G be a finite group with generators a and b, and suppose every element can be written as $a^i b^j$ for (non-negative) integers i, j. Since the inverse of any group element can be written as $a^i b^j$, it is seen that any group element can also be written as $b^{j'} a^{i'}$ for non-negative i', j' (let $i' = (|a| - 1)i$ and $j' = (|b| - 1)j$). So, assume that $n := |a| \leq |b|$.
We claim that any irreducible representation φ of G is of degree at most n. Let $\varphi : G \to \mathrm{GL}(V)$ be a representation. Let v be an eigenvector of φ_b and consider

$$W = \langle v, \varphi_a v, \varphi_{a^2} v, \ldots, \varphi_{a^{n-1}} v \rangle.$$

Clearly, $0 < \dim W \leq n$. If we manage to show that W is G-invariant, we are done since φ is irreducible so $V = W$ (in particular, $\dim V \leq n$).
Let $0 \leq k < n$ and consider some arbitrary $g = a^i b^j \in G$. Let $a^i b^j a^k = a^p b^q$. Then,

$$\begin{aligned}\varphi_{a^i b^j}(\varphi_{a^k} v) &= \varphi_{a^i b^j a^k} v \\ &= \varphi_{a^p} \varphi_{b^q} v \\ &= \varphi_{a^p} \lambda v && (v \text{ is an eigenvector of } \varphi_b \text{ and so } \varphi_{b^q}) \\ &= \lambda \varphi_{a^p} v \in W.\end{aligned}$$

In particular, any irreducible representation of the dihedral group D_n has degree at most two.

Proposition 1.5. Let $\rho : H \to \mathrm{GL}(V)$ be an irreducible representation and $\psi : G \to H$ be a surjective group homomorphism. Then, $\rho \circ \psi$ is an irreducible representation of G.

Proof. Let $\varphi = \rho \circ \psi$. Let W be a G-invariant subspace wrt φ. We shall show that it is also H-invariant wrt ρ to complete the proof. Indeed, for any $w \in W$ and $h \in H$, we have $h = \psi(g)$ for some $g \in G$. As a result,

$$\rho_h(w) = \rho_{\psi(g)}(w) = (\rho \circ \psi)_g(w) = \varphi_g(w) \in W.$$ ■

Proposition 1.6. If $\varphi : G \to \mathrm{GL}(V)$ is a degree two representation, φ is irreducible iff there is no common eigenvector v to all φ_g with $g \in G$.

Proof. If v is an eigenvector of all φ_g, then $\mathbb{C}v$ is a G-invariant subspace, so the forward direction is done.
Now, suppose that there is no common eigenvector v to all of the φ_g but there is a non-trivial G-invariant subspace W of V. Because it is a degree-two representation, $W = \mathbb{C}v$ for some $v \in V$. It follows that for each $g \in G$, $\varphi_g v = \lambda_g v$ (for some $\lambda_g \in \mathbb{C}$), so the desideratum follows. ■

Remark. The above result almost directly generalizes to degree three representations for *finite* groups as well. The key point to note is that if the representation of a finite group is reducible, then we can write $V = W \oplus W'$ for some non-zero G-invariant subspaces W, W'.
We shall prove this later in Proposition 1.15.

1.1.4. Decomposability

Definition 1.6 (Complete Reducibility)**.** Let G be a group. A representation $\varphi : G \to \mathrm{GL}(V)$ is said to be *completely reducible* if $V = V_1 \oplus \cdots \oplus V_n$ where each V_i is G-invariant and $\varphi|_{V_i}$ is irreducible for each i.

Equivalently, by Proposition 1.4, the above is equivalent to saying that $\varphi = \varphi^{(1)} \oplus \cdots \varphi^{(n)}$ for some irreducible representations $\varphi^{(i)}$.

Remark. Note that any irreducible representation is completely reducible. Indeed, the V_i need not be proper subspaces of V.

In some sense, complete reducibility says that we do not run into the weird situation wherein the representation is not irreducible yet we cannot "reduce" it to a direct sum of 'smaller' representations.
The main result of this section is showing that any representation of a finite group is completely reducible.
Based on the above remark, we can further define the more logical thing to consider as follows.

Definition 1.7 (Decomposability)**.** A non-zero representation φ is said to be *decomposable* if $V = V_1 \oplus V_2$ for some non-zero G-invariant subspaces $V_1, V_2 \leq V$. Otherwise, φ is said to be *indecomposable*.

First, let us show that irreducibility, complete reducibility, and decomposability are preserved under equivalence.

Lemma 1.7. Let $\varphi : G \to \mathrm{GL}(V)$ and $\psi : G \to \mathrm{GL}(W)$ be equivalent representations with $T : V \to W$ being a corresponding equivalence. If $V_1 \leq V$ is G-invariant, so is $W_1 = T(V_1)$.

Proof. Let $w \in W_1$ and $g \in G$. We have by definition that $\psi w = T\varphi T^{-1} w$. We have that $T^{-1}w \in V_1$, so since V_1 is G-invariant $\varphi T^{-1} w \in V_1$, so $T\varphi T^{-1} w \in W_1$ by definition of W_1. ■

Lemma 1.8. Let $\varphi : G \to \mathrm{GL}(V)$ and $\psi : G \to \mathrm{GL}(W)$ be equivalent representations. Then,

1. If φ is reducible, so is ψ.
2. If φ is decomposable, so is ψ.
3. If φ is completely reducible, so is ψ.

Proof. Let $T : V \to W$ be a corresponding equivalence.

1. Let $V_1 \leq V$ be a proper non-zero G-invariant subspace. Because T is an isomorphism, W_1 is also non-zero and proper. By the previous lemma, this is also G-invariant and we are done.
2. If $V = V_1 \oplus V_2$ for non-zero V_1, V_2, then $W = T(V_1) \oplus T(V_2)$ since T is an isomorphism. If V_1, V_2 are G-invariant, so are $T(V_1)$ and $T(V_2)$ by the previous lemma so we are done.
3. Again, if $V = V_1 \oplus \cdots \oplus V_n$, then $W = W_1 \oplus \cdots \oplus W_n$ where $W_i = T(V_i)$ and each V_i or W_i is G-invariant (with respect to the appropriate representation).
   We must check that if $\varphi|_{V_i}$ is irreducible, so is $\psi|_{W_i}$. However, this is direct as the following diagram commutes for all $g \in G$.

$$\begin{array}{ccc} V_i & \xrightarrow{\left(\varphi|_{V_i}\right)_g} & V_i \\ \downarrow{\scriptstyle T|_{V_i}} & & \downarrow{\scriptstyle T|_{V_i}} \\ W_i & \xrightarrow{\left(\psi|_{W_i}\right)_g} & W_i \end{array}$$

   It is easily seen that $T|_{V_i}$ is an isomorphism from V_i to W_i. ■

Proposition 1.9 (Irreducible representations of finite cyclic groups)**.** Let G be a finite cyclic group. Then all irreducible representations of G are of degree one.

Proof. We may assume that $G = \mathbb{Z}/n\mathbb{Z}$ by Lemma 1.8. Let $\varphi : G \to \mathrm{GL}_m(\mathbb{C})$ be a representation with $m \geq 2$.
Note that $\varphi_{\overline{1}}^n = I_n$. Recall Definition 0.5. It follows that the minimal polynomial of $\varphi_{\overline{1}}$ is a factor of $X^n - 1$, and in particular, has distinct roots. It follows from Theorem 0.8 that $\varphi_{\overline{1}}$ is diagonalisable.
Let D be a diagonal matrix and $T \in \mathrm{GL}_m(\mathbb{C})$ such that $T\varphi_{\overline{1}}T^{-1} = D$. Then $T\varphi_{\overline{k}}T^{-1} = D^k$ for any $1 \leq k \leq n$. Therefore, consider the equivalent representation $\psi : G \to \mathrm{GL}_m(\mathbb{C})$ defined by $\psi_g = T\varphi_g T^{-1}$. ψ_g is diagonal for all $g \in G$. Clearly, ψ is decomposable into m non-zero proper representations, contradicting irreducibility. ■

1.2. Maschke's Theorem and Complete Reducibility

The aim of this section is to show that any representation of a **finite** group is completely reducible in **??**.
To begin, we shall show that a representation of a **finite** group is decomposable iff it is reducible in Theorem 1.14. We first prove this for a specific type of representation in Lemma 1.10.

Definition 1.8 (Unitary)**.** Let V be an inner product space. A representation $\varphi : G \to \mathrm{GL}(V)$ is said to be *unitary* if φ_g is unitary for every $g \in G$.

That is, φ is a map from G to $U(V)$. Observe that unitarity depends on the inner product we place on the latent space! The usefulness arises when one observes certain properties of unitary representations (independent of the inner product), as we shall shortly see in Lemma 1.13.
Identifying $\mathrm{GL}_1(\mathbb{C})$ with $\mathbb{C}^*$, one sees that $U_1(\mathbb{C})$ ends up becoming S_1. Therefore, a degree-one unitary representation is a homomorphism $\varphi : G \to S^1$.
Recall that any degree-one representation of a finite group maps into S^1. Indeed, we have that $\varphi_g^{|G|} = 1$. Therefore, any such representation is unitary.

Example. $\varphi : \mathbb{R} \to S^1$ defined by $t \mapsto \exp(2\pi\iota t)$ is a degree-one unitary representation of $(\mathbb{R}, +)$.

Recall that decomposability implies reducibility, but the converse need not hold for a general representation.

Lemma 1.10. Let $\varphi : G \to \mathrm{GL}(V)$ be a unitary representation. Then, φ is decomposable iff it is not irreducible.

Proof. Suppose that φ is not irreducible. We shall show that it is decomposable. Let $W \leq V$ be a non-zero proper G-invariant subspace. We are done if we show that $W^\top$ is G-invariant as well. Let $g \in G$. We know that φ_g is unitary and W is φ_g-invariant. Recalling Proposition 0.6, $W^\perp$ is φ_g-invariant. Since g was arbitrary, $W^\perp$ is G-invariant with respect to φ, completing the proof. ■

As usual, we denote by $\langle \cdot, \cdot \rangle$ the standard inner product on $\mathbb{C}^n$.
Over the next three lemmas, we define a new inner product and show that any representation is equivalent to a unitary representation using this inner product.

Lemma 1.11. Let G be a finite group and $\rho : G \to \mathrm{GL}_n(\mathbb{C})$ a representation. Consider the product $(\cdot, \cdot)$ on $\mathbb{C}^n$ defined by

$$(v, w) = \sum_{g \in G} \langle \rho_g v, \rho_g w \rangle.$$

$(\cdot, \cdot)$ is an inner product.

Note that the sum is well-defined because G is finite.

Proof. Let $c_1, c_2 \in \mathbb{C}$ and $v_1, v_2, v, w \in \mathbb{C}$. Then,

$$\begin{aligned}
(c_1 v_1 + c_2 v_2, w) &= \sum_{g \in G} \langle \rho_g (c_1 v_1 + c_2 v_2), \rho_g w \rangle \\
&= \sum_{g \in G} \langle c_1 \rho_g v_1 + c_2 \rho_g v_2, \rho_g w \rangle \\
&= \sum_{g \in G} c_1 \langle \rho_g v_1, \rho_g w \rangle + c_2 \langle \rho_g v_2, w \rangle \\
&= c_1 (v_1, w) + c_2 (v_2, w).
\end{aligned}$$

Next,

$$\begin{aligned}
(w, v) &= \sum_{g \in G} \langle \rho_g w, \rho_g v \rangle \\
&= \sum_{g \in G} \overline{\langle \rho_g v, \rho_g w \rangle} \\
&= \overline{\sum_{g \in G} \langle \rho_g v, \rho_g w \rangle} = \overline{(v, w)}.
\end{aligned}$$

Finally,

$$(v,v) = \sum_{g\in G}(\rho_g v, \rho_g v) \geq 0.$$

with equality iff $\rho_g v = 0$ for every $g \in G$. In particular, $v = \rho_1 v = 0$. ■

Lemma 1.12. With the same notation as in the previous lemma, ρ is unitary with respect to the inner product $(\cdot,\cdot)$.

