MATH-314: Representation Theory of Finite Groups

Sidharth Hariharan

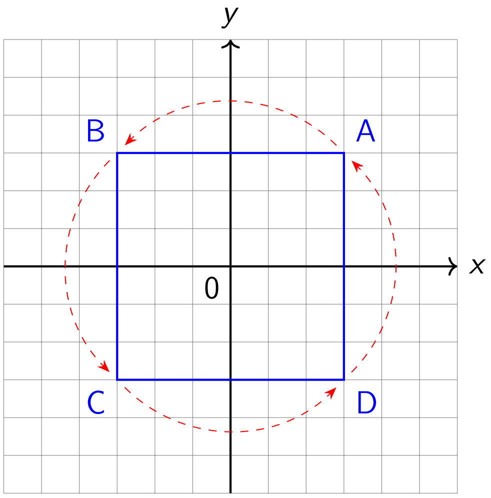
École Polytechnique Fédérale de Lausanne - Spring 2024

Contents

Chapter 1

An Introduction to the Theory of Representations of Groups

As I understand it, the fundamental idea behind Representation Theory is to study the actions of groups on vector spaces. While arbitrary vector spaces over arbitrary fields might not have naturally visualisable geometric properties, representations of groups in the ones that do can greatly illustrate the nature of these groups, especially to individuals like myself who delight in (somewhat literally) *seeing* mathematics come alive.



A key motivating example in the study of representation theory would be the representations of Dihedral groups over $\mathbb{R}^2$. It is very natural to (at least informally) view the Dihedral group D_n of order $2n$ as the group of symmetries of the regular n-gon; in other words, elements of D_n have natural actions on a regular n-gon that preserve its structure. For instance, D_4 contains an element that rotates a square clockwise by 90°, an action under which the square is, of course, invariant.

If one were to now plot this square in $\mathbb{R}^2$, then action of the same element on the square can be extended to an orthogonal transformation of $\mathbb{R}^2$ that maps the x-axis to the y-axis and vice-versa, but in a manner preserving orientation (ie, that *rotates the plane clockwise by* 90°). In a similar fashion, one can extend the actions of all dihedral groups D_n to actions on the entirety of $\mathbb{R}^2$. More precisely, to every element of a dihedral group, one can ascribe a specific *matrix* that transforms $\mathbb{R}^2$ in a manner preserving the regular n-gon.

This motivates the formal definition of a representation.

1.1 Important Definitions

1.1.1 What is a Representation?

It turns out that representations can be defined quite broadly, sidestepping the geometric niceties (or are they constraints?) of Euclidean spaces.

Definition 1.1.1 (Group Representation). Let G be a group. A representation of G is a pair (V, ρ) of a vector space V and a group homomorphism $\rho : G \to \mathrm{GL}(V)$.

Here, $\mathrm{GL}(V)$ refers to the **G**eneral **L**inear group over V, consisting of all vector space automorphisms of V equipped with the binary operation of composition.

Definition 1.1.2 (Degree of a Representation). Let G be a group and let (V, ρ) be a representation of G. We define the degree of V to be the dimension of V over its base field.

There exist innumerable examples of representations throughout mathematics. Below, we give some important ones.

Example 1.1.3 (Important Classes of Representations).

1. The trivial representation. Let G be a group and V be any vector space. The map $\rho : G \to \mathrm{GL}(V) : g \mapsto \mathrm{id}_V$ is a representation.
2. The zero representation. Let G be a group and let $V = \{0\}$ be the zero vector space over an arbitrary field K. The trivial representation over V is known as the zero representation.

3. The sign representation. Let $G = S_n$, the symmetric group on n elements, and let $V = K$, a field. Then, $\mathrm{GL}(V) = K^\times$, the multiplicative group of K. Denoting by ξ the canonical map from $\mathbb{Z}$ to K, the map

$$\rho : G \to \mathrm{GL}(V) : \sigma \mapsto \xi(\mathrm{sgn}(\sigma))$$

is a representation, where $\mathrm{sgn} : G \to \{-1, 1\}$ denotes the sign homomorphism.

4. Permutation representations. Let G be a group acting on a finite set X, and let $V = K[X]$, the free vector space (over some field K) generated by X. Consider a K-basis $\{e_x \in V : x \in X\}$ of V. Then, the map $\rho : G \to \mathrm{GL}(V)$ given by

$$\rho(g)(e_x) = e_{g(x)}$$

is a representation.

5. The regular representation. Let G be a *finite* group. The permutation representation corresponding to the canonical action of G on itself by left-multiplication gives a representation of G over $K[G]$, the free vector space generated by G (as a set) over any field K.

Non-Example 1.1.4. Let G be a group and let V be a nonzero vector space over an arbitrary field. The map $g \mapsto 0 : G \to (V \to V)$ is not a representation because the zero map $0 : V \to V$ is not invertible.

A useful perspective to adopt is that a representation is merely an action of a group on a vector space. And, just as faithful actions are an important class of actions, it will, later on, turn out to be important to have a corresponding notion for representations as well.

Definition 1.1.5 (Faithfulness). Let G be a group and let (V, ρ) be a representation of G. We say (V, ρ) is faithful if $\ker(\rho)$ is trivial.

In the next subsection, we begin to develop the theory of morphisms of representations, which will be crucial to the study of interactions and relationships between representations.

1.1.2 Morphisms of Representations

Definition 1.1.6 (Homomorphism of Representations)**.** Let G be a group and let (V, ρ) and (V', ρ') be two representations of G. A homomorphism of representations $T : V \to V$ is a linear map $T : V \to V'$ such that $\forall g \in G$,

$$T \circ \rho(g) = \rho'(g) \circ T$$

or equivalently, the following diagram commutes:

$$\begin{tikzcd} V \arrow[r, "\rho(g)"] \arrow[d, "T"'] & V \arrow[d, "T"] \\ V' \arrow[r, "\rho'(g)"'] & V' \end{tikzcd} \tag{1.1.1}$$

Such a map T is said to be G-*linear*.

Remark. The term G-linear comes from the fact that a homomorphism of representations satisfies the property that $T(g(v)) = g(T(v))$, where the notation $g(\cdot)$ represents the action of some $g \in G$, encoded by a representation. In this sense, T is somehow "linear over G".

A natural way to define two representations to be equal, or 'isomorphic,' is as follows.

Definition 1.1.7 (Equivalence of Representations)**.** Let G be a group and let (V, ρ) and (V', ρ') be two representations of G. We say that (V, ρ) and (V', ρ') are equivalent, denoted $(V, \rho) \sim (V', \rho')$, if there exists a homomorphism $T : (V, \rho) \to (V', \rho')$ that is invertible as a linear map—ie, that gives a linear isomorphism between V and V'.

Representations of the same group over the same vector space need not be equivalent.

Example 1.1.8 (Non-Equivalent Representations of the Klein 4-Group)**.** Let $G = C_2 \times C_2$ be the Klein 4-group (where $C_2 = \langle x \rangle$ is the cyclic group of order 2). Let $\alpha = (x, 1)$ and $\beta = (1, x)$. Together, they generate G.

Now, let K be a field. Consider a degree 1 representation $\rho : G \to K^\times$. We know that $\rho(G)$ must be a subgroup of $K^\times$ such that $|\rho(G)| \in \{1, 2, 4\}$. If $\text{char}(K) = 2$, then ρ must be the trivial representation, since $2 \nmid |K^\times|$. Else, all four maps ρ satisfying

$$(\rho(\alpha), \rho(\beta)) = (\pm 1, \pm 1)$$

give *non-equivalent* representations of G in $K^\times$. In particular, we see the non-equivalence because $K^\times$ is commutative.

The point of morphisms of representations is to be able to move from one vector space to another without losing the structural information captured by the representation. This is precisely illustrated in (1.1.1).

Example 1.1.9 (Representations of Cyclic Groups over $\mathbb{R}^2$ and $\mathbb{R}^3$). Consider the cyclic group $C_n = \langle g \rangle$ of order n. Let $V = \mathbb{R}^2, V' = \mathbb{R}^3$. Together with the respective maps

$$\rho : G \to \mathrm{GL}\big(\mathbb{R}^2\big) : g^m \mapsto \begin{bmatrix} \cos(2\pi/m) & -\sin(2\pi/m) \\ \sin(2\pi/m) & \cos(2\pi/m) \end{bmatrix}$$
$$\rho' : G \to \mathrm{GL}\big(\mathbb{R}^3\big) : g^m \mapsto \begin{bmatrix} \cos(2\pi/m) & -\sin(2\pi/m) & 0 \\ \sin(2\pi/m) & \cos(2\pi/m) & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

they give representations of C_n. Consider now the inclusion $T : \mathbb{R}^2 \to \mathbb{R}^3$ whose matrix with respect to the standard bases of $\mathbb{R}^2$ and $\mathbb{R}^3$ is $\begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{bmatrix}$. One can see that T gives a map from (V, ρ) to (V', ρ'). Indeed, the corestriction of T to its image is a linear isomorphism, which gives an equivalence between (V, ρ) and $(T(V), \rho)$, where we restrict the domains of each $\rho(g^m)$ to $T(V)$.