Proof. Let v, w and $g \in G$. We would like to show that $(\rho_g v, \rho_g w) = (v, w)$. Indeed,

$$\begin{aligned}(\rho_g v, \rho_g w) &= \sum_{g'\in G}\langle \rho_{g'}\rho_g v, \rho_{g'}\rho_g w\rangle \\ &= \sum_{g'\in G}\langle \rho_{g'g} v, \rho_{g'g} w\rangle \\ &= \sum_{g'\in G}\langle \rho_{g'} v, \rho_{g'} w\rangle && (g' \mapsto g'g \text{ is a bijection}) \\ &= (v,w). && \blacksquare\end{aligned}$$

Lemma 1.13. Every representation of a finite group G is equivalent to a unitary representation.

Proof. Let $\varphi : G \to \mathrm{GL}(V)$ be a representation and $n = \dim V$. Fix an isomorphism $T : V \to \mathbb{C}^n$ and set $\rho_g = T\varphi_g T^{-1}$ for each $g \in G$. Clearly, ρ is a representation $G \to \mathrm{GL}_n(\mathbb{C})$ that is equivalent to φ.
By Lemma 1.12, ρ is a unitary representation with respect to the inner product defined in Lemma 1.11 and we are done. ■

Theorem 1.14. Let $\varphi : G \to \mathrm{GL}(V)$ be a non-zero representation of a finite group. Then, φ is reducible iff it is decomposable.

Proof. The desideratum follows directly from lemmas 1.8, 1.10 and 1.13. ■

The above further shows that if $\varphi : G \to \mathrm{GL}(V)$ is a representation of a finite group G and V_1 is a non-zero proper G-invariant subspace, then we can decompose $V = V_1 \oplus V_2$, where V_2 is the subspace orthogonal to V_1 (for an appropriate inner product structure) and is also G-invariant (and non-zero and proper).

Proposition 1.15. Let $\varphi : G \to \mathrm{GL}(V)$ be a degree 3 representation of a finite group. φ is reducible iff there is a common vector v to all the φ_g for $g \in G$.

The proof of the above is exactly as described in the remark after Proposition 1.6. Reducibility implies decomposability, so we get a one-dimensional invariant subspace.
Now, let us give an example of an infinite group that is reducible but not decomposable.

Example. Let $\varphi : \mathbb{Z} \to \mathrm{GL}_2(\mathbb{C})$ be the representation defined by

$$\varphi_n = \begin{bmatrix} 1 & n \\ & 1 \end{bmatrix}.$$

φ is reducible because $\mathbb{C}e_1$ is a $\mathbb{Z}$-invariant subspace. However, there is no other eigenvector to all the φ_n, so there is no other $\mathbb{Z}$-invariant subspace. As a result, φ is not decomposable.
It is worth noting that Lemma 1.10 is true even for an infinite group, and Lemma 1.11 is where it breaks.

Further, the above cannot be strengthened to degree 4 representations since we need not have a 1-dimensional invariant subspace.

Example. Let $\psi : D_4 \to \mathrm{GL}_4(\mathbb{C})$ be defined by

$$\psi_r = \begin{bmatrix} \iota & & & \\ & -\iota & & \\ & & \iota & \\ & & & -\iota \end{bmatrix} \text{ and } \psi_s = \begin{bmatrix} & 1 & & \\ 1 & & & \\ & & & 1 \\ & & 1 & \end{bmatrix}.$$

It may be checked that ψ_r and ψ_s have no common eigenvector.

Now, we arrive at the main result of this section.

Theorem 1.16 (Maschke's Theorem)**.** Every representation of a finite group is completely reducible.

Proof. We prove this by induction on the degree of the representation $\varphi : G \to \mathrm{GL}(V)$.
If $\dim V = 1$, then φ is irreducible (so completely reducible) and we are done.
Let $n \geq 1$ and suppose that the statement is true for representations of degree $\leq n$. Let $\dim V = n + 1$. If φ is irreducible, we are done. Otherwise, by Theorem 1.14, $V = U \oplus W$ for non-zero G-invariant subspaces U, W. We may then apply the inductive hypothesis on U, W to write

$$U = U_1 \oplus \cdots \oplus U_n \text{ and } W = W_1 \oplus \cdots \oplus W_m$$

for non-zero G-invariant subspaces U_i and W_i such that $\varphi|_{U_i}$ and $\varphi|_{W_j}$ are irreducible for $1 \leq i \leq n$, $1 \leq j \leq m$. Consequently,

$$V = U_1 \oplus \cdots \oplus U_n \oplus W_1 \oplus \cdots \oplus W_m$$

and we are done. ∎

§2. Character Theory and Orthogonality Relations

2.1. Morphisms

Definition 2.1 (Morphism)**.** Let $\varphi : G \to \mathrm{GL}(V)$ and $\rho : G \to \mathrm{GL}(W)$ be representations. A *morphism* from φ to ρ is a linear map $T : V \to W$ such that the following diagram commutes for all $g \in G$.

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

The set of all morphisms from φ to ρ is denoted $\mathrm{Hom}_G(\varphi, \rho)$.

By definition, $\mathrm{Hom}_G(\varphi, \rho) \subseteq \mathrm{Hom}(V, W)$.

Recall that any representation is just a special group action of G on the vector space of interest. Based off this, writing gv instead of $\varphi_g v$, the definition of a morphism can be alternatively written as saying that $Tgv = gTv$ for all $g \in G, v \in V$.[2].
Also observe that if $T \in \mathrm{Hom}_G(\varphi, \rho)$ is an isomorphism, then $\varphi \sim \rho$.

Remark. $T \in \mathrm{Hom}(V, V)$ is in $\mathrm{Hom}_G(\varphi, \varphi)$ iff it commutes with every φ_g. In particular, the identity map is an element of $\mathrm{Hom}_G(\varphi, \varphi)$.

Proposition 2.1. Let $\varphi : G \to \mathrm{GL}(V)$ and $\rho : G \to \mathrm{GL}(W)$ be representations, and $T \in \mathrm{Hom}_G(\varphi, \rho)$. $\ker T$ and $\mathrm{im}\, T$ are G-invariant subspaces of V and W with respect to φ and ρ respectively.

Proof. Let $v \in \ker T$. Then, for $g \in G$,

$$T(\varphi_g v) = \rho_g T v = 0,$$

so $\varphi_g v \in \ker T$. Similarly, for $w \in \mathrm{im}\, T$, letting $v \in V$ such that $Tv = w$,

$$\rho_g w = \rho_g T v = T(\varphi_g v) \in \mathrm{im}\, T.$$

■

We had mentioned earlier that $\mathrm{Hom}_G(\varphi, \rho) \subseteq \mathrm{Hom}(V, W)$. In fact, the following stronger statement is true.

Proposition 2.2. Let G be a group and $\varphi : G \to \mathrm{GL}(V)$, $\rho : G \to \mathrm{GL}(W)$ be representations. Then $\mathrm{Hom}_G(\varphi, \rho)$ is a subspace of $\mathrm{Hom}(V, W)$.

Proof. Clearly, $0 \in \mathrm{Hom}_G(\varphi, \rho)$. If $S, T \in \mathrm{Hom}_G(\varphi, \rho)$ and $\alpha \in \mathbb{C}$, then for any $g \in G$ and $v \in V$,

$$\begin{aligned} (S + \alpha T)\varphi_g v &= S\varphi_g v + \alpha T \varphi_g v \\ &= \rho_g S v + \alpha \rho_g T v \\ &= \rho_g S v + \rho_g(\alpha T) v = \rho_g (S + \alpha T) v, \end{aligned}$$

so $S + \alpha T \in \mathrm{Hom}_G(\varphi, \rho)$. ■

[2] the first g is a φ_g and the second is a ρ_g

Another expected result is that the homomorphism subspaces of equivalent representations are isomorphic.

Proposition 2.3. Let G be a group and $\varphi_i : G \to \mathrm{GL}(V_i)$, $\rho_i : G \to \mathrm{GL}(W_i)$ be representations for $i = 1, 2$. If $\varphi^{(1)} \sim \varphi^{(2)}$ and $\rho^{(1)} \sim \rho^{(2)}$, then $\dim \mathrm{Hom}_G(\varphi^{(1)}, \rho^{(1)}) = \dim \mathrm{Hom}_G(\varphi^{(2)}, \rho^{(2)})$.

Proof. Let $P : V_1 \to V_2$ and $R : W_1 \to W_2$ be corresponding equivalences. Consider $\Phi : \mathrm{Hom}_G(\varphi^{(1)}, \rho^{(1)}) \to \mathrm{Hom}_G(\varphi^{(2)}, \rho^{(2)})$ defined by $\Phi(S) = R \circ S \circ P^{-1}$. We claim that Φ is an isomorphism between the subspaces. Let us first show that this does indeed map into $\mathrm{Hom}_G(\varphi^{(2)}, \rho^{(2)})$. We have that for any $g \in G$ and $v \in V_1$,

$$\begin{aligned}
\Phi(S)(\varphi^{(2)})_g v &= RSP^{-1}(\varphi^{(2)})_g v \\
&= RS(\varphi^{(1)})_g P^{-1} v && (P^{-1} \text{ is an equivalence}) \\
&= R(\rho^{(1)})_g SP^{-1} v && (S \in \mathrm{Hom}_G(\varphi^{(1)}, \rho^{(1)})) \\
&= (\rho^{(2)})_g RSP^{-1} v && (R \text{ is an equivalence}) \\
&= (\rho^{(2)})_g \Phi(S) v.
\end{aligned}$$

It is clear that Φ is linear, and further that Φ is a bijection as an inverse is easily constructed similarly. ■

Lemma 2.4 (Schur's Lemma)**.** Let G be a group, $\varphi : G \to \mathrm{GL}(V)$ and $\rho : G \to \mathrm{GL}(W)$ be irreducible representations of G, and $T \in \mathrm{Hom}_G(\varphi, \rho)$. Then, either T is an equivalence or $T = 0$.

Proof. Suppose that $T \neq 0$. It suffices to show that T is a bijection. If $\ker T \neq 0$, then we have a nonzero proper subspace $\ker T$ that is G-invariant (with respect to φ), contradicting irreducibility (of φ). Therefore, T is injective. Similarly, $\mathrm{im}\, T \neq 0$ and if $\mathrm{im}\, T \neq W$, we have a nonzero proper subspace $\mathrm{im}\, T$ that is G-invariant (with respect to ρ), contradicting irreducibility (of ρ). Therefore, T is surjective, completing the first part of the proof. ■

Corollary 2.5. Let G be a group, $\varphi : G \to \mathrm{GL}(V)$ and $\rho : G \to \mathrm{GL}(W)$ be irreducible representations of G, and $T \in \mathrm{Hom}_G(\varphi, \rho)$.

(a) If $\varphi \not\sim \rho$, then $\mathrm{Hom}_G(\varphi, \rho) = 0$.

(b) If $\varphi = \rho$, $T = \lambda I$ for some $\lambda \in \mathbb{C}$. That is, $\mathrm{Hom}_G(\varphi, \varphi)$ is one-dimensional with basis $\{I\}$.

Proof. (a) is immediate from Schur's Lemma.
For (b), let λ be an eigenvalue of T (which exists since $\mathbb{C}$ is algebraically closed). Recall that $I \in \mathrm{Hom}_G(\varphi, \varphi)$. It follows from Proposition 2.2 that $T - \lambda I \in \mathrm{Hom}_G(\varphi, \varphi)$. By the definition of an eigenvalue, $T - \lambda I$ is not invertible. Therefore, $T - \lambda I = 0$, proving the required. ■

Next, let us show that a direct sum of representations corresponds to a direct sum of their Homs as well.

Proposition 2.6. Let $\varphi : G \to \mathrm{GL}(V)$ and $\rho_i : G \to \mathrm{GL}(W_i)$ be representations for $i = 1, 2$. It is true that

$$\mathrm{Hom}_G(\varphi, \rho^{(1)} \oplus \rho^{(2)}) \cong \mathrm{Hom}_G(\varphi, \rho^{(1)}) \oplus \mathrm{Hom}_G(\varphi, \rho^{(2)}).$$

In particular,

$$\dim \mathrm{Hom}_G(\varphi, \rho^{(1)} \oplus \rho^{(2)}) = \dim \mathrm{Hom}_G(\varphi, \rho^{(1)}) + \dim \mathrm{Hom}_G(\varphi, \rho^{(2)}).$$

Proof. Let $T \in \mathrm{Hom}_G(\varphi, \rho^{(1)} \oplus \rho^{(2)}) \subseteq \mathrm{Hom}(V, W_1 \oplus W_2)$. Letting π_i denote the projection maps, $\pi_i \circ T : V \to W_i$ is linear for $i = 1, 2$. Further, $(\pi_i \circ T) \in \mathrm{Hom}_G(\varphi, \rho_i)$ because

$$(\pi_i \circ T)\varphi_g v = \pi_i(\rho^{(1)} \oplus \rho^{(2)})_g T v = (\rho_i)_g T v.$$

On the other hand, given morphisms $T_i \in \mathrm{Hom}_G(V, W_i)$ for $i = 1, 2$, $T : V \to W$ defined by $T(v) = (T_1(v), T_2(v))$ is also a morphism. As a result, the correspondence $(T_1, T_2) \mapsto T$ is bijective and $\mathbb{C}$-linear, so is an isomorphism. ■

Corollary 2.7. Let $\varphi^{(1)}, \ldots, \varphi^{(s)}$ be pairwise inequivalent irreducible representations of G. Set

$$\varphi = \underbrace{\varphi^{(1)} \oplus \cdots \oplus \varphi^{(1)}}_{m_1} \oplus \cdots \oplus \underbrace{\varphi^{(s)} \oplus \cdots \oplus \varphi^{(s)}}_{m_s}.$$

Then,

$$\dim \mathrm{Hom}_G(\varphi^{(r)}, \varphi) = m_r$$

for $1 \leq r \leq s$.

Proof. We have

$$\begin{aligned} \dim \mathrm{Hom}_G(\varphi^{(r)}, \varphi) &= \sum_{i=1}^{s} m_i \dim \mathrm{Hom}_G(\varphi^{(r)}, \varphi^{(i)}) && \text{(by Proposition 2.6)} \\ &= m_r && \text{(by Corollary 2.5)} \end{aligned}$$

■

The above says that if we know that a representation is completely reducible and we know the (pairwise inequivalent and irreducible) representations that occur in a decomposition, then the number of times each representation occurs is fixed as well.

Corollary 2.8. Let $\varphi^{(1)}, \ldots, \varphi^{(s)}$ and $\psi^{(1)}, \ldots, \psi^{(r)}$ be pairwise[3] inequivalent irreducible representations of G. Let φ be a representation of G such that

$$\varphi \cong \bigoplus_{i=1}^{s} (\varphi^{(i)})^{m_i} \cong \bigoplus_{j=1}^{r} (\psi^{(j)})^{n_j}$$

where $m_i, n_j > 0$. Then, $r = s$ and there is a permutation σ of $[r]$ such that $\varphi^{(i)} \sim \psi^{(\sigma_i)}$ and $m_i = n_{\sigma(i)}$.

Proof. It suffices to show that each φ_i is equivalent to some ψ_j. Indeed, pairwise inequivalence then implies that $r = s$, and the previous corollary shows that $m_i = n_j$. Suppose instead that $\varphi^{(1)}$ is not equivalent to any ψ_j. Then, denoting by $(psi^{(j)})^{n_j}$ the direct sum of n_j $\psi^{(j)}$s,

$$\begin{aligned} m_1 &= \mathrm{Hom}(\varphi^{(1)}, \varphi) \\ &= \mathrm{Hom}(\varphi^{(1)}, \bigoplus_{j=1}^{s} (\psi^{(j)})^{n_j}) \\ &= \sum_{j=1}^{s} n_j \mathrm{Hom}(\varphi^1, \psi^{(j)}) = 0, \end{aligned}$$

leading to a contradiction and completing the proof. ■

Compare this to Maschke's Theorem. There we had that any representation of a finite group is completely reducible. Here, we have shown that the decomposition of any completely reducible representation is "unique"!

Recall Proposition 1.9.

Theorem 2.9 (Irreducible representations of finite abelian groups)**.** Let G be an abelian group. Any irreducible representation of G has degree 1.

Proof. Let $\varphi : G \to \mathrm{GL}(V)$ be an irreducible representation.
For any $h \in G$, for all $g \in G$ $\varphi_h\varphi_g = \varphi_g\varphi_h$, so $\varphi_h \in \mathrm{Hom}_G(\varphi, \varphi)$. Corollary 2.5(b) then shows that $\varphi_h = \lambda_h I$ for some $\lambda_h \in \mathbb{C}$ (this uses that φ is irreducible). Fix any $v \in V$. Then, $\varphi_h v = \lambda_h I v = \lambda_h v \in \mathbb{C}v$, so $\mathbb{C}v$ is a G-invariant subspace. By irreducibility, $V = \mathbb{C}v$ and is thus one-dimensional. ■

Further recall that we had characterized the degree one representations of an abelian group in Corollary 1.3.

Corollary 2.10. Let G be a finite abelian group and $\varphi : G \to \mathrm{GL}_n(\mathbb{C})$ a representation. Then, there exists invertible T such that $T^{-1}\varphi_g T$ is diagonal for all $g \in G$.

Note that T is independent of g.

Proof. Since G is finite and abelian, we can write using Theorems 1.16 and 2.9 that

$$\varphi = \varphi^{(1)} \oplus \cdots \oplus \varphi^{(n)}$$

where each $\varphi^{(i)}$ is degree 1. If T is an isomorphism giving the above equivalence, then

$$T^{-1}\varphi_g T = \mathrm{diag}(\varphi_g^{(1)}, \ldots, \varphi_g^{(n)}).$$

■

Corollary 2.11. Let $A \in \mathrm{GL}_n(\mathbb{C})$ be of finite order. Then A is diagonalisable.

Proof. Consider the representation $\varphi : \mathbb{Z}/n\mathbb{Z} \to \mathrm{GL}_n(\mathbb{C})$ defined by $\overline{k} \mapsto A^k$. Corollary 2.10 implies that $\varphi_{\overline{1}} = A$ is diagonalisable (in fact, $I, A, \ldots, A^{n-1}$ are simultaneously diagonalisable). ■

2.2. The Orthogonality Relations

For the remainder of this report, assume that any group G is finite unless otherwise mentioned.

Definition 2.2. Let G be a group. Define the *group algebra* $L(G) \coloneqq \mathbb{C}^G$. $L(G)$ is a vector space over $\mathbb{C}$ in the natural sense. It is also an inner product space when equipped with the inner product

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

In particular, the *norm* of $f \in L(G)$ is $\|f\| = \sqrt{\langle f, f \rangle}$.

Note that the sum involved in $\langle f_1, f_2 \rangle$ makes sense because G is finite. Given a representation $\varphi : G \to \mathrm{GL}_n(\mathbb{C})$, we get n^2 elements $\varphi_{ij} : G \to \mathbb{C}$ corresponding to the n^2 entries of the matrix. We shall study φ_{ij} when φ is irreducible and unitary.

Proposition 2.12. Let $\varphi : G \to \mathrm{GL}(V)$ and $\rho : G \to \mathrm{GL}(W)$ be representations. Define for any linear transformation $T : V \to W$

$$T^\sharp = \frac{1}{|G|} \sum_{g \in G} \rho_{g^{-1}} T \varphi_g \in \mathrm{Hom}_G(\varphi, \rho).$$

Then,

(a) $T^\sharp \in \mathrm{Hom}_G(\varphi, \rho)$,

(b) if $T \in \mathrm{Hom}_G(\varphi, \rho)$, then $T^\sharp = T$, and

(c) the map $P : \mathrm{Hom}_{\mathbb{C}}(V, W) \to \mathrm{Hom}_G(\varphi, \rho)$ defined by $T \mapsto T^\sharp$ is a surjective linear map.

Proof.

1. For any $h \in H$,

$$\begin{aligned} T^\sharp \varphi_h &= \frac{1}{|G|} \sum_{g \in G} \rho_{g^{-1}} T \varphi_g \varphi_h \\ &= \frac{1}{|G|} \sum_{g \in G} \rho_{g^{-1}} T \varphi_{gh} \\ &= \frac{1}{|G|} \sum_{g' \in G} \rho_{hg'^{-1}} T \varphi_{g'} && (g \mapsto gh \text{ defines a bijection } G \to G) \\ &= \rho_h \frac{1}{|G|} \sum_{g' \in G} \rho_{g'^{-1}} T \varphi_{g'} = \rho_h T^\sharp. \end{aligned}$$

2. If $T \in \mathrm{Hom}_G(\varphi, \rho)$, then

$$\begin{aligned} T^\sharp &= \frac{1}{|G|} \sum_{g \in G} \rho_{g^{-1}} T \varphi_g \\ &= \frac{1}{|G|} \sum_{g \in G} \rho_{g^{-1}} \rho_g T \\ &= \frac{1}{|G|} \sum_{g \in G} T = T. \end{aligned}$$

3. (b) shows that P is surjective. For linearity, we have that for any $T_1, T_2 \in \mathrm{Hom}_{\mathbb{C}}(V, W)$ and $c \in \mathbb{C}$,

$$\begin{aligned} P(cT_1 + T_2) &= \frac{1}{|G|} \sum_{g \in G} \rho_{g^{-1}} (cT_1 + T_2) \varphi_g \\ &= c \frac{1}{|G|} \sum_{g \in G} \rho_{g^{-1}} T_1 \varphi_g + \frac{1}{|G|} \sum_{g \in G} \rho_{g^{-1}} T_2 \varphi_g \\ &= cP(T_1) + P(T_2). \end{aligned}$$

■

Proposition 2.13. Let $\varphi : G \to \mathrm{GL}(V)$ and $\rho : G \to \mathrm{GL}(W)$ be irreducible representations and let $T : V \to W$ be a linear map. Then,

(a) if $\varphi \not\sim \rho$, $T^\sharp = 0$ and

(b) if $\varphi = \rho$, $T^\sharp = \frac{\mathrm{Tr}\, T}{\deg \varphi} I$.