The above example leads to an interesting question. Can we think of one representation as being "contained" in another?

It turns out that we can.

1.1.3 Subrepresentations

We have the objects; we have the morphisms. It is only natural to think about what the subobjects would be in the context of group representations. And if Example 1.1.9 is any indication, they involve something more than just an inclusion. There is some structural property of a sub-vector space of a representation that makes it *compatible* with the representation structure. In the case of Example 1.1.9, for instance, this is the fact that the representation ρ' acted only “horizontally"–ie, “parallel" to the subspace $T(V)$.

More generally, it turns out that the property we really require a subspace to have in order to be ‘compatible’ with the representation structure is the following.

Definition 1.1.10 (G-Invariance). Let G be a group and let (V, ρ) be a representation of G. We say that a sub-vector space $W \leq V$ is G-invariant if for all $w \in W$ and $g \in G$,

$$\rho(g)(w) \in W$$

In other words, W is G-invariant if W is $\rho(g)$-invariant for every $g \in G$.

One can make the following observation. Let G be a group, (V, ρ) a representation of G, and $W \leq V$ a G-invariant subspace. Then, $\forall g \in G$, $\rho(g) \in \mathrm{GL}(W)$. That is, $\rho(g)$ is a linear automorphism of W whose inverse, $\rho(g^{-1})$, is *also* a linear automorphism of W. This then leads to the following definition of a subrepresentation.

Definition 1.1.11 (Subrepresentation). Let G be a group and let (V, ρ) be a representation of G. A subrepresentation of V is a pair $(W, \rho|_W)$ consisting of a G-invariant subspace $W \leq V$ and the map

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

It is very important to note that the map $\rho|_W$ is *not actually a restriction of* ρ *to a specific domain*. Rather, it is a map that restricts the domain of $\rho(g)$ for every $g \in G$.

One can also observe easily that a subrepresentation is given uniquely by a G-invariant subspace. Hence, we will often abuse notation and not distinguish between the pair $(W, \rho|_W)$ (which is actually a representation) and simply W (which is merely a subspace).

Example 1.1.12. Let G be a finite group and K a field. Consider the regular representation $\rho : G \to K[G]$. Let $\{e_g : g \in G\}$ denote a basis of $K[G]$. Then, the subspace $W := \operatorname{Span}\left(\sum_{g \in G} e_g\right)$ is G-invariant.

It turns out that morphisms of representations also give us subrepresentations.

Proposition 1.1.13. *Let G be a group and let (V, ρ) be a representation of G. Let $T : (V, \rho) \to (V, \rho)$ be a homomorphism of representations. Then, the subspaces $\ker(T)$ and $\operatorname{im}(T)$ of V are G-invariant.*

Proof. Fix $g \in G$ and $v \in \ker(T)$. We know $T(\rho(g)(v)) = \rho(g)(T(v))$. Since $T(v) = 0$, $T(\rho(g)(v)) = 0$. Hence, $\rho(g)(v) \in \ker(T)$, proving that $\ker(T)$ is G-invariant.

Now, fix $w \in \operatorname{im}(T)$. Then, $w = T(u)$ for some $u \in V$. Clearly, $\rho(g)(w) = \rho(g)(T(u)) = T(\rho(g)(u)) \in \operatorname{im}(T)$, proving that $\operatorname{im}(T)$ is G-invariant as well. □

1.1.4 Irreducibility

Having discussed the subobjects of representations (namely, subrepresentation), it is only natural to wish to describe whether a representation ever contains a nontrivial subrepresentation. I say “nontrivial" because any representation naturally admits two (uninteresting) subrepresentations: the trivial representation and itself.

Akin to the definition of simple groups, where we answer a similar question, we have the following definition that captures this idea.

Definition 1.1.14 (Irreducibility). Let G be a group and (V, ρ) a nonzero representation of G. We say (V, ρ) is irreducible if V contains no proper, nonzero G-invariant subspaces.

In similar fashion, we say a nonzero representation is reducible if it is not irreducible.

Given that MATH-314 focuses on *finite* groups, the following result is quite useful.

Proposition 1.1.15. *Let G be a group and let (V, ρ) be a representation of G. If G is finite and (V, ρ) is irreducible, then V is finite-dimensional.*

Proof. Since (V, ρ) is irreducible, in particular, $V \supsetneq \{0\}$—ie, $\exists v \in V$ such that $v \neq 0$. Let $W := \text{Span}(\{\rho(g)(v) : g \in G\})$. Since $0 \neq v \in W$, W is a nonzero subspace of V. Furthermore, since G is finite, W is finite-dimensional. We show that W is, in fact, G-invariant. Then, since V is irreducible, W could not possibly be a proper subspace of V, meaning that $W = V$, making V finite-dimensional as well.

Fix $h \in G$, and consider an arbitrary element $w = \sum_{g \in G} \lambda_g \rho(g)(v) \in W$. Then,

$$\begin{aligned} \rho(h)(w) &= \sum_{g \in G} \lambda_g \rho(h)(\rho(g)(v)) \\ &= \sum_{g \in G} \lambda_g \left(\rho(h) \circ \rho(g)\right)(v) \\ &= \sum_{g \in G} \lambda_g \rho(hg)(v) \in W \end{aligned}$$

proving that W is $\rho(h)$-invariant for every $h \in G$, making it a G-invariant subspace of V. Therefore, as argued above, $W = V$, proving that V is finite-dimensional. □

Example 1.1.16 (Simple Examples of Irreducible Representations).

1. Any representation of degree 1 is irreducible.
2. Let K be a field. The trivial embedding $\text{SL}(n, K) \hookrightarrow \text{GL}(n, K)$ gives an irreducible representation of $\text{SL}(n, K)$ over K^n.

   Proof. Assume $n > 1$ (else, the result follows from the previous point). For the sake of contradiction, suppose there exists a nonzero, $\text{SL}(n, K)$-invariant subspace W of K^n having dimension $m < n$. Let $\mathcal{B} = \{e_1, \ldots, e_m\}$ be a basis of W, extending to a basis $\overline{\mathcal{B}} = \{e_1, \ldots, e_m, e_{m+1}, \ldots, e_n\}$ of V. Consider the linear map $T \in \text{SL}(n, K)$

having matrix

$$[T]_{\overline{\mathcal{B}}} = \begin{bmatrix} & & & (-1)^{n+1} \\ & & \iddots & \\ & -1 & & \\ 1 & & & \end{bmatrix}$$

with respect to $\overline{\mathcal{B}}$. Clearly, $T(e_1) = e_n$, even though $e_1 \in W$ and $e_n \notin W$, contradicting the $\mathrm{SL}(n, K)$-invariance of W. □

Non-Example 1.1.17. Let G be a finite group and K a field. Consider the regular representation $(K[G], \rho)$. In the notation of Example 1.1.12, we know that $W := \mathrm{Span}\left(\sum_{g \in G} e_g\right)$ is G-invariant. If $|G| > 1$, then W is a proper subspace of $K[G]$, as it has dimension 1 (whereas $K[G]$ has dimension $|G|$). Furthermore, W is nonzero. Hence, $(K[G], \rho)$ is not irreducible (unless $|G| = 1$, in which case it follows from the first point of Example 1.1.16 that $(K[G], \rho)$ is irreducible).

We also have the following interesting criterion for irreducibility of representations of finite groups over $\mathbb{C}$.

Lemma 1.1.18. *Let G be a finite group and let $(\mathbb{C}^2, \rho)$ be a representation of G over $\mathbb{C}$. If there exist $g, h \in G$ such that g and h do not commute, then $(\mathbb{C}^2, \rho)$ is irreducible.*

Proof. `sorry` □

1.2 Invariant Constructions

In this section, we briefly examine how ordinary linear algebraic constructions can interact with representations. We are particularly interested in the notion of *invariance*, wherein a construction respects the structure of the representation(s) involved.

1.2.1 Direct Sums of Representations

The most elementary operation we can think about when we have two objects is *putting them together*. One of the most meaningful ways of doing so in the context of linear algebra is the direct sum of two vector spaces. It turns out that this extends rather naturally to representations.

Definition 1.2.1 (The Direct Sum of Two Representations)**.** Let G be a group and let (V, ρ) and (V', ρ') be representations of G. We define the direct sum of (V, ρ) and (V', ρ') to be the pair $(V \oplus V', \rho \oplus \rho')$, where $V \oplus V'$ is the direct sum of V and V' as vector spaces and $\rho \oplus \rho' : G \to \mathrm{GL}(V \oplus V')$ maps every $g \in G$ to the map

$$(\rho \oplus \rho')(g)(v \oplus v') = \rho(g)(v) \oplus \rho'(g)(v') \in \mathrm{GL}(V)$$

Remark. In similar fashion, we can also define the tensor product of two representations, though we will not do so here.

Proposition 1.2.2. *Let G be a group and let (V, ρ) and (V', ρ') be representations of G.*

1. *The direct sum $(V \oplus V', \rho \oplus \rho')$ of (V, ρ) and (V', ρ') is, indeed, a representation of G.*
2. *V and V' are G-invariant subspaces*[1] *of $V \oplus V'$.*

Proof.

1. Fix $g, h \in G$. For all $v \oplus v' \in V \oplus V'$,

$$\begin{aligned}(\rho \oplus \rho')(gh)(v \oplus v') &= \rho(gh)(v) \oplus \rho'(gh)(v') \\ &= \rho(g)(\rho(h)(v)) \oplus \rho'(g)(\rho'(h)(v')) \\ &= (\rho \oplus \rho')(g)((\rho \oplus \rho')(h)(v \oplus v'))\end{aligned}$$

proving that $\rho \oplus \rho'$ is multiplicative. Then, for any $g \in G$, $(\rho \oplus \rho')(g)$ has inverse $(\rho \oplus \rho')(g^{-1})$. Hence, $\rho \oplus \rho'$ is a homomorphism from G to $\mathrm{GL}(V \oplus V')$.

2. Fix $g \in G$ and $v \in V$. Clearly, $(\rho \oplus \rho')(g)(v) = \rho(g)(v)$. Since $\rho(g) \in \mathrm{GL}(V)$, it follows that $\rho(g)(v) \in V$. The proof that V' is G-invariant is identical.

[1] Technically, isomorphic to the subspaces $V \oplus \{0\}$ and $\{0\} \oplus V'$, but we overlook such distinctions.

□

The above proposition gives us another reason to consider the direct sum to be an "invariant" construction: while it enriches both the vector space structure and the representation structure of a summand by adding another representation into the mix, it does not take anything away from the constructions that already exist.

With direct sums, we also have similar notions to reducibility.

Definition 1.2.3 (Indecomposability)**.** A nonzero representation is said to be indecomposable if it is inexpressible as a direct sum of two proper, nonzero subrepresentations.

Nonzero representations that are not indecomposable are said to be decomposable.

We have a natural relationship between irreducibility and indecomposability.

Proposition 1.2.4. *Let G be a group and let (V, ρ) be a representation of G. If (V, ρ) is irreducible, then it is indecomposable.*

Proof. If $V = \{0\}$, then the result is vacuously true. If $V \neq \{0\}$, then if it is decomposable, it contains a proper, nonzero, G-invariant subspace, making it reducible. □

Example 1.2.5. Let $C_2 = \langle a \rangle$ be the cyclic group of order 2, and let (V, ρ) be the regular representation of C_2 over a field K.

1. Let $K = \mathbb{C}$. Then, let $W_1 := \text{Span}(e_1 + e_a)$ and $W_2 := \text{Span}(e_1 - e_a)$. It is obvious that $W_1 \oplus W_2 = V$. Furthermore, W_1 and W_2 are both C_2-invariant. Hence, the regular representation of C_2 over $\mathbb{C}$ is decomposable.
2. Let $K = \mathbb{F}_2$. Then, $V = \{0, e_1, e_a, e_1 + e_a\}$. If (V, ρ) were reducible, it would need to be expressible as the direct sum of two subrepresentations of degree 1. But, the only G-invariant subspace of V of dimension 1 is $\{0, e_1 + e_a\}$. Hence, (V, ρ) cannot be indecomposable.

The $K = \mathbb{F}_2$ case in the above example demonstrates an important fact: *the converse of Proposition*

1.2.4 is not true. The regular representation of C_2 over $\mathbb{F}_2$ is clearly reducible—the subspace $\{0, e_1 + e_a\}$ is clearly C_2-invariant—but it is still indecomposable. That said, it turns out that under certain conditions, we *do* have a converse.

Proposition 1.2.6. *Let G be a finite group and let K be a field. All indecomposable representations of G are irreducible if and only if* $\text{char}(K)$ *does not divide* $|G|$.

Proof. If $|G| = 1$, the result is trivial: we already know that $\text{char}(K)$ cannot divide $|G|$, and

$(\implies)$ Assume that all indecomposable representations of G are irreducible.

□

Finally, just like everywhere else in mathematics where we encounter the word "irreducible," in the context of representation theory, too, we have a notion of decomposition into irreducibles.

Definition 1.2.7 (Complete Reducibility)**.** A representation is said to be completely reducible if it is expressible as a direct sum of irreducible representations.

It turns out that complete reducibility can be better understood through complementary subrepresentations.

1.2.2 Complementary Subrepresentations

It is a well-known fact from Linear Algebra that for any finite-dimensional vector space V, for any subspace $W \leq V$, there exists a *complementary* subspace $W' \leq V$ such that $W \oplus W' = V$. As it turns out, we can define a notion of complementarity for representations, too.

Definition 1.2.8 (Complementary Subrepresentation)**.** Let G be a group and let (V, ρ) be a representation of G. Let $(W, \rho|_W)$ be a subrepresentation of (V, ρ). A complementary subrepresentation of $(W, \rho|_W)$ is a subrepresentation $(U, \rho|_U)$ such that $V = U \oplus W$.

This notion of complementarity is, indeed, compatible with the notion of direct sums of representations.

Proposition 1.2.9. *Let G be a group and let (V, ρ) be a representation of G. Let $(W, \rho|_W)$ and $(U, \rho|_U)$ be complementary subrepresentations. Then, their direct sum $(V, \rho|_W \oplus \rho|_U)$ is equivalent to (V, ρ) as a representation of G.*

Proof. It suffices to show that $\rho = \rho|_W \oplus \rho|_U$. Then, the identity map would give an equivalence of representations. Indeed, every $v \in V$ is expressible uniquely as a direct sum $w \oplus u$ for some $w \in W$ and $u \in U$. So, for all $g \in G$,

$$\begin{aligned}\rho(g)(v) &= \rho(g)(w \oplus u)\\ &= \rho(g)(w) \oplus \rho(g)(u)\\ &= \rho|_W(g)(w) \oplus \rho|_U(g)(u)\\ &= (\rho|_W \oplus \rho|_U)(g)(w \oplus u)\end{aligned}$$

where the sum in the second equality is direct because W and U are $\rho(g)$-invariant. □

We now recall an important result from Linear Algebra.

Definition 1.2.10 (Projection). Let V be a vector space and let $T : V \to V$ be linear. Observe that we have the following equivalence:

$$T^2 = T \iff \forall w \in \text{im}(T)\,,\ T(w) = w \tag{1.2.1}$$

If T satisfies either one of the above conditions, T is said to be a projection.

We do not prove (1.2.1), but we do prove the following lemma, which will prove to be useful.

Lemma 1.2.11. *Let V be a vector space. For all projections $T : V \to V$, $V = \ker(T) \oplus \text{im}(T)$.*

Proof. Let $T : V \to V$ be a projection. We then have the following.

<u>$\text{im}(T) \cap \ker(T) = \{0\}$:</u> Fix $w \in \text{im}(T) \cap \ker(T)$. Since $w \in \text{im}(T)$, $\exists v \in V$ such that $w = T(v)$. Furthermore, since $w \in \ker(T)$, $T(w) = 0$. Since $w = T(v)$, this is equivalent to saying that $T(T(v)) = 0$. But, by (1.2.1), $T(T(v)) = T(v)$. Hence, $T(v) = 0$. Then, since $T(v) = w$, it follows that $w = 0$.

$\underline{V = \ker(T) + \operatorname{im}(T)}$: Fix $v \in V$. We write $v = T(v) + (v - T(v))$. Clearly, $T(v) \in \operatorname{im}(T)$. Further, $T(v - T(v)) = T(v) - T(v) = 0$. Hence, $v - T(v) \in \ker(T)$.

Therefore, we do, indeed, have $V = \ker(T) \oplus \operatorname{im}(T)$. □

It turns out that this gives us an important criterion for decomposability.

Corollary 1.2.12. *Let G be a group and let (V, ρ) be a representation of G. If $T : (V, \rho) \to (V, \rho)$ is a G-linear projection, then $V = \ker(T) \oplus \operatorname{im}(T)$ is a direct sum of subrepresentations.*

Proof. The result follows immediately from Lemma 1.2.11 and Proposition 1.1.13. □

One also has a converse criterion for G-linearity.