Proof.

(a) This is straightforward on an application of Schur's Lemma since $T^\sharp \in \mathrm{Hom}_G(\varphi, \rho)$.

(b) Again, by Schur's Lemma, we have that $T^\sharp = \lambda I$ for some $\lambda I \in \mathbb{C}$. Now, note that

$$\mathrm{Tr}\, T^\sharp = \mathrm{Tr}(\lambda I) = \lambda \deg \varphi.$$

We also have

$$\begin{aligned}
\mathrm{Tr}\, T^\sharp &= \mathrm{Tr}\left(\frac{1}{|G|}\sum_{g\in G} \varphi_{g^{-1}} T \varphi_g\right) \\
&= \frac{1}{|G|}\sum_{g\in G} \mathrm{Tr}\left(\varphi_{g^{-1}} T \varphi_g\right) \\
&= \frac{1}{|G|}\sum_{g\in G} \mathrm{Tr}\left(\varphi_{g^{-1}} \varphi_g T\right) && (\mathrm{Tr}(ABC) = \mathrm{Tr}(ACB)) \\
&= \mathrm{Tr}\, T,
\end{aligned}$$

so the required follows.

■

Suppose that $V = \mathbb{C}^n$ and $W = \mathbb{C}^m$. P is then a linear form from $\mathrm{GL}(V, W) = M_{m\times n}(\mathbb{C})$ to itself. A natural question to ask is: how do we represent P as a matrix with respect to the standard basis vectors E_{ij}? (Recall that E_{ij} is the $m \times n$ matrix with 1 in the (i, j)th entry and 0 elsewhere)
It is a straightforward computational task to check that if $A = (a_{ij}) \in M_{r\times m}(\mathbb{C})$, $E_{ki} \in M_{m\times n}(\mathbb{C})$, and $B = (b_{ij}) \in M_{n\times s}(\mathbb{C})$, then

$$(AE_{ki}B)_{lj} = a_{lk}b_{ij}. \tag{2.1}$$

Lemma 2.14. Let $\varphi : G \to U_n(\mathbb{C})$ and $\rho : G \to U_m(\mathbb{C})$ be unitary representations of G. Let $A = E_{ki} \in M_{m\times n}(\mathbb{C})$. Then,

$$A^\sharp_{lj} = \langle \varphi_{ij}, \rho_{kl} \rangle.$$

Proof. Let $g \in G$. Because ρ_g is unitary, $\rho_{g^{-1}} = \rho_g^*$. As a result, $(\rho_{g^{-1}})_{lk} = \overline{(\rho_g)_{kl}}$. Consequently,

$$\begin{aligned}
(A^\sharp)_{lj} &= \frac{1}{|G|}\sum_{g\in G} (\rho_{g^{-1}} A \varphi_g)_{lj} \\
&= \frac{1}{|G|}\sum_{g\in G} (\rho_{g^{-1}})_{lk} (\varphi_g)_{ij} \\
&= \frac{1}{|G|}\sum_{g\in G} \overline{(\rho_g)_{kl}} (\varphi_g)_{ij} \\
&= \langle \varphi_{ij}, \rho_{kl} \rangle.
\end{aligned}$$

■

Theorem 2.15 (Schur's Orthogonality Relations)**.** Let $\varphi : G \to U_n(\mathbb{C})$ and $\rho : G \to U_m(\mathbb{C})$ be inequivalent irreducible unitary representations of a group G. Then,

(a) $\langle \varphi_{ij}, \rho_{kl} \rangle = 0$.

(b) $\langle \varphi_{ij}, \varphi_{kl} \rangle = \begin{cases} 1/n, & (i,j) = (k,l), \\ 0, & \text{otherwise.} \end{cases}$

In particular, the set $\{\varphi_{ij} : 1 \leq i, j \leq n\} \cup \{\rho_{kl} : 1 \leq k, l \leq m\}$ is a linearly independent set.

Proof.

(a) Let $A = E_{ki} \in M_{m \times n}(\mathbb{C})$. By Proposition 2.13, $A^\sharp = 0$ because $\varphi \not\sim \rho$, so in particular, using Lemma 2.14, $\langle \varphi_{ij}, \rho_{kl} \rangle = (A^\sharp)_{lj} = 0$.

(b) Let $A = E_{ki} \in M_{n \times n}(\mathbb{C})$. By Proposition 2.13, $A^\sharp = \frac{\operatorname{Tr} A}{n} I$. $\operatorname{Tr} A$ is 1 if $k = i$ and 0 otherwise. We also have $\langle \varphi_{ij}, \rho_{kl} \rangle = \left(\frac{\operatorname{Tr} A}{n} I \right)_{lj}$, which is zero if $l \neq j$. That is, the quantity of interest is equal to $1/n$ if $k = i$ and $l = j$ and 0 otherwise. ■

Corollary 2.16. Let φ be an irreducible unitary representation of G of degree n. The set $\{\sqrt{n}\varphi_{ij} : 1 \leq i, j \leq n\}$ of functions forms an orthonormal set.

Proposition 2.17. Let G be a (finite) group. The following are true.

(a) There are finitely many equivalence classes of irreducible representations of G.

(b) Let $\varphi^{(1)}, \ldots, \varphi^{(s)}$ be a transversal of unitary representatives of irreducible representations of G. Set $d_i = \deg \varphi^{(i)}$. Then, the set of functions

$$\{\sqrt{d_k}\varphi_{ij}^{(k)} : 1 \leq k \leq s, 1 \leq i, j \leq d_k\}$$

is orthonormal.

Proof.

(a) By Lemma 1.13, any equivalence class of representations (any class of irreducible representations in particular) contains a unitary representation. As $\dim L(G) = |G|$, no linearly independent set of vectors in $L(G)$ can contain more than $|G|$ elements. Because orthonormal sets are linearly independent, Corollary 2.16 and theorem 2.15(a) show that there can only be finitely many classes of irreducible representations.

(b) This again directly follows from Corollary 2.16 and theorem 2.15(a).

■

In particular, using the same notation as the above proposition, we have that

$$s \leq d_1^2 + d_2^2 + \cdots + d_s^2 \leq |G|. \tag{2.2}$$

Indeed, the lower bound is obvious as each $d_i \geq 1$. For the upper bound, each representation of degree d_k corresponds to d_k^2 many orthonormal functions, so the overall set of representations corresponds to $\sum d_i^2$ orthonormal functions, which can be at most $\dim L(G) = |G|$. This also says that the degree of any irreducible representation is at most $\sqrt{|G|}$.
In fact, we shall see later that it is *exactly* $|G|$.

2.3. Characters and Class Functions

Recall the remark after Corollary 2.8, which said that the decomposition given by Maschke's Theorem is unique. In this section, we shall prove a stronger version of the same (explicitly finding the number of irreducible representations), arriving at some interesting results along the way.
Given an endomorphism of a finite dimensional vector space, we can talk about its trace, which is just the trace of any matrix representation after fixing an ordered basis. It is not too difficult to see that this trace is basis-invariant. We extensively use this fact in this section, namely that $\operatorname{Tr}(ABC) = \operatorname{Tr}(ACB)$ so if $C = A^{-1}$ then $\operatorname{Tr}(ABA^{-1}) = \operatorname{Tr}(B)$.

Definition 2.3 (Character)**.** Let $\varphi : G \to \mathrm{GL}(V)$ be a representation. The *character* $\chi_\varphi : G \to \mathbb{C}$ of φ is defined by $\chi_\varphi(g) = \operatorname{Tr} \varphi_g$. The character of an irreducible representation is called an *irreducible character*.

As mentioned, the character does not depend on the basis we choose, so we may assume that we are talking about matrix representations. If $\varphi : G \to \mathrm{GL}_n(\mathbb{C})$ is a representation given by $\varphi_g = ((\varphi_g)_{ij})$, $\chi_\varphi(g) = \sum_{i=1}^n (\varphi_g)_{ii}$.

Occasionally, we cut out the explicit writing of the representation and directly refer to characters of a group. The degree of this character is just the degree of the corresponding representation.

Remark. If $z : G \to \mathbb{C}^* \hookrightarrow \mathbb{C}$ is a degree 1 representation, then $\chi_z = z$. Henceforth, we treat degree 1 representations and their characters as the same.

Proposition 2.18. If $\varphi : G \to \mathrm{GL}(V)$ is a representation, $\chi_\varphi(1) = \deg \varphi = \dim V$.

Proof. Indeed, $\varphi_1 = \mathrm{Id}_V$ so $\chi_\varphi(1) = \operatorname{Tr} \varphi_1 = \operatorname{Tr} \mathrm{Id}_V = \dim V = \deg \varphi$. ∎

Proposition 2.19. If φ and ρ are equivalent representations, $\chi_\varphi = \chi_\rho$.

Proof. We may assume that $\varphi, \rho : G \to \mathrm{GL}_n(\mathbb{C})$. If $T \in \mathrm{GL}_n(\mathbb{C})$ is an invertible matrix such that $\varphi_g = T\rho_g T^{-1}$ for all $g \in G$, then

$$\chi_\varphi(g) = \operatorname{Tr} \varphi_g = \operatorname{Tr}(T\rho_g T^{-1}) = \operatorname{Tr} \rho_g = \chi_\rho(g).$$ ∎

Corollary 2.20. Let G be a group of order n and χ a character of degree m of G. Then, $\chi(g)$ is a sum of m nth roots of unity for each $g \in G$.

Proof. Because characters are invariant under equivalence, let us assume that the representation is of the form $\varphi : G \to \mathrm{GL}_m(\mathbb{C})$. Fix $g \in G$. Then, $\varphi_g^n = I$ so φ_g is diagonalisable by Corollary 2.11. So, we may assume that φ_g is diagonal. It has eigenvalues $(\lambda_i)_{i=1}^m$, where each λ_i is an nth root of unity. The desideratum follows. ∎

A proof similar to Proposition 2.19 also shows the following.

Proposition 2.21. Let χ be a character of G. Then, χ is constant on conjugacy classes of G.

Proof. Let $g, h \in G$ and φ be a representation corresponding to χ. Then,

$$\begin{aligned}\chi(g) &= \operatorname{Tr} \varphi_g \\ &= \operatorname{Tr}(\varphi_{h^{-1}} \varphi_g \varphi_h) \\ &= \operatorname{Tr} \varphi_{h^{-1}gh} = \chi(h^{-1}gh).\end{aligned}$$ ∎

Functions such as these have a name of their own.

Definition 2.4 (Class function)**.** A function $f : G \to \mathbb{C}$ is said to be a *class function* if $f(g) = f(h^{-1}gh)$ for all $g, h \in G$. The set of all class functions is denoted $Z(L(G))$.

Given a conjugacy class $C \subseteq G$ and a class function f, we denote by $f(C)$ the constant value taken by f on C.

Proposition 2.22. $Z(L(G))$ is a subspace of $L(G)$.

We omit the proof of the above as it is very straightforward.

Definition 2.5. Given a group G, the set of conjugacy classes of G is denoted $\mathrm{Cl}(G)$. For $C \in \mathrm{Cl}(G)$, we define $\delta_C : G \to \mathbb{C}$ by

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

That is, δ_C is the indicator function of C.

Proposition 2.23. The set $B = \{\delta_C : C \in \mathrm{Cl}(G)\}$ is a basis of $Z(L(G))$. In particular, $\dim Z(L(G)) = |\mathrm{Cl}(G)|$.