Proposition 1.2.13. *Let G be a group and let (V, ρ) be a representation of G, and let $T : V \to V$ be a projection. If $\ker(T)$ and $\operatorname{im}(T)$ are both G-invariant, then T is G-linear.*

Proof. Since T is a projection, we know that $V = \ker(T) \oplus \operatorname{im}(T)$. Now, fix $g \in G$ and $v \in V$. We know v can uniquely be expressed as $u + w$, where $u \in \ker(T)$ and $w \in \operatorname{im}(T)$. Then,

$$\begin{aligned} T(\rho(g)(v)) &= T\left(\underbrace{\rho(g)(u)}_{\in \ker(T)} + \underbrace{\rho(g)(w)}_{\in \operatorname{im}(T)}\right) \\ &= \rho(g)(w) \\ &= \rho(g)(T(v)) \end{aligned}$$

proving that T is, indeed, G-linear. □

Example 1.2.14. Consider the situation in Example 1.1.9. As we discussed briefly at the beginning of Subsection 1.1.3, we can view (V, ρ) as a subrepresentation of (V', ρ'). Now, consider the linear map $S : V' \to V' : (x, y, z) \mapsto (x, y, 0)$, where (x, y, z) are coordinates with respect to the standard basis. This is clearly a projection operator with image V, the (x, y) plane, and kernel the z-axis. These are both clearly G-invariant, making S a G-linear projection.

Finally, we relate complementary subrepresentations and complete reducibility, which makes it clear why we are so interested in complementary subrepresentations.

Proposition 1.2.15. *A representation of a finite group is completely reducible if and only if each of its subrepresentations admits a complementary subrepresentation.*

Proof. Let G be a finite group and let (V, ρ) be a representation of G.

($\implies$) Assume (V, ρ) is completely reducible, with decomposition $V = \bigoplus_{i \in \mathcal{I}} W_i$ into irreducible subrepresentations. Let $U \leq V$ be G-invariant.

($\impliedby$) Assume every subrepresentation of (V, ρ) admits a complementary subrepresentation. We know that (V, ρ) is either irreducible, in which case we'd be done, or reducible, in which case there exists a proper, nonzero, G-invariant subspace $W_1 \leq V$.

□

1.2.3 Maschke's Theorem

Given the theme of this section—namely, understanding the compatibility of ordinary linear-algebraic constructions with representation structures—one might wonder under what conditions (if any) we have the existence of a complementary subrepresentations. The answer lies in Maschke's Theorem, which is the first major result of the course.

Theorem 1.2.16 (Maschke's Theorem). *Let G be a finite group, K a field such that $\operatorname{char}(K) \nmid |G|$, and (V, ρ) a representation of G over K. Then, any subrepresentation of V admits a complementary subrepresentation.*

Proof. Let $W \leq V$ be G-invariant. The idea is to construct a G-linear map from V to V with image W. Then, by Corollary 1.2.12, its kernel would give a complementary subrepresentation.

From Linear Algebra, we know that W admits a complementary (but not necessarily G-invariant) subspace $U \leq V$. Then, every $v \in V$ can uniquely be expressed as a sum $u + w$, where $u \in U$ and $w \in W$. Define $T : V \to V : u + w \mapsto w$. Clearly, T is a projection operator with image W and kernel U.

If T were G-linear, we would be done with the proof; unfortunately, T does not have to be G-linear. We therefore "convert" T into a G-linear projection $S : V \to V$ by *averaging over* G. Specifically, define

$$S := \frac{1}{|G|} \sum_{g \in G} \rho(g) \circ T \circ \rho(g)^{-1} \tag{1.2.2}$$

which is well-defined because $|G| \neq 0$ in K. We then show the following.

S is a projection with image W. Fix $v \in V$ and express it as $u + w$ for a unique $u \in U$ and $w \in W$. Then, for all $g \in G$,

- $T(\rho(g)^{-1}(v)) \in W$ because T is a projection with image W.
- $\rho(g)(T(\rho(g)^{-1}(v))) \in W$ because $T(\rho(g)^{-1}(v)) \in W$ and W is G-invariant.

Combined with the fact that W is closed under addition, this proves that $\mathrm{im}(S) \subseteq W$. Conversely, for all $w \in W$ and $g \in G$,

- $(\rho(g)^{-1})(w) = \rho(g^{-1})(w) \in W$ because W is G-invariant.
- $T(\rho(g^{-1})(w)) \in W$ because $\rho(g^{-1})(w) \in W$ and W is T-invariant.
- $\rho(g)(T(\rho(g^{-1})(w))) \in W$ because W is G-invariant.

Combined, again, with the fact that W is closed under addition, this proves that $W \subseteq \mathrm{im}(S)$. Therefore, we have that $W = \mathrm{im}(S)$.

Finally, since $T|_W = \mathrm{id}_W$, we have that $\forall w \in \mathrm{im}(S) = W$,

$$\begin{aligned} S(w) &= \frac{1}{|G|} \sum_{g \in G} \rho(g) \left(T \left(\underbrace{\rho(g)^{-1}(w)}_{\in W} \right) \right) \\ &= \frac{1}{|G|} \sum_{g \in G} \left(\rho(g) \circ \rho(g)^{-1} \right)(w) \\ &= \frac{1}{|G|} \sum_{g \in G} w = w \end{aligned}$$

proving that S is, indeed, a projection.

S is G-linear. Fix $v \in V$ and $h \in G$. We have

$$\begin{aligned} S(\rho(h)(v)) &= \frac{1}{|G|}\sum_{g\in G}(\rho(g)\circ T\circ \rho(g)^{-1})(\rho(h)(v)) \\ &= \frac{1}{|G|}\sum_{g\in G}(\rho(g)\circ T\circ \rho(g^{-1}h))(v) \end{aligned}$$

We now perform a change of variables. Observe that the map $g \mapsto h^{-1}g : G \to G$ is an automorphism. Hence, writing $g' = h^{-1}g$, we have

$$\begin{aligned} S(\rho(h)(v)) &= \frac{1}{|G|}\sum_{g'\in G}\Big(\rho(hg')\circ T\circ \rho\big((g')^{-1}\big)\Big)(v) \\ &= \rho(h)\left(\frac{1}{|G|}\sum_{g'\in G}\Big(\rho(g')\circ T\circ \rho(g')^{-1}\Big)\right)(v) \\ &= \rho(h)(S(v)) \end{aligned}$$

proving that S is, indeed, G-linear.

Therefore, by Corollary 1.2.12, $\ker(S)$ is a complementary subrepresentation of W. □

We also have the following important corollary.

Corollary 1.2.17. *Let G be a finite group, K a field such that* $\operatorname{char}(K) \nmid |G|$. *Then, every representation of G over K is completely reducible.*

Proof. Let (V, ρ) be a representation of G over K. If (V, ρ) is irreducible, we are done; else, it admits a nonzero, proper subrepresentation, which, by Maschke's Theorem, admits a complementary subrepresentation that is also proper and nonzero. If both of these are irreducible, then we are done; else, repeat this process. □

Remark. Nowhere in Definition 1.2.7 do we specify that the decomposition must be finite.

We note that both hypotheses of Maschke's Theorem—namely, that G is a finite group and that $\operatorname{char}(K) \nmid |G|$—are essential for Theorem 1.2.16 (and hence Corollary 1.2.17) to hold.

Non-Example 1.2.18 (Failure of Maschke's Theorem when $\operatorname{char}(K) \mid |G|$). Let $G = \langle a \rangle$ be a cyclic group of prime order p. Let $V = \mathbb{F}_p^2$, and define $\rho : G \to \mathrm{GL}(2, \mathbb{F}_p)$ by

$$\rho(a^r) = \begin{bmatrix} 1 & r \\ 0 & 1 \end{bmatrix} \quad \text{for } 0 \leq r \leq p-1.$$

1. (V, ρ) is a representation of G over $\mathbb{F}_p$.
2. (V, ρ) is not irreducible.
3. (V, ρ) is not completely reducible.

It turns out that Maschke's Theorem also has a *converse*.

Theorem 1.2.19 (Converse of Maschke's Theorem). *Let G be a finite group such that every finite-dimensional representation of G over some field K is completely reducible. Then,* $\operatorname{char}(K) \nmid |G|$.

Proof. Consider the regular representation $(K[G], \rho)$ of G over K, with basis $\mathcal{B} = \{e_g : g \in G\}$. The idea is to take advantage of the G-invariant properties of $\mathcal{B}$.

Consider the subspace

$$W := \left\{ \sum_{g \in G} \alpha_g e_g : \sum_{g \in G} \alpha_g = 0 \right\}$$

of dimension $\dim(V) - 1$. It turns out that W is G-invariant: for all $\sum_{g \in G} \alpha_g e_g \in W$ and $h \in G$, we have

$$\rho(h) \left(\sum_{g \in G} \alpha_g e_g \right) = \sum_{g \in G} \alpha_g e_{hg} \in W$$

(where the sum of the coefficients α_g is still zero). Then, by assumption, $\exists U \leq V$ that is both G-invariant and complementary to W. This means that U must be of dimension 1, and is hence the span of a single vector $u \in U$.

We study the action of G on U. Fix $h \in G$, and write $u = \sum_{g \in G} \beta_g e_g$ for $\beta_g \in K$. Then,

$$\rho(h)(u) - u = \sum_{g \in G} \underbrace{\beta_g e_{hg} - \beta_g e_g}_{\in W}$$

meaning that $\rho(h)(u) - u \in W$. But, $\rho(h)(u) - u \in U$ as well. Since $U \cap W = \{0\}$, this means that $\rho(h)(u) = u$ for all $h \in G$. Hence, the action of G on U is *trivial*. Therefore, for all $x \in G$,

$$\sum_{g \in G} \beta_g e_{hg} = \sum_{g \in G} \beta_g e_g$$

Comparing coefficients, we conclude that $\beta_{h^{-1}g} = \beta_g$ for all $h, g \in G$. Letting $h = g$, we get, in particular, that $\forall g \in G$, $\beta_g = \beta_1$. Therefore, $u = \beta_1 \sum_{g \in G} e_g$. This, in particular, implies that $u' := \sum_{g \in G} e_g \notin W$, because otherwise, $u = \beta_1 u'$ would also lie in W, which it does not. Therefore, the sum of the coordinates of u' with respect to $\mathcal{B}$ cannot be zero. But, this sum is nothing but the cardinality of G (or rather, its image in the canonical map $\mathbb{Z} \to K$). Since this is nonzero, it must be that $\mathrm{char}(K) \nmid |G|$, as required. □

Combining Theorems 1.2.16 and 1.2.19, we conclude that $\mathrm{char}(K) \mid |G|$ if and only if every subrepresentation of G over K admits a complementary subrepresentation.

1.2.4 The G-Invariant Inner-Product

It turns out that we also have a notion of inner-products being compatible with representation strutures.

Definition 1.2.20 (G-Invariant Inner-Product). Let G be a group and let (V, ρ) be a representation of G over $\mathbb{C}$ such that V admits an inner-product $\langle \cdot, \cdot \rangle$.We say that $\langle \cdot, \cdot \rangle$ is G-invariant if $\forall g \in G$ and $\forall x, y \in V$,

$$\langle x, y \rangle = \langle \rho(g)(x), \rho(g)(y) \rangle$$

Equivalently, $\langle \cdot, \cdot \rangle$ is G-invariant if $\mathrm{im}(\rho) \subseteq \mathrm{U}(V)$, ie, if, for every $g \in G$, $\rho(g)$ is a *unitary* $\mathbb{C}$-linear map from V to V.

Intrinsic to the notion of an inner-product is that of orthogonality. In the following proposition, we understand the significance of G-invariance in the context of subrepresentations.

Proposition 1.2.21. *Let G be a group and let (V, ρ) be a representation of G over $\mathbb{C}$ of finite dimension. Let $\langle \cdot, \cdot \rangle$ be a G-invariant inner-product on V. Then, the orthogonal complement of any G-invariant subspace of V is also G-invariant.*

Proof. Let $W \leq V$ be G-invariant, and denote by $W^{\perp}$ its orthogonal complement. Fix $g \in G$ and $w \in W^{\perp}$. To show that $\rho(g)(w) \in W^{\perp}$, we show it is orthogonal to every $v \in W$ with respect to $\langle \cdot, \cdot \rangle$.

Fix $v \in W$. Then, since $\langle \cdot, \cdot \rangle$ is G-invariant,

$$\begin{aligned} \langle v, \rho(g)(w) \rangle &= \left\langle \rho(g^{-1})(v), \rho(g^{-1}g)(w) \right\rangle \\ &= \left\langle \rho(g^{-1})(v), w \right\rangle \end{aligned}$$

Since W is G-invariant, $\rho(g^{-1})(v) \in W$, making it orthogonal to w, which lies in the orthogonal complement of W. Therefore, $\langle v, \rho(g)(w) \rangle = 0$, proving that $\rho(g)(w) \in W^{\perp}$ as required. □

Corollary 1.2.22. *Let G be a group and let (V, ρ) be a representation of G over $\mathbb{C}$. If V is finite dimensional and admits a G-invariant inner-product, then V is completely reducible.*

Proof. If V is finite dimensional and admits a G-invariant inner-product, then by Proposition 1.2.21, for any $W \leq V$ G-invariant, $W^{\perp}$ is G-invariant as well. Since $W \oplus W^{\perp} = V$ and both W and $W^{\perp}$ are finite-dimensional, we can prove the result using similar reasoning to what we used to prove Corollary 1.2.17. □

1.3 Group Algebras and Modules

In this section, we study an important class of field algebras, namely, group algebras, and an important class of modules over said algebras, namely, group modules.

1.3.1 Preliminaries

Definition 1.3.1 (Group Algebra). Let G be a finite group and let K be a field. The group algebra KG is the K-algebra obtained by endowing the free vector space $K[G]$ generated by G (as a set) with the multiplication

$$\left(\sum_{g \in G} \alpha_g e_g \right) \cdot \left(\sum_{g \in G} \beta_g e_g \right) := \sum_{g \in G} \sum_{h \in G} \alpha_g \beta_h e_{gh}$$

Remark.

1. It is easy to verify that KG is, indeed, a K-algebra, with the multiplicative identity given by e_1 (where $1 \in G$ is the identity).
2. The map $g \mapsto e_g : G \to KG$ gives a trivial embedding of G in KG.
3. Going forward, for ease of notation, we will denote each basis element e_g as simply g.

We have a similar notion of group modules.

Definition 1.3.2 (Group Module). Let G be a group and let V be a vector space over a field K. We say that V is a KG-module if we can define a multiplication $g \cdot v$ for some $g \in G$ and $v \in V$ that satisfies the following conditions for all $u, v \in V$, $g, h \in G$ and $\lambda \in K$:

1. $g \cdot v \in V$
2. $(gh) \cdot v = g \cdot (h \cdot v)$
3. $1 \cdot v = v$
4. $g \cdot (\lambda v) = \lambda (g \cdot v)$
5. $g \cdot (u + v) = g \cdot u + g \cdot v$

Note that a KG-module is, indeed, a module over KG.

Proposition 1.3.3. *Let G be a group and let V be a vector space over a field K. If V is a KG-module with multiplication $\cdot$ (as per Definition 1.3.2), then for $v \in V$, the multiplication*

$$\left(\sum_{g \in G} \lambda_g e_g\right) \cdot v := \sum_{g \in G} \lambda_g (g \cdot v)$$

endows V with a module structure over $K[G]$.

Furthermore, it turns out that we can move from modules to representations and vice-versa quite easily.

Proposition 1.3.4. *Let G be a group and let V be a vector space over a field K.*

1. *If $\rho : G \to \mathrm{GL}(V)$ gives a representation of G, then V is a KG-module with multiplication given by $g \cdot v = \rho(g)(v)$ for all $g \in G$ and $v \in V$.*

2. *If V is a KG-module with multiplication $\cdot$, the map $\rho : G \to \mathrm{GL}(V)$ given by $\rho(g)(v) := g \cdot v$ is a representation.*

The proofs of the above propositions are trivial and merely involve manually checking several basic conditions. Hence, we omit them.

We now give a basic 'dictionary' of sorts to go back and forth between the language of group modules and that of representations:

KG-Modules	**Representations**
Simple	Irreducible
Semi-Simple	Completely Irreducible
Submodule	Subrepresentation
Viewing KG as a KG-Module	The Regular Representation
Isomorphism	Equivalence of Representations
Dimension (as a K-vector space)	Degree

We illustrate the above equivalence by stating Maschke's Theorem in the language of KG-Modules.

Lemma 1.3.5 (Maschke's Theorem, Module Version). *Let G be a finite group, K a field whose characteristic does not divide the order of G. Then, any KG-Module V is semi-simple.*

1.3.2 Schur's Lemmas

In this subsection, we explore several versions of an important result by Schur. The main result consists of two cases, the first of which shall (by convention) deal with the non-isomorphic case and the second of which shall deal with the isomorphic case. We will refer to them as Schur's First and Second Lemmas respectively. We begin by stating them in their most general form.

Theorem 1.3.6 (Schur's Lemmas for Rings). *Let A be a ring and let S, T be simple A-modules.*

1. *If S and T are non-isomorphic, then $\mathrm{Hom}_A(S,T) = \{0\}$.*
2. *If S and T are isomorphic, then $\mathrm{Hom}_A(S,T)$ is a division ring.*

Proof. We rely on the fact that for all $\phi \in \mathrm{Hom}_A(S,T)$, $\ker(\phi) \leq S$ and $\mathrm{im}(\phi) \leq T$.