Proof. It is clear that $\delta_C \in \mathrm{Cl}(G)$ for each $C \in \mathrm{Cl}(G)$.
To show that B spans $Z(L(G))$, note that for any $f \in Z(L(G))$,

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

This is easily checked by computing both sides at an arbitrary $g \in G$.
To show linear independence on the other hand, we have for $C, C' \in \mathrm{Cl}(G)$

$$\langle \delta_C, \delta_{C'} \rangle = \sum_{g \in G} \delta_C(g)\overline{\delta_{C'}(g)} = \begin{cases} 0, & C \neq C', \\ \frac{|C|}{|G|}, & C = C' \end{cases}$$

and any set of orthogonal nonzero vectors is linearly independent.
The desideratum follows. ∎

Theorem 2.24. Let φ, ρ be irreducible representations of G. Then

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

Thus, the set of irreducible characters of G forms an orthonormal set of class functions.

Proof. By Lemma 1.13 and proposition 2.19, we may assume that $\varphi : G \to U_n(\mathbb{C})$ and $\rho : G \to U_m(\mathbb{C})$. We have

$$\begin{aligned} \langle \chi_\varphi, \chi_\rho \rangle &= \frac{1}{|G|} \sum_{g \in G} \chi_\varphi(g)\overline{\chi_\rho(g)} \\ &= \frac{1}{|G|} \sum_{g \in G} \left(\sum_{1 \le i \le n} \varphi_{ii}(g) \right) \overline{\left(\sum_{1 \le j \le m} \rho_{jj}(g) \right)} \\ &= \sum_{\substack{1 \le i \le n \\ 1 \le j \le m}} \frac{1}{|G|} \sum_{g \in G} \varphi_{ii}(g)\overline{\rho_{jj}(g)} \\ &= \sum_{\substack{1 \le i \le n \\ 1 \le j \le m}} \langle \varphi_{ii}, \rho_{jj} \rangle. \end{aligned}$$

Recall Schur's Orthogonality Relations. If $\varphi \not\sim \rho$, then it immediately follows that the above quantity of interest is 0. If $\varphi \sim \rho$ on the other hand, we may assume that $\varphi = \rho$ by Proposition 2.19. We then again have by Schur's orthogonality relations that the summand is nonzero only when $i = j$, and in this case it is just equal to $1/n$. The overall sum is then $n \cdot 1/n = 1$, completing the proof. ■

Corollary 2.25. Given two inequivalent irreducible representations φ, ρ of G, $\chi_\varphi \neq \chi_\rho$.

Proof. We have $\langle \chi_\varphi, \chi_\rho \rangle = 0$, but if $\chi_\varphi = \chi_\rho$ we also have $\langle \chi_\varphi, \chi_\varphi \rangle = 1$. ■

Corollary 2.26. Two irreducible representations are equivalent if and only if they have the same character.

In Corollary 2.29, we shall see that the above holds in more generality.

Consequently, there are at most $|\mathrm{Cl}(G)|$ equivalence classes of irreducible representations.

Definition 2.6. If V is a vector, φ is a representation, and $m \in \mathbb{N}$, then

$$mV = \underbrace{V \oplus \cdots \oplus V}_{m} \text{ and } m\varphi = \underbrace{\varphi \oplus \cdots \oplus \varphi}_{m}.$$

$0V$ is the zero vector space and 0φ is the degree zero representation.

Now, we would like to show the uniqueness of decomposition, just as we did in Corollary 2.8. Indeed, this is easier now since we have a finite number of irreducible representations. Suppose we are given a transerversal $\varphi^{(1)}, \ldots, \varphi^{(s)}$ of irreducible representations, and let

$$\varphi \sim m_1\varphi^{(1)} \oplus m_2 \cdots \oplus m_s\varphi^{(s)}.$$

Lemma 2.27. Let $\varphi = \rho \oplus \psi$. Then $\chi_\varphi = \chi_\rho + \chi_\psi$.

Proof. We may suppose that $\rho : G \to \mathrm{GL}_n(\mathbb{C})$ and $\psi : G \to \mathrm{GL}_m(\mathbb{C})$. The block matrix form of $\varphi : G \to \mathrm{GL}_{n+m}(\mathbb{C})$ can then be written as

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

and the required immediately follows. ■

As an immediate consequence of the above lemma and Theorem 2.24, we get the following.

Theorem 2.28. Suppose we are given a transerversal $\varphi^{(1)}, \ldots, \varphi^{(s)}$ of irreducible representations, and let φ be a representation such that

$$\varphi \sim m_1\varphi^{(1)} \oplus m_2 \cdots \oplus m_s\varphi^{(s)}.$$

Then, $m_i = \langle \chi_\varphi, \chi_{\varphi^{(i)}}$.

That is, as we saw earlier, the decomposition of φ into irreducible representations is "unique".

Corollary 2.29. φ is determined up to equivalence by its character.

The above follows quite directly from the fact that the decomposition is unique.

Corollary 2.30.

1. $\|\chi\|^2 \in \mathbb{N}$, and $\|\chi\| = 1$ iff χ is irreducible.
2. $\langle \chi_1, \chi_2 \rangle \in \mathbb{N}_0$. Note that the characters themslves need not necessarily be real-valued.

To see this, note that if

$$\rho_1 \sim m_1\varphi^{(1)} \oplus \cdots \oplus m_s\varphi^{(s)}$$

and

$$\rho_2 \sim n_1\varphi^{(1)} \oplus \cdots \oplus n_s\varphi^{(s)},$$

then $\langle \chi_{\rho_1}, \chi_{\rho_2} \rangle = \sum_i m_i n_i$.

Corollary 2.31. Let $z : G \to \mathbb{C}^*$ be a degree one representation and $\rho : G \to \mathrm{GL}_n(\mathbb{C})$ be a representation. Consider $\varphi : G \to \mathrm{GL}_n(\mathbb{C})$ defined by $\varphi_g = z_g\rho_g$. Then,

(a) φ is a representation,

(b) $\chi_\varphi = z\chi_\rho$ and $\|\chi_\varphi\| = \|\chi_\rho\|$,

(c) φ is irreducible iff ρ is, and

(d) if there exists $g_0 \in G$ such that $z_{g_0} \neq 1$ and $\chi_\varphi(g_0) \neq 0$, then $\rho \not\sim \varphi$.

Proof.

(a) This is direct as $z_{g_1}\rho_{g_2} = \rho_{g_2}z_{g_1}$.

(b) We have $\chi_\varphi(g) = \mathrm{Tr}(\varphi_g) = \mathrm{Tr}(z_g\rho_g) = z_g \,\mathrm{Tr}(\rho_g)$, so $\chi_\varphi = (z\chi_\rho)(g)$.
Because G is finite, we have $z_g^{|G|} = 1$, and so $|z_g| = 1$. Consequently, $\|\chi_\varphi(g)\| = \|z_g\chi_\rho(g)\| = \|\chi_\rho(g)\|$. As a result, $\|\chi_\varphi\| = \|\chi_\rho\|$ as well.

(c) Since φ (resp. ρ) is irreducible iff $\|\chi_\varphi\|$ (resp. $\|\chi_\rho\|$) is 1, we are done.

(d) This follows from Corollary 2.29 since in this case, $\chi_\varphi(g_0) \neq \chi_\rho(g_0)$.

■

Definition 2.7. Let G be a finite group and $\varphi^{(1)}, \ldots, \varphi^{(s)}$ be a transversal of irreducible unitary representations of G. If $\rho \sim m_1\varphi^{(1)} \oplus \cdots \oplus m_s\varphi^{(s)}$, then m_i is said to be the *multiplicity* of $\varphi^{(i)}$ in ρ. If $m_i > 0$, $\varphi^{(i)}$ is said to be an *irreducible constituent* of ρ.

Using the notation of the above definition, $\deg \rho = \sum m_i \deg \varphi^{(i)}$.
Letting $m_i = \langle \chi_\rho, \chi_{\varphi^{(i)}} \rangle$, we have

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

2.4. The Regular Representation

Recall linearisation.

Definition 2.8 (Regular representation)**.** Let G be a finite group. The *regular representation* of G is the homomorphism $L : G \to \mathrm{GL}(\mathbb{C}G)$ defined by

$$L_g\left(\sum_{h\in G} c_h h\right) = \sum_{h\in G} c_h gh = \sum_{x\in G} c_{g^{-1}x} x$$

for $g \in G$.

The above representation can be understood very simply on noting that given a standard basis vector $h \in G$ of $\mathbb{C}G$, $L_g h$ is just gh, that is, it permutes the basis vectors. It acts on arbitrary elements by extending this map linearly to $\mathbb{C}G$. This may be used to check that the regular representation is indeed a representation.
Clearly, $\deg L = |G|$. As a result, by Equation (2.2), L is *not* irreducible.

Proposition 2.32. The regular representation is a unitary representation of G.

Proof. Fix $g \in G$. We have

$$\begin{aligned}\left\langle L_g \sum_{h\in G} c_h h, L_g \sum_{h\in G} d_h h\right\rangle &= \left\langle \sum_{h\in G} c_{g^{-1}h} h, \sum_{h\in G} d_{g^{-1}h} h\right\rangle \\ &= \sum_{h\in G} c_{g^{-1}h} d_{g^{-1}h} \\ &= \sum_{h\in G} c_h d_h = \left\langle \sum_{h\in G} c_h h, \sum_{h\in G} d_h h\right\rangle.\end{aligned}$$

■

Proposition 2.33. The character of the regular representation L is given by

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

Proof. By Proposition 2.18, $\chi_L(1) = |G|$. Let $g \neq 1$ and fix an ordering $(g_1, \ldots, g_n)$ of $|G|$. We claim that all the diagonal entries of the matrix representation $[L_g]$ of L_g with respect to this basis are 0. Indeed, for any g_i, $gg_i \neq g_i$, so the ith entry of the ith column is 0. It follows that $\chi_L(g) = \mathrm{Tr}[L_G] = 0$. ■

The above can be used in conjunction with Corollary 2.30 to give an alternate proof that L is not irreducible.
For the remainder of this subsection, fix a finite group G, $\varphi^{(1)}, \ldots, \varphi^{(s)}$ as a transversal of irreducible unitary representations of G, $d_i = \deg \varphi^{(i)}$, and let $\chi_i = \chi_{\varphi^{(i)}}$.

We shall now show that the second inequality is in fact an equality in Equation (2.2).

Theorem 2.34. Let L denote the regular representation of G. Then,

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

In particular,

$$|G| = \sum d_i^2.$$

Proof. It suffices to show that $\langle \chi_L, \chi_i \rangle = d_i$. Indeed, this is immediate as

$$\langle \chi_L, \chi_i \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_L(g)\overline{\chi_i(g)} = \frac{1}{|G|}\chi_L(1)\chi_i(1) = d_i.$$

■

Using Proposition 2.17, we get the following.

Corollary 2.35. The set $B = \{\sqrt{d_k}\varphi_{ij}^{(k)} : 1 \leq k \leq s, 1 \leq i, j \leq d_k\}$ is an orthonormal basis of $L(G)$.

Proposition 2.36. The set $B = \{\chi_1, \ldots, \chi_s\}$ is an orthonormal basis of $Z(L(G))$.