1. Let S and T be non-isomorphic. Fix $\phi \in \mathrm{Hom}_A(S,T)$. Since S is simple, we must have that $\ker(\phi) \in \{\{0\}, S\}$. If $\ker(\phi) = \{0\}$, then $\mathrm{im}(\phi) = T$, meaning $S \cong T$, a contradiction.

2. Let $\phi \in \mathrm{Hom}_A(S, T) \setminus \{0\}$. Then, $\ker(\phi) \neq S$, meaning that $\ker(\phi) = \{0\}$. Then, $\mathrm{im}(\phi) = T$, making ϕ an isomorphism. In particular, this means that ϕ admits an inverse, making $\mathrm{Hom}_A(S, T)$ a division ring.

□

It turns out we can do a bit better when dealing with a specific class of rings, namely, algebras over fields.

Theorem 1.3.7 (Schur's Lemmas for Algebras). *Let K be an algebraically closed field and A a K-algebra. Let S and T be simple A-modules.*

1. *If $S \ncong T$, then $\mathrm{Hom}_A(S, T) = \{0\}$.*
2. *If $S \cong T$, then $K \cong \mathrm{Hom}_A(S, T)$ via the map $\alpha \mapsto \alpha \cdot \mathrm{id}$.*

Proof.

1. As before.

2. We do not distinguish S and T in this proof.

   Fix $\phi \in \mathrm{Hom}_A(S, S)$. Then, ϕ can be viewed as an element of $\mathrm{M}_n(K)$, where $n = \dim(S)$. Since K is algebraically closed, ϕ admits an eigenvalue $\lambda \in K$. Now, consider the map $\phi - \lambda\,\mathrm{id} \in \mathrm{Hom}_A(S, S)$. Clearly, $\ker(\phi - \lambda\,\mathrm{id}) \neq \{0\}$, since it contains all eigenvectors with eigenvalue λ. Since S is simple, it must be that $\ker(\phi - \lambda\,\mathrm{id}) = S$, meaning $\phi - \lambda\,\mathrm{id} = 0$. In other words, $\phi = \lambda\,\mathrm{id}$.

□

We also have a converse when working with algebras.

Theorem 1.3.8 (Converse of Schur's Lemma for Algebras). *Let K be a field, A a K-algebra and M a completely reducible A-module. If $\mathrm{Hom}_A(M, M) = K$, then M is simple.*

Proof. `sorry` □

Theorem 1.3.9 (Schur's Lemmas for Finite Groups, over $\mathbb{C}$). *Let G be a finite group and let S and T be simple $\mathbb{C}G$ modules that are finite-dimensional (as vector spaces) over K, with associated representations $\rho_S : G \to \mathrm{GL}(S)$ and $\rho_T : G \to \mathrm{GL}(T)$. Let $f : S \to T$ be an arbitrary $\mathbb{C}$-linear map. Define the map*

$$\widehat{f} := \frac{1}{|G|} \sum_{g \in G} \rho_T(g) \circ f \circ \rho_S\left(g^{-1}\right) \tag{1.3.1}$$

Then, $\widehat{f}$ is, in fact, a $\mathbb{C}G$-module homomorphism. Furthermore, we have the following:

1. *If $S \ncong T$, then $\widehat{f}$ is identically zero.*
2. *If $S \cong T$, then*

$$\widehat{f} = \frac{1}{\dim(S)} \mathrm{Tr}(f) \cdot \mathrm{id}_S$$

Proof. We only really need to show that $\widehat{f} \in \mathrm{Hom}_{\mathbb{C}G}(S, T)$. The rest follows relatively naturally from Theorem 1.3.7 (Schur's Lemmas for Algebras), as we shall see. So, fix $h \in G$. Observe that

$$\begin{aligned}
\rho_T(h) \circ \widehat{f} &= \rho_T(h) \left(\frac{1}{|G|} \sum_{g \in G} \rho_T(g) \circ f \circ \rho_S\left(g^{-1}\right) \right) \\
&= \frac{1}{|G|} \sum_{g \in G} \rho_T(hg) \circ f \circ \rho_S\left(g^{-1}\right) \circ \rho_S\left(h^{-1}\right) \circ \rho_S(h) \\
&= \frac{1}{|G|} \sum_{g \in G} \left(\rho_T(hg) \circ f \circ \rho_S\left(g^{-1}h^{-1}\right)\right) \circ \circ \rho_S(h) \\
&= \widehat{f} \circ \rho_S(h)
\end{aligned}$$

proving that $\widehat{f}$ is, indeed, a homomorphism of $\mathbb{C}G$-modules. Then,

1. If $S \ncong T$, then by Schur's First Lemma for Algebras, $\widehat{f}$ is identically 0.

2. If $S \ncong T$, then by Schur's Second Lemma for Algebras, $\widehat{f}$ is a scalar multiple of the identity. Write $\widehat{f} = \lambda \cdot \mathrm{id}_S$. Clearly, we have that $\mathrm{Tr}\left(\widehat{f}\right) = \lambda \dim(S)$. But, by the definition of $\widehat{f}$, we have that

$$\mathrm{Tr}\left(\widehat{f}\right) = \frac{1}{|G|} \sum_{g \in G} \mathrm{Tr}\left(\rho_T(g) \circ f \circ \rho_S\left(g^{-1}\right)\right)$$

$$= \frac{1}{|G|} \sum_{g \in G} \mathrm{Tr}\big(f \circ \rho_T(g) \circ \rho_S(g^{-1})\big)$$
$$= \frac{1}{|G|} \sum_{g \in G} \mathrm{Tr}(f) = \mathrm{Tr}(f)$$

where we can apply the Trace Theorem to the composition $\rho_T(g) \circ f \circ \rho_S(g^{-1})$ because $S \cong T$, meaning $\rho_S = \rho_T$ and $\dim(S) = \dim(T)$ (meaning that we can, indeed, change the order of composition and get a 'sensible' linear map, as all dimensions agree). Since the trace of a linear map is unique, we must have that $\lambda \cdot \dim(S) = \mathrm{Tr}(f) \iff \lambda = \frac{1}{\dim(S)} \mathrm{Tr}(f)$ (we know $\dim(S) \neq 0$ because S is simple). This then tells us that $\widehat{f}$ is of the desired form.

□

Schur's Lemmas (especially the version thereof pertaining to complex representations of finite groups) will prove to be incredibly useful. In the next subsection, we will give a direct application to the classification of representations of finite abelian groups; however, this is not the last that we will be seeing of them.

1.3.3 Representations of Finite Abelian Groups over $\mathbb{C}$

It is natural to wonder what the purpose was of studying group algebras and modules. It turns out that one of the reasons the correspondence between representations and group modules is so powerful is that it allows the application of Schur's Lemmas to representation theoretic problems. For instance, in the following Lemma, we classify all irreducible representations of finite abelian groups over $\mathbb{C}$.

Lemma 1.3.10. *Let G be a fininte abelian group. Then, all irreducible $\mathbb{C}G$-modules are of dimension 1. Equivalently, all irreducible representations of G over $\mathbb{C}$ are of degree 1.*

Proof. Let V be an irreducible $\mathbb{C}G$-module. Since G is abelian, for all $g, h \in G$ and $v \in V$, $(gh) \cdot v = (hg) \cdot v$. Therefore, for some fixed $h \in G$, the following map is $\mathbb{C}G$-linear:

$$\phi_h : V \to V : v \mapsto h \cdot v$$

By Theorem 1.3.9, we know that $\exists \lambda_h \in \mathbb{C}$ such that $\widehat{\phi_h} = \phi_h = \lambda_h \cdot \mathrm{id}_V$. Hence, any subspace of V must be a $\mathbb{C}G$-submodule. But, since V is irreducible, V cannot admit any nonzero, proper $\mathbb{C}G$-submodules unless V is of ($\mathbb{C}$-)dimension 1. □

We now have a complete classification of irreducible representations of cyclic groups over $\mathbb{C}$.

Corollary 1.3.11. *Let $G = C_n = \langle a \rangle$ be the cyclic group of order n. Then, there are precisely n irreducible representations of G over $\mathbb{C}$.*

Proof. Let G be a group and let (V, ρ) be a representation of G. We know, from Lemma 1.3.10, that $V \cong \mathbb{C}$ and hence, $\mathrm{GL}(V) \cong \mathbb{C}^\times$. Now, let $x := \rho(a)$. It must be that $x^n = 1$, making x an nth root of unity. In other words, $\exists 1 \leq k \leq n$ such that $x = e^{\frac{2\pi i}{k}}$. Therefore, there are precisely n possible choices of x, each giving a different representation. □

Lemma 1.3.10 is also useful in the study of representations over $\mathbb{C}$ of arbitrary finite groups.

Proposition 1.3.12. *Let G be a finite group and let (V, ρ) be a representation of G over $\mathbb{C}$. For all $g \in G$, there is a basis of V with respect to which $\rho(g)$ has matrix $\mathrm{diag}(\varepsilon_1, \cdots, \varepsilon_n)$, with $\varepsilon_i^{\mathrm{ord}(g)} = 1$ for all $1 \leq i \leq n$.*

Proof. Fix $g \in G$, and consider the representation $\rho' : \langle g \rangle \to \mathrm{GL}(V)$ given by $\rho' = \rho|_{\langle g \rangle}$. Then, ρ' is a representation of a finite abelian group.

By Maschke's Theorem, $\rho' = \sigma_1 \oplus \cdots \oplus \sigma_k$ for irreducible subrepresentations $\sigma_1, \ldots, \sigma_m$ of $\langle g \rangle$. By Lemma 1.3.10, we know that $\deg(\sigma_i) = 1$ for each i, and hence, that $m = n$. Picking $\mathcal{B}$ to be the basis corresponding to this decomposition of ρ', we get that the matrix of ρ with respect to $\mathcal{B}$ is, indeed, of the desired form. □

As it turns out, we can combine the theory developed here with the Structure Theorem for Finite Abelian Groups to get an interesting result.

Lemma 1.3.13. *Let G be a finite abelian group, expressed as a product $C_{n_1} \times \cdots \times C_{n_r}$ of cyclic groups C_{n_i} of order $n_i > 1$. Then, G has a faithful representation of degree r over $\mathbb{C}$.*

Proof. Consider the space $V = \mathbb{C}^r = \mathbb{C}_1 \oplus \cdots \oplus \mathbb{C}_r$ (where each $\mathbb{C}_i$ is the one-dimensional subspace spanned by the ith element of some chosen $\mathbb{C}$-basis for V). Let $C_{n_i} = \langle g_i \rangle$ and denote by e_i the corresponding generators $(1, \ldots, 1, g_i, 1, \ldots, 1)$ of G. Define the map

$$\rho : G \to \mathbb{C} : e_i \mapsto R_i \tag{1.3.2}$$

where R_i is the rotation by $2\pi/n_i$ acting on the subspace $\mathbb{C}_i \cong \mathbb{C}$. In other words, with respect to the isomorphism $\mathrm{GL}(\mathbb{C}_i) \cong \mathbb{C}^\times$, the map R_i corresponds to $\exp(2\pi/n_i)$.[2]

ρ has the following effect on group elements: for two group elements acting on the same component of V, ρ maps their product to the composition of their associated rotations, and for elements acting on different components, ρ combines their componentwise actions into a single action across two components. Therefore, ρ is a group homomorphism, and hence, (V, ρ) is a representation of G over $\mathbb{C}$.

We now show that ρ is injective. If $g \in G$ acts identically on all of V, it must, in particular, act identically on each component. But, the action of g on each $\mathbb{C}_j$ is merely the action of the jth component of g on $\mathbb{C}_j$. It is easy to see that the componentwise actions of ρ on V are all faithful, meaning that each component of g is the identity in its respective cyclic group. Therefore, g must be the identity in G, making ρ a faithful representation. □

[2] To be perfectly precise, e_i is mapped not to R_i but to the image of R_i in the inclusion $\mathrm{GL}(\mathbb{C}_i) \to \mathrm{GL}(V)$ that extends R_i by acting as the identity on components other than i and as R_i on component i. We use the word 'component' to refer to a one-dimensional direct summand $\mathbb{C}_j$ of V.

Chapter 2

Character Theory

Figure 2.1: The thumbnail of a YouTube video titled “What is Character Theory? | Let’s Talk Theory" by Dapper Mr. Tom. The video has nothing to do with mathematics.

In this chapter, we study an important type of functions from groups to fields known as characters. As we shall see, characters encode several useful properties of a group, and have been used extensively to prove several results about finite groups, (the representations of) which are the main object of study in this course. One of the reasons characters are useful to understand representation structures is that they are *class functions*. That is, they encode information not about an individual element of a group but about its conjugacy class, making them good indicators of *structural* and *behavioural* properties. In particular, the character of a representation is independent of the choice of basis of the associated vector space.

Throughout this chapter, we denote by G an arbitrary finite group.

2.1 The Theory of Irreducible Characters

In this section, we give an overview of the theory of irreducilbe characters. Our approach focuses extensively on the notion of orthogonality with respect to an inner product we shall soon define. An interesting result we will go on to prove is that irreducilbe characters play an important role in a broader class of functions on groups, telling us that representation theory can be used to study not only groups themselves but also functions thereof.

2.1.1 On Central Functions

As we all know, a group can contain several elements that all behave similarly—take, for instance, similar matrices in any general linear group. This is why we have the notion of *conjugacy classes*, which allow us to study the elements of a group in terms of their actions or behaviours.

The purpose of character theory is to understand the structural and behavioural properties of a group, without focusing on syntactic particularities. This is why we define the notion of a *class function*.

Definition 2.1.1 (Class Function)**.** Let X be any set. A function $f : G \to X$ is said to be a class function if $f(x) = f(g^{-1}xg)$ for all $x, g \in G$—in other words, if it is constant on all conjugacy classes of G.

In this section, we will primarily be focusing on complex representations. Therefore, the following definition is useful.

Definition 2.1.2 (Central Function)**.** We say $f : G \to \mathbb{C}$ is central if it is a class function. In other words, central functions are precisely $\mathbb{C}$-valued class functions.

We are already familiar with several examples of central functions.

Example 2.1.3 (Examples of Central Functions)**.** The following are all central:

1. The order function $h \mapsto \text{ord}(h) : H \to \mathbb{N} \subset \mathbb{C}$ for any group H
2. The determinant function $A \mapsto \det(A) : \text{GL}(n, \mathbb{C}) \to \mathbb{C}$ for any $n \in \mathbb{N}$
3. The trace function $A \mapsto \text{Tr}(A) : \text{GL}(n, \mathbb{C}) \to \mathbb{C}$ for any $n \in \mathbb{N}$

The last two examples are, in particular, compatible with representations of G over $\mathbb{C}$. This will prove to be important when we define the character of a representation. Before doing so, however, we will need to outline the structure of the inner-product space of central functions on G. First, some notation.

Notation. We define

1. $\mathcal{F}(G, \mathbb{C}) := \{f : G \to \mathbb{C}\}$
2. $\mathcal{F}_C(G, \mathbb{C}) := \{f \in \mathcal{F}(G, \mathbb{C}) : f \text{ is central}\}$
3. $\delta_g(x)$ to be the indicator function (for $g, x \in G$).

We have the following natural result.

Proposition 2.1.4 ($\mathbb{C}$-Vector Space Structure of $\mathcal{F}(G, \mathbb{C})$ and $\mathcal{F}_C(G, \mathbb{C})$).

1. *$\mathcal{F}(G, \mathbb{C})$ is a $\mathbb{C}$-vector space of dimension $|G|$, with basis $\{\delta_g : g \in G\}$.*
2. *$\mathcal{F}_C(G, \mathbb{C})$ is a subspace of $\mathcal{F}(G, \mathbb{C})$ of dimension equal to the number of conjugacy classes of G, with basis $\{\delta_g : g$ uniquely represents a conjugacy class of $G\}$.*

Proof. The model we choose for this proof is that of k^n being isomorphic to the set of functions from $\{1, \ldots, n\}$ to k (for any field k). Under this model, the indicator functions on $\{1, \ldots, n\}$ correspond to the standard basis of k^n.

1. Since G is finite, this is immediate from the model described above.

2. That $\mathcal{F}_C(G, \mathbb{C})$ is a subspace follows from the fact that the sum of two central functions is central, as is any scalar multiple of a central function. Furthermore, since central functions are uniquely determined by their values on each conjugacy class, $\dim(\mathcal{F}_C(G, \mathbb{C}))$ is the number of conjugacy classes of G.

   I also offer a more formal argument here for the dimensionality, as I found it instructive to think about it this way. Let $C_1, \ldots, C_r$ be the conjugacy classes of G. Write $C_i = \left\{g_{i_1}, g_{i_2}, \ldots, g_{i_{l_i}}\right\}$. Let $w_i := \sum_{j=1}^{l_i} \delta_{g_{i_j}}$. It is easy to see that the w_i are linearly independent: any linear combination of all the w_i is, in particular, a linear combination of δ_g as g ranges over G, with each δ_g appearing exactly once. Furthermore, the w_i span $\mathcal{F}_C(G, \mathbb{C})$: their span is clearly contained in $\mathcal{F}_C(G, \mathbb{C})$, and every element of $\mathcal{F}_C(G, \mathbb{C})$ must be constant on any given conjugacy class, meaning that the coordinates of conjugate components must be the same.

□

It turns out that there is also a natural inner-product on $\mathcal{F}(G,\mathbb{C})$.