Proof. Assume that $\varphi^{(i)} : G \to U_{d_i}(\mathbb{C})$.
Recall by Theorem 2.24 that B is an orthonormal set. We are done if we show that it is a basis. Let $f \in Z(L(G)) \leq L(G)$. By Corollary 2.35, we have constants $c_{ij}^{(k)} \in \mathbb{C}$ such that

$$f = \sum c_{ij}^{(k)} \varphi_{ij}^{(k)}.$$

Let $x \in G$. We have

$$\begin{aligned}
f(x) &= \frac{1}{|G|}\sum_{g\in G} f(g^{-1}xg) && (f \in Z(L(G))) \\
&= \frac{1}{|G|}\sum_{g\in G}\sum_{i,j,k} c_{ij}^{(k)}\varphi_{ij}^{(k)}(g^{-1}xg) \\
&= \sum_{i,j,k} c_{ij}^{(k)}\frac{1}{|G|}\sum_{g\in G}\varphi_{ij}^{(k)}(g^{-1}xg) \\
&= \sum_{i,j,k} c_{ij}^{(k)}\left[\frac{1}{|G|}\sum_{g\in G}\varphi^{(k)}(g^{-1})\varphi^{(k)}(x)\varphi^{(k)}(g)\right]_{ij} \\
&= \sum_{i,j,k} c_{ij}^{(k)}\left[\left(\varphi^{(k)}(x)\right)^{\sharp}\right]_{ij} && \text{(recall Proposition 2.12)} \\
&= \sum_{i,j,k} c_{ij}^{(k)}\frac{\operatorname{Tr}\varphi^{(k)}(x)}{d_k} I_{ij} && \text{(recall Proposition 2.13)} \\
&= \sum_{i,k} \frac{c_{ii}^{(k)}}{d_k}\chi_k(x) \\
&= \sum_{k}\left(\sum_{i}\frac{c_{ii}^{(k)}}{d_k}\right)\chi_k(x),
\end{aligned}$$

so B is a basis and we are done. ■

Now use Proposition 2.23 to get the following.

Corollary 2.37. There are precisely $|\operatorname{Cl}(G)|$ equivalence classes of irreducible representations of a group G.

Recall that $|\operatorname{Cl}(G)| = |G|$ iff G is abelian.

Corollary 2.38. G has $|G|$ equivalence classes of irreducible representations iff G is abelian.

In the above scenario, we have $|G| = d_1^2 + \cdots + d_{|G|}^2$, so we get the following.

Corollary 2.39. G is abelian iff all its irreducible representations have degree one.

Definition 2.9. Let G be a finite group with irreducible characters $\chi_1, \ldots, \chi_s$ and conjugacy classes $C_1, \ldots, C_s$. The *character table* of G is the $s \times s$ matrix X with $\mathsf{X}_{ij} = \chi_i(C_j)$.

The above table is square because of Corollary 2.37.

Proposition 2.40. Let C, C' be conjugacy classes of G and $g \in C, h \in C'$. Then,

$$\sum_{i=1}^{s} \chi_i(g)\overline{\chi_i(h)} = \begin{cases} |G|/|C|, & C = C', \\ 0, & \text{otherwise.} \end{cases}$$

Consequently, the columns of the character table are orthogonal, and it is invertible.

Proof. Recall Proposition 2.36 and also that $\delta_{C'} \in Z(L(G))$. So,

$$\delta_{C'} = \sum_{i=1}^{s} \langle \delta_{C'}, \chi_i \rangle \chi_i.$$

So,

$$\begin{aligned} \delta_{C'}(g) &= \sum_{i=1}^{s} \frac{1}{|G|} \sum_{x \in G} \delta_{C'}(x)\overline{\chi_i(x)}\chi_i(g) \\ &= \frac{1}{|G|} \sum_{i=1}^{s} \sum_{x \in C'} \overline{\chi_i(x)}\chi_i(g) \\ &= \frac{|C'|}{|G|} \sum_{i=1}^{s} \overline{\chi_i(h)}\chi_i(g) && (\chi_i \text{ is a class function}) \\ \sum_{i=1}^{s} \overline{\chi_i(h)}\chi_i(g) &= \frac{|G|}{|C'|}\delta_{C'}(g). \end{aligned}$$

The desideratum follows. ∎

2.5. Representations of abelian groups

We conclude this section by completing our discussion of representations of abelian groups. For this subsection, let G be an abelian group.
By Proposition 1.9 and corollary 2.38, we know that the $|G|$ degree one representations of G are precisely the irreducible representations of G.
Recall from Proposition 0.2 that we know all of these representations when $G = \mathbb{Z}/n\mathbb{Z}$. By the structure theorem of finite abelian groups, we get a complete description of the irreducible representations of G for any abelian group in general using the following lemma.

Lemma 2.41. Let G_1, G_2 be finite abelian groups. with $m = |G_1|$ and $n = |G_2|$. Suppose that $\rho_1, \ldots, \rho_m$ and $\varphi_1, \ldots, \varphi_n$ are all the irreducible representations of G_1 and G_2 respectively. The functions $\alpha_{ij} : G_1 \times G_2 \to \mathbb{C}$ for $1 \leq i \leq m$ and $1 \leq j \leq n$ defined by

$$\alpha_{ij}(g_1, g_2) = \rho_i(g_1)\varphi_j(g_2)$$

form a complete set of irreducible representations of G.

Proof. Note that $\alpha_{ij}(g, 1) = \rho_i(g)$ and $\alpha_{ij}(1, g) = \varphi_j(g)$. This gives that all the α_{ij} are distinct as α_{ij} and α_{kl} are identical iff ρ_i and ρ_k are identical and φ_j and φ_l are identical.
Further, because each α_{ij} is degree-one, it suffices to show that each α_{ij} is a homomorphism. This is immediate as

by commutativity,

$$\begin{aligned}\alpha_{ij}((g_1,g_2)(g_1',g_2')) &= \alpha_{ij}(g_1g_1',g_2g_2')\\ &= \varphi_i(g_1g_1')\rho_j(g_2g_2')\\ &= \varphi_i(g_1)\varphi_i(g_1')\rho_j(g_2)\rho_j(g_2')\\ &= \varphi_i(g_1)\rho_j(g_2)\varphi_i(g_1')\rho_j(g_2') = \alpha_{ij}(g_1,g_2)\alpha_{ij}(g_1',g_2').\end{aligned}$$ ■

Further observe that because degree-one representations are the same as their characters, the above can be used quite easily to get the character table of the product.

2.6. The Dimension Theorem

Recall the previous section where we showed that a given group G has only finitely many irreducible representations. In this section, we shall show that the degree of any irreducible representation divides the order of the group. Also recall algebraic integers (Definition 0.8).

Proposition 2.42. Let χ be a character of G. Then, $\chi(g)$ is an algebraic integer for all $g \in G$.

Proof. Recall that any root of unity is an algebraic integer. The required then follows on using Corollary 2.20 and proposition 0.11. ■

For the remainder of this section, let G be a finite group with conjugacy classes $\{C_i\}_{i=1}^s$ with $C_1 = \{1\}$. For $i \in [s]$, let $h_i = |C_i|$. Let $\varphi : G \to \mathrm{GL}(V)$ denote a degree d representation and $\chi_i = \chi_\varphi(C_i)$. Finally, let $T_i = \sum_{x\in C_i} \varphi_x$.

Lemma 2.43. If φ is irreducible, $T_i = \frac{h_i}{d}\chi_i \cdot I$.

Proof. First, for any $g \in G$,

$$\varphi_g T_i \varphi_{g^{-1}} = \varphi_g \left(\sum_{x\in C_i} \varphi_x\right) \varphi_{g^{-1}} = \sum_{x\in C_i} \varphi_{gxg^{-1}} = \sum_{y\in C_i} \varphi_y = T_i,$$

so $T_i \in \mathrm{Hom}(\varphi,\varphi)$. By Corollary 2.5, $T_i = \lambda I$ for some $\lambda \in \mathbb{C}$. Now,

$$\lambda = \frac{1}{d}\operatorname{Tr} T_i = \frac{1}{d}\sum_{x\in C_i} \operatorname{Tr}\varphi_x = \frac{1}{d}\sum_{x\in C_i}\chi_i = \frac{h_i}{d}\chi_i,$$

completing the proof. ■

Lemma 2.44. $T_i \circ T_j = \sum_{k=1}^s a_{ijk}T_k$ for some $\{a_{ijk}\}_{1\le i,j,k\le s} \subseteq \mathbb{Z}$.

Note that φ is not assumed to be irreducible in this lemma.

Proof. First,

$$T_i \circ T_j = \left(\sum_{x\in C_i}\varphi_x\right)\circ\left(\sum_{y\in C_j}\varphi_y\right) = \sum_{\substack{x\in C_i\\ y\in C_j}} \varphi_{xy} = \sum_{g\in G} a_{ijg}\varphi_g,$$

where $a_{ijg} = |\{(x,y) \in C_i \times C_j : xy = g\}|$. Let X_{ijg} be this set. Suppose that $g_1, g_2 \in C_k$, and let $g_2 = kg_1k^{-1}$. Observe then that the function $X_{ijg_1} \to X_{ijg_2}$ defined by $(x,y) \mapsto (kxk^{-1}, kyk^{-1})$ is a bijection. Indeed, it has inverse $(x,y) \mapsto (k^{-1}xk, k^{-1}yk)$. So, $a_{ijg_1} = a_{ijg_2}$. Letting the value of a_{ijg} for $g \in C_k$ be a_{ijk}, we get

$$T_i \circ T_j = \sum_{g \in G} a_{ijg}\varphi_g = \sum_{k=1}^{s} \sum_{g \in C_k} a_{ijk}\varphi_g = \sum_{k=1}^{s} a_{ijk}T_k.$$

■

Combining the two lemmas, we get the following.

Corollary 2.45. For some $\{a_{ijk}\}_{1 \le i,j,k \le s} \subseteq \mathbb{Z}$,

$$\left(\frac{h_i}{d}\chi_i\right)\left(\frac{h_j}{d}\chi_j\right) = \sum_{k=1}^{s} a_{ijk}\frac{h_k}{d}\chi_k.$$

Lemma 2.46. If φ is irreducible, $h_i\chi_i/d_i$ is an algebraic integer for every i.

Proof. Using the previous corollary, it is not too difficult to come up with an appropriate integer matrix in the context of Proposition 0.10. ■

Theorem 2.47 (Dimension Theorem)**.** Let φ be an irreducible degree d representation of G. Then, d divides $|G|$.

Proof. By Theorem 2.24, $\langle \chi_\varphi, \chi_\varphi \rangle = 1$. So,

$$\frac{|G|}{d} = \frac{|G|}{d} \cdot \frac{1}{|G|} \sum_{g \in G} \chi_\varphi(g)\overline{\chi_\varphi(g)} = \sum_{g \in G} \frac{\chi_\varphi(g)}{d}\overline{\chi_\varphi(g)} = \sum_{i=1}^{s} \sum_{g \in C_i} \frac{\chi_\varphi(g)}{d}\overline{\chi_\varphi(g)} = \sum_{i=1}^{s} \left(\frac{h_i\chi_i}{d}\right)\overline{\chi_i}.$$

Note that $h_i\chi_i/d$ is an algebraic integer by Lemma 2.46, and $\overline{\chi_i}$ is an algebraic integer by Proposition 2.42 (recall that $\mathbb{A}$ is closed under conjugation). By Proposition 0.11, $|G|/d$ is an algebraic integer too. However, this is rational, so the desideratum follows from Proposition 0.9. ■

Corollary 2.48. Let p, q be primes with $p \le q$ and $q \not\equiv 1 \pmod{p}$. Then, any group G of order pq is abelian. In particular, so are groups of order p^2.

Proof. Let $d_1, \ldots, d_s$ be the degrees of the irreducible representations of G. We shall show that $d_i = 1$ for all i, then use Corollary 2.39. Let us assume without loss of generality that $d_1 = 1$. We have

$$pq = 1 + d_2^2 + \cdots + d_s^2.$$

By the Dimension Theorem, $d_i \in \{1, p, q, pq\}$ for all i. In fact, because $p \le q$, $d_i \in \{1, p\}$. Let m be the number of representations of degree 1 and n that of degree p. We have $pq = m + np^2$. So, $p \mid m$. Let $m = pm'$. We have $q = m' + np$. By Corollary 1.2, $m \mid pq$, so $m' \mid q$. As a result, $m' \in \{1, q\}$. However, m' cannot be 1 because that with the previous equation would contradict the fact that $q \not\equiv 1 \pmod{p}$. Therefore, $m' = q$ and $m = pq$, completing the proof. ■

Recall that the above is a basic fact from group theory which is typically proved using the Sylow theorems.

Porism 2.49. Let G be a group of order pq for primes $p < q$. Then, all irreducible representations of G have degree either 1 or p. Moreover, G has an irreducible representation of degree p iff it is non-abelian.

Noting that $m = |G/[G, G]|$ and $p \mid m$ in the proof of the previous corollary, we get the following.

Porism 2.50. Let G be a group of order pq for primes $p < q$. Then, $|[G, G]| \in \{1, q\}$. Moreover, $|[G, G]| = q$ iff G is non-abelian.

As before, this can be proved using elementary group theory as well. We leave the details of this as an exercise to the reader.

§3. Fourier Analysis on Finite Groups

3.1. Basic definitions

3.1.1. Introduction

Definition 3.1. Let $n \in \mathbb{N}$. A function $f : \mathbb{Z} \to \mathbb{C}$ is said to be *periodic* with *period* n iff $f(x+n) = f(x)$ for all $x \in \mathbb{Z}$.

Note that the period of a given function is not unique.
It is not difficult to check that the set of functions periodic with period n is in bijection with $L(\mathbb{Z}/n\mathbb{Z})$, the set of complex-valued functions on $\mathbb{Z}/n\mathbb{Z}$. Also recall that $L(\mathbb{Z}/n\mathbb{Z})$ has orthonormal basis $\{\chi_k : 0 \leq k < n\}$, where $\chi_k(\overline{m}) = \omega_m^{nk}$, so for $f \in L(\mathbb{Z}/n\mathbb{Z})$,

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

Definition 3.2 (Fourier transform on $\mathbb{Z}/n\mathbb{Z}$)**.** Let $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}$. The *Fourier transform* $\mathcal{F}(f) = \hat{f} : \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}$ of f is defined by

$$\hat{f}(\overline{m}) = \sum_{k=0}^{n} f(\overline{k})e^{-2\pi\iota mk/n} = \sum_{k=0}^{n} f(\overline{k})\omega_n^{-mk}.$$

By the definition of the inner product,

$$\hat{f}(\overline{m}) = n\langle f, \chi_m\rangle. \tag{3.1}$$

Note that $\mathcal{F} : L(\mathbb{Z}/n\mathbb{Z}) \to L(\mathbb{Z}/n\mathbb{Z})$ is linear.

Proposition 3.1. The Fourier transform is invertible. More precisely,

$$f = \frac{1}{n}\sum_{k=1}^{n-1} \hat{f}(\overline{k})\chi_k.$$

This is immediate since Equation (3.1) gives that $\langle f, \chi_k\rangle = \hat{f}(\overline{k})/n$.

3.1.2. The convolution product

Definition 3.3 (Convolution)**.** Let G be a group and $a, b \in L(G)$. Then, the *convolution* $a * b \in L(G)$ of a with b is defined by

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

This is well-defined because G is finite.

Changing y to xz^{-1} above, we get

$$(a * b)(x) = \sum_{z\in G} b(xz^{-1})a(xzx^{-1}).$$

As a result, if a is a class function, $(a * b) = (b * a)$. In particular, if G is abelian, $(a * b) = (b * a)$ for all $a, b \in L(G)$. In fact, the converse holds as well, as we shall see shortly.
Similar to how we defined δ_C earlier, we define the following.

Definition 3.4. Let G be a group. For $g \in G$, define $\delta_g : G \to \mathbb{C}$ by

$$\delta_g(x) = \begin{cases} 1, & g = x, \\ 0, & \text{otherwise.} \end{cases}$$

We omit the proofs of the next three lemmas, as they are very easy to check.

Proposition 3.2. Let G be a group and $g, h \in G$. Then, $\delta_g * \delta_h = \delta_{gh}$.

If G is not abelian, then the above shows that $*$ is not commutative. Indeed, for $g, h \in G$ such that $gh \neq hg$, $\delta_g * \delta_h \neq \delta_h * \delta_g$.

Proposition 3.3. Let $a \in L(G)$ and $g, h \in G$. Then, $(a * \delta_h)(g) = a(gh^{-1})$ and $(\delta_h * a)(g) = a(h^{-1}g)$.

Proposition 3.4. For all $a, b, c \in L(G)$,

1. $a * \delta_1 = \delta_1 * a$,
2. $a * (b * c) = (a * b) * c$, and
3. $a * (b + c) = (a * b) + (a * c)$.

That is, $(L(G), +, *)$ is a ring with multiplicative identity δ_1.

$L(G)$ is a commutative ring iff G is commutative. This also justifies why we earlier called $L(G)$ the group algebra. Also note that the map $i : G \to L(G)$ defined by $g \mapsto \delta_g$ is a group homomorphism into the group $(L(G))^\times$ of units. Recall Definition 0.7.

Proposition 3.5. $a : G \to \mathbb{C}$ is a class function iff a is in the center of $L(G)$.

This explains why we denoted the set of class functions as $Z(L(G))$ earlier!

Proof. We already saw earlier that if a is a class function, it commutes with all of $L(G)$.
On the other hand, let a be in the center of $L(G)$ and let $g, h \in G$. Then, by Proposition 3.3,

$$a(gh) = (a * \delta_{h^{-1}})(g) = (\delta_{h^{-1}} * a)(g) = a(hg).$$

Setting g as xy^{-1} and h as y then shows that a is a class function, completing the proof. ∎

3.2. Fourier analysis on finite groups

Recall the dual group of a group from Definition 0.1. In the case where G is finite and abelian, the elements of $\hat{G}$ are precisely the irreducible characters of G. Earlier, we had defined the Fourier transform for only groups of the form $\mathbb{Z}/n\mathbb{Z}$. Now, we shall extend it more generally to abelian groups, as a function $\mathcal{F} : L(G) \to L(\hat{G})$. Also recall from Theorem 0.3 that $G \cong \hat{G}$.

Definition 3.5 (Fourier transform on abelian groups)**.** Let G be a finite abelian group and $f \in L(G)$ a function. The *Fourier transform* $\mathcal{F}(f) = \hat{f} \in L(\hat{G})$ is defined by

$$\hat{f}(\chi) = |G|\langle f, \chi \rangle = \sum_{g \in G} f(g)\overline{\chi(g)}.$$

The complex numbers $|G|\langle f, \chi \rangle$ are called the *Fourier coefficients* of f.

For the case where $G = \mathbb{Z}/n\mathbb{Z}$, an example of an isomorphism $G \to \hat{G}$ is given by $\overline{k} \mapsto \chi_{\overline{k}}$, where $\chi_{\overline{k}}$ is defined by $\chi_{\overline{k}}(\overline{m}) = \omega_n^{mk}$. It is then easy to see that this Fourier transform does correspond with that we gave earlier.

Since any irreducible character $\chi \in L(G)$, it makes sense to talk about the Fourier transform of a character (this takes irreducible characters as input). Using Theorem 2.24, we then have for any irreducible character $\theta \in L(G)$,

$$\hat{\chi}(\theta) = |G|\langle \chi, \theta \rangle = \begin{cases} |G|, & \theta = \chi, \\ 0, & \text{otherwise.} \end{cases}$$

That is, $\hat{\chi} = |G|\delta_\chi$.

Again, as before, the Fourier transform is invertible.

Lemma 3.6 (Fourier inversion)**.** Let G be an abelian group. $\mathcal{F} : L(G) \to L(\hat{G})$ is injective. In particular, if $f \in L(G)$,

$$f = \frac{1}{|G|} \sum_{\chi \in \hat{G}} \hat{f}(\chi)\chi.$$

Proof. We have

$$f = \sum_{\chi \in \hat{G}} \langle f, \chi \rangle \chi = \frac{1}{|G|} \sum_{\chi \in \hat{G}} |G| \langle f, \chi \rangle \chi = \frac{1}{|G|} \sum_{\chi \in \hat{G}} \hat{f}(\chi)\chi. \qquad \blacksquare$$

Proposition 3.7. $\mathcal{F} : L(G) \to L(\hat{G})$ is an isomorphism of vector spaces.

Proof. For $f_1, f_2 \in L(G)$, $\alpha \in \mathbb{C}$, and $\chi \in \hat{G}$,

$$\mathcal{F}(\alpha f_1 + f_2)(\chi) = |G|\langle \alpha f_1 + f_2, \chi \rangle = |G|\alpha \langle f_1, \chi \rangle + |G| \langle f_2, \chi \rangle = \alpha \mathcal{F}(f_1)(\chi) + \mathcal{F}(f_2)(\chi).$$

Since $\mathcal{F}$ is injective, linear, and $\dim L(G) = \dim L(\hat{G}) = |G|$, $\mathcal{F}$ is an isomorphism. $\blacksquare$

We would also like $\mathcal{F}$ to be an isomorphism of rings. However, the convolution product on $L(\hat{G})$ does not work out for this, and we must use the point-wise product $\cdot$ instead. Clearly, this makes $L(\hat{G})$ a commutative ring with identity as the constant map $g \mapsto 1$. $L(G)$ is also commutative in this case, but with identity δ_1.

Theorem 3.8. Let G be an abelian group and $a, b \in L(G)$. The Fourier transform satisfies

$$\widehat{a * b} = \hat{a} \cdot \hat{b}.$$

As a result, $\mathcal{F} : L(G) \to L(\hat{G})$ is an isomorphism between the rings $(L(G), +, *)$ and $(L(\hat{G}), +, \cdot)$.

Proof. Let $\chi \in \hat{G}$. Then,

$$\begin{aligned}\widehat{a * b}(\chi) &= \sum_{x\in G}(a*b)(x)\overline{\chi(x)} \\ &= \sum_{x\in G}\left(\sum_{y\in G} a(xy^{-1})b(y)\right)\overline{\chi(x)} \\ &= \sum_{y\in G} b(y)\sum_{x\in G} a(xy^{-1})\overline{\chi(x)} \\ &= \sum_{y\in G} b(y)\sum_{z\in G} a(z)\overline{\chi(zy)} \\ &= \sum_{y\in G} b(y)\overline{\chi(y)}\sum_{z\in G} a(z)\overline{\chi(z)} = \hat{a}(\chi)\cdot\hat{b}(\chi).\end{aligned}$$

■

For the remainder of this subsection, we discuss an application of Fourier analysis in graph theory.
Recall the definition of a(n undirected) graph and its adjacency matrix.

Definition 3.6 (Cayley Graph)**.** Let G be a finite group written in some fixed order. A subset $S \subseteq G$ is said to be *symmetric* if

1. $1 \notin S$ and
2. $s \in S \implies s^{-1} \in S$.

If S is a symmetric subset of G, the *Cayley graph* of G with respect to S is the graph with vertex set G and edge $\{g, h\}$ iff $gh^{-1} \in S$.

Note that the above definition makes sense because $gh^{-1} \in S$ iff $hg^{-1} \in S$.
Whenever $G = \mathbb{Z}/n\mathbb{Z}$, we assume this "fixed order" to be $\{\overline{0}, \ldots, \overline{n-1}\}$.

Definition 3.7. A Cayley graph of $\mathbb{Z}/n\mathbb{Z}$ (with respect to any symmetric set) is called a *circulant graph* (on n vertices).

Definition 3.8. A matrix $A = (a_{ij})$ is said to be *circulant* if there exists a function $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}$ such that $a_{ij} = f(\overline{j}-\overline{i})$.

Equivalently, a circulant matrix is of the form

$$\begin{bmatrix} a_0 & a_1 & \cdots & a_{n-2} & a_{n-1} \\ a_{n-1} & a_0 & \cdots & a_{n-3} & a_{n-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_2 & a_3 & \cdots & a_0 & a_1 \\ a_1 & a_2 & \cdots & a_{n-1} & a_0 \end{bmatrix}.$$

It is not too difficult to verify that for any symmetric subset S of $G = \mathbb{Z}/n\mathbb{Z}$, the circulant matrix corresponding to $f = \delta_S$ is the adjacency matrix of the Cayley graph of G with respect to S.

Lemma 3.9. Let G be an abelian group and $a \in L(G)$. Define $A : L(G) \to L(G)$ by $A(b) = a * b$. Then, A is linear and χ an eigenvector of A with eigenvalue $\hat{a}(\chi)$ for all $\chi \in \hat{G}$. Consequently, A is diagonalisable.

Proof. Linearity is easily checked and we omit the proof.
Let $\chi \in \hat{G}$ be arbitrary. Then,

$$\widehat{a * \chi} = \hat{a}\cdot\hat{\chi} = |G|\hat{a}\cdot\delta_\chi = |G|\hat{a}(\chi)\delta_\chi.$$

By Lemma 3.6,

$$A(\chi) = a * \chi = \hat{a}(\chi)\chi,$$

and χ is an eigenvector of A with eigenvalue $\hat{a}(\chi)$.
Because G is abelian, $Z(L(G)) = L(G)$ and $\hat{G}$, a basis of $Z(L(G))$, is constituted of precisely the irreducible characters of G. As a result, $\hat{G}$ is an eigenbasis of $Z(L(G))$ and A is diagonalisable. ■

Theorem 3.10. Let $G = \{g_1, \ldots, g_n\}$ be an ordered abelian group, $S \subseteq G$ a symmetric set, $\chi_1, \ldots, \chi_n$ the irreducible characters of G, and A the adjacency matrix of the Cayley graph of G with respect to S. Then,

(a) The eigenvalues of A are

$$\lambda_i = \sum_{s \in S} \chi_i(s)$$

for $1 \leq i \leq n$.

(b) A corresponding orthonormal basis of eigenvectors is given by

$$v_i = \frac{1}{\sqrt{|G|}} \begin{bmatrix} \chi_i(g_1) & \cdots & \chi_i(g_n) \end{bmatrix}^\top.$$

Note that given the above, the λ_i must be symmetric as A is symmetric.

Proof. Define $F : L(G) \to L(G)$ by $F(b) = \delta_S * b = \sum_{x \in S} b(x)$. We shall analyze the eigenvalues and eigenvectors of F, and finally show that A is the matrix representation of F with respect to another ordered basis.
By Lemma 3.9, F has eigenvectors χ_i with corresponding eigenvalue

$$\hat{\delta}_S(\chi_i) = |G|\langle \delta_S, \chi_i \rangle = \sum_{x \in S} \overline{\chi_i(x)} = \sum_{x \in S} \chi_i(x^{-1}) = \sum_{y \in S} \chi_i(y) = \lambda_i.$$

Consider $B = (\delta_{g_1}, \ldots, \delta_{g_n})$ of $L(G)$, and let $[F]_B$ denote the matrix of F with respect to this ordered basis. The coordinate vector of χ_i with respect to B is precisely $\sqrt{|G|}v_i$, and the above argument shows that it is an eigenvector with eigenvalue λ_i. The orthonormality of the (v_i) follows from Theorem 2.24.
It suffices to show that $A = [F]_B$. Let $1 \leq i, j \leq n$. $([F]_B)_{ij}$ is the coefficient of δ_{g_i} in $F(g_j)$, which is

$$([F]_B)_{ij} = F(\delta_{g_j})(g_i) = (\delta_S * \delta_{g_j})(g_i) = \delta_S(g_i g_j^{-1})$$

by Proposition 3.3. This is precisely A_{ij}, completing the proof. ■

Corollary 3.11. Let A be a $n \times n$ circulant matrix, which is the adjacency matrix of the Cayley graph of $G = \mathbb{Z}/n\mathbb{Z}$ with respect to some symmetric $S \subseteq G$. Then, the eigenvalues of A are

$$\lambda_k = \sum_{\overline{m} \in S} \omega_n^{km}$$

for $k = 0, \ldots, n-1$ with a corresponding orthonormal eigenbasis given by

$$v_k = \frac{1}{\sqrt{n}} \begin{bmatrix} 1 & \omega_n^k & \omega_n^{2k} & \cdots & \omega_n^{(n-1)k} \end{bmatrix}.$$

3.3. Fourier analysis on non-abelian groups

The issue in non-abelian groups is that $Z(L(G)) \neq L(G)$, and a pointwise product of functions remains commutative. As a result, we cannot have a Fourier transform converting convolution to a pointwise product while staying an isomorphism. To remedy this, we shall look at matrix multiplication instead of pointwise multiplication.

Before going to this, let us look at abelian groups in a different light. Recall that $\mathbb{C}^n$ is a ring with product given by

$$(w_1, \dots, w_n) \cdot (z_1, \dots, z_n) = (w_1 z_1, \dots, w_n z_n).$$

Proposition 3.12. Let G be a finite abelian group with irreducible characters $\chi_1, \dots, \chi_n$. Define $T : L(G) \to \mathbb{C}^n$ by

$$Tf = (\hat{f}(\chi_1), \dots, \hat{f}(\chi_n)).$$

Then, T is an isomorphism of rings.

Proof. Similar to the proof of Proposition 3.7, T is an isomorphism of vector spaces, so we only need to show that for $f, g \in L(G)$, $T(f * g) = Tf \cdot Tg$. This however, follows directly from the fact that $\widehat{f * g}(\chi_i) = \hat{f}(\chi_i) \cdot \hat{g}(\chi_i)$. ∎

Theorem 3.13. Let G be a finite abelian group of order n. Then, $L(G) \cong \mathbb{C}^n$ as rings.

The above says that

$$\mathbb{C}^n \cong \underbrace{M_1(\mathbb{C}) \times \cdots \times M_1(\mathbb{C})}_{n \text{ copies}}.$$

In general, we replace the 1s with the degrees of the irreducible representations (recall that all irreducible representations of abelian groups are degree one).

For the rest of this subsection, let G be a finite group of order n, and $\varphi^{(1)}, \dots, \varphi^{(s)}$ a transversal of irreducible unitary representations of G. Set $d_k = \deg \varphi^{(k)}$.
Let $D = \{(i, j, k) : 1 \leq k \leq s, 1 \leq i, j \leq d_k\}$. Finally, let $B = \{\sqrt{d_k}\varphi_{ij}^{(k)} : (i, j, k) \in D\}$. Recall from Proposition 2.17 that B is an orthonormal basis of $L(G)$.

Definition 3.9 (Fourier transform)**.** Define $\mathcal{F} : L(G) \to M_{d_1}(\mathbb{C}) \times \cdots M_{d_s}(\mathbb{C})$ by $\mathcal{F}(f) = (\hat{f}(\varphi^{(1)}), \dots, \hat{f}(\varphi^{(s)}))$, where

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

$\mathcal{F}(f)$ is said to be the *Fourier transform* of f.

That is, $\hat{f}(\varphi^{(k)})$ is just a matrix with

$$\left(\hat{f}(\varphi^{(k)})\right)_{ij} = \hat{f}(\varphi_{ij}^{(k)}). \tag{3.2}$$

Note that $\dim L(G) = |G|$, and $\dim(M_{d_1}(\mathbb{C}) \times \cdots \times M_{d_s}(\mathbb{C})) = d_1^2 + \cdots + d_s^2 = |G|$. We shall show that $\mathcal{F}$ is an isomorphism.

Lemma 3.14. Let $f \in L(G)$. Then,

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

In particular, $\mathcal{F}$ is injective.

Proof. Because B is an orthonormal basis, it suffices to show that

$$\langle f, \sqrt{d_k}\varphi_{ij}^{(k)} \rangle = \frac{1}{n} \sqrt{d_k} \hat{f}(\varphi^{(k)})_{ij},$$

which is just Equation (3.2). ■

Lemma 3.15. $\mathcal{F}$ is an isomorphism of vector spaces.

Proof. As usual, checking linearity is easy. $\mathcal{F}$ is injective by Lemma 3.14. We also saw earlier that the dimensions of $L(G)$ and $M_{d_1}(\mathbb{C}) \times \cdots \times M_{d_s}(\mathbb{C})$ are equal, so we are done. ■

$M_{d_1}(\mathbb{C}) \times \cdots \times M_{d_s}(\mathbb{C})$ is a ring as well, with the coordinate-wise product.

Theorem 3.16 (Wedderburn's Theorem)**.** The Fourier transform is an isomorphism of rings.

Proof. Let $a, b \in L(G)$. All we need to show is that $\widehat{a,b} = \hat{a} \cdot \hat{b}$. Since the latter product is coordinate-wise, this is equivalent to showing that $\widehat{a * b}(\varphi^{(k)}) = \hat{a}(\varphi^{(k)}) \cdot \hat{b}(\varphi^{(k)})$ for all $1 \leq k \leq s$ (the product on the right is matrix multiplication). The proof is very similar to that of Theorem 3.8:

$$\begin{aligned}
\widehat{a * b}(\varphi^{(k)}) &= \sum_{g \in G} (a * b)(g) \overline{\varphi^{(k)}(g)} \\
&= \sum_{g,h \in G} a(gh^{-1}) b(h) \overline{\varphi^{(k)}(g)} \\
&= \sum_{h \in G} b(h) \sum_{g \in G} a(gh^{-1}) \overline{\varphi^{(k)}(g)} && (a, b \text{ commute because they take values in } \mathbb{C}) \\
&= \sum_{h \in G} b(h) \sum_{g \in G} a(g) \overline{\varphi^{(k)}(gh)} \\
&= \sum_{h \in G} b(h) \sum_{g \in G} a(g) \overline{\varphi^{(k)}(g)} \cdot \overline{\varphi^{(k)}(h)} \\
&= \left(\sum_{g \in G} a(g) \overline{\varphi^{(k)}(g)} \right) \cdot \left(\sum_{h \in G} b(h) \overline{\varphi^{(k)}(h)} \right) = \hat{a}(\varphi^{(k)}) \cdot \hat{b}(\varphi^{(k)}).
\end{aligned}$$

■