Definition 2.1.5 (Standard Inner-Product on $\mathcal{F}(G,\mathbb{C})$). Define the function $\langle\cdot,\cdot\rangle : \mathcal{F}(G,\mathbb{C})\times\mathcal{F}(G,\mathbb{C})\to\mathbb{C}$ by

$$\langle f_1, f_2\rangle = \frac{1}{|G|}\sum_{g\in G} f_1(g)\overline{f_2(g)} \tag{2.1.1}$$

It is easy enough to show that the $\langle\cdot,\cdot\rangle$ is, indeed, an inner-product on $\mathcal{F}(G,\mathbb{C})$. We will also use it as an inner-product on $\mathcal{F}_C(G,\mathbb{C})$.

An obvious orthogonal basis for $\mathcal{F}_C(G,\mathbb{C})$ is that of the indicator functions of representatives of distinct conjugacy classes. However, in this paradigm, the set S of conjugacy classes of G merely acts as an *index* set for the standard basis of $\mathbb{C}^{|S|}$. Ie, we can infer nothing about S beyond its size, a quantity that does not tell us about the actual *group* structure of G (for instance, for any prime p, the decidedly non-isomorphic abelian groups $\mathbb{Z}/_{p^2\mathbb{Z}}$ and $\mathbb{Z}/_{p\mathbb{Z}}\oplus\mathbb{Z}/_{p\mathbb{Z}}$ both have exactly p^2 conjugacy classes). It turns out that we can find a much better orthogonal (indeed, ortho*normal*) basis for $\mathcal{F}_C(G,\mathbb{C})$ in the world of *characters*, a class of central functions closely related to the group structure of G.

2.1.2 Introduction to Character Theory

In this subsection, we introduce a central function that is compatible with the notion of a representation, namely, the *character*. As we saw in Example 2.1.3, both the trace and the determinant would be good options, but the convention is to define the character in terms of the trace. A heuristic reason is that this way, given characters associated to two representations, their sum will give the character of the direct sum, and their product that of the tensor product of the underlying representations. There are deeper reasons too, which will become clearer as we progress.

Definition 2.1.6 (Character). Let V be a $\mathbb{C}G$-module. The character of V is the map $\chi_V : G\to\mathbb{C}$ given by $\chi_V(g) = \mathrm{Tr}(\rho(g))$, where ρ is the representation associated to V.

Immediately, we are able to "import" the following definitions from Chapter 1.

Definition 2.1.7 (Irreducibility). We say a character χ_V is irreducible if the associated representation (V, ρ) is irreducible over $\mathbb{C}$.

Definition 2.1.8 (Degree). We define the degree of a character to be that of its associated representation.

Definition 2.1.9 (Trivial Character). We define the trivial character to be that associated with the trivial representation.

Characters have several important properties, which we list below. We will make extensive use of these properties for the remainder of this chapter.

Proposition 2.1.10 (On the Behaviour of Characters). *Let V be a $\mathbb{C}G$-module, with associated representation ρ.*

1. *For all $\mathbb{C}G$-modules W, $\chi_{V \oplus W} = \chi_V + \chi_W$*
2. *For all $\mathbb{C}G$-modules W, $V \cong W \implies \chi_V = \chi_W$*
3. $\dim(V) = \chi_V(1)$
4. *For all $g \in G$, $\chi_V(g)$ is a sum of dth roots of unity, where $d = \operatorname{ord}(g)$.*
5. *For all $g \in G$, $|\chi_V(g)| \leq \dim(V)$, with equality iff $g \in \ker(\rho)$.*
6. *For all $g \in G$, $\chi_V(g^{-1}) = \overline{\chi_V(g)}$*

Proof. We just give sketches here, not complete proofs.

1. This follows from the fact that the trace of a direct sum is the sum of the traces.
2. This follows from the invariance of the trace under change of basis.
3. This follows from the fact that the trace of the identity is the dimension of the space.
4. For any $g \in G$ of order d, $\rho(g)$ is of order d. Hence, its minimal polynomial divides $X^d - 1 \in \mathbb{C}[X]$, which has distinct roots in $\mathbb{C}$. This means that the eigenvalues of $\rho(g)$ are dth roots of unity. Putting $\rho(g)$ in Jordan Normal Form, we see that its trace is a sum of dth roots of unity.[1]
5. `sorry`
6. `sorry`

[1] It is not necessarily a sum of *all* dth roots of unity, or even *distinct* dth roots of unity.

□

We now give a few examples of characters of representations.

Example 2.1.11 (The Dihedral Group of Order 8). Let $G = D_8$, the dihedral group of order 8. Consider the presentation

$$G = \left\langle a, b \mid a^4 = b^2 = 1, b^{-1}ab = a^{-1} \right\rangle$$

Let $\rho : G \to \mathrm{GL}(2, \mathbb{C})$ be a representation of G over $\mathbb{C}$ given by

$$\rho(a) = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \qquad \text{and} \qquad \rho(b) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

The associated character χ_V then takes on the following values:

g	1	a	a^2	a^3	b	ab	a^2b	a^3b
$\rho(g)$	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$	$\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$	$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$	$\begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}$	$\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
$\chi_V(g)$	2	0	-2	0	0	0	0	0

One can show the conjugacy classes of D_8 to be precisely $\{1\}$, $\{a, a^3\}$, $\{a^2\}$, $\{b, a^2b\}$, and $\{ab, a^3b\}$. From the table above, it is clear that conjugate elements do, indeed, have the same character value. Therefore, for the sake of brevity, one typically only lists the values of a character corresponding to the representatives of its conjugacy classes.

Example 2.1.12 (The Cyclic Group of Order 3). Let $G = C_3 = \langle a \rangle$ be the cyclic group of order 3. By Corollary 1.3.11, we know that G admits exactly three irreducible representations over $\mathbb{C}$, all of degree 1, each corresponding to choice of 3rd root of unity to which to send a. Denote these by ρ_1, ρ_2 and ρ_3, so that $\rho_j(a) = e^{\frac{2\pi i(j-1)}{3}}$ for $j = 1, 2, 3$. Denote their corresponding (irreducible) characters χ_1, χ_2 and χ_3. Since the trace map is simply the constant map on a space of dimension 1, we have the following values for the characters:

g	1	a	a^2
$\chi_1(g)$	1	1	1
$\chi_2(g)$	1	$e^{\frac{2\pi i}{3}}$	$e^{\frac{4\pi i}{3}}$
$\chi_3(g)$	1	$e^{\frac{4\pi i}{3}}$	$e^{\frac{2\pi i}{3}}$

In the above example, we see that the characters of the irreducible representations of G form an orthonormal system with respect to the standard inner-product (2.1.1)—for instance, $\chi_1 \neq \chi_2$, and clearly,

$$\begin{aligned}\langle \chi_1, \chi_2 \rangle &= \frac{1}{3} \sum_{g \in G} \chi_1(g)\overline{\chi_2(g)} \\ &= \frac{1}{3}\left(1 + \overline{e^{\frac{2\pi i}{3}}} + \overline{e^{\frac{4\pi i}{3}}}\right) \\ &= \frac{1}{3}\left(1 + e^{\frac{4\pi i}{3}} + e^{\frac{2\pi i}{3}}\right) = 0\end{aligned}$$

whereas $\langle \chi_1, \chi_1 \rangle = 1$. In similar fashion, one can check the remaining 7 cases to show that $\langle \chi_i, \chi_j \rangle = \delta_{ij}$ for $i, j = 1, 2, 3$. It turns out that this is merely one instance of a more general orthogonality phenomenon. We will understand this better in the next subsection.

2.1.3 The Orthogonality Theorem

In this subsection, we dive into the heart of Character Theory, proving one of the most fundamental results in the field: the Orthogonality Theorem. This theorem generalises the orthogonality that we observed in Example 2.1.12, and has several important consequences, most notably the fact that the irreducible characters of a group form an orthonormal basis for the space of class functions on that group, a result we will see in the next subsection.

First, we state and prove a useful lemma that helps us understand the *matrices* of irreducible representations (taken, as per convention, with respect to the standard basis of $\mathbb{C}^n$). The point of this is that matrices are more computation-friendly.

Lemma 2.1.13. *Let $\rho : G \to \mathrm{GL}(n, \mathbb{C})$ and $\rho' : G \to \mathrm{GL}(m, \mathbb{C})$ be irreducible representations of G over $\mathbb{C}$. Fix $j, s \in \{1, \ldots, m\}$ and $r, i \in \{1, \ldots, n\}$.*

1. *If ρ and ρ' are not equivalent, then*

$$\frac{1}{|G|} \sum_{g \in G} [\rho(g)]_{ri} \left[\rho'(g^{-1})\right]_{js} = 0$$

2. *If ρ and ρ' are equivalent, then*

$$\frac{1}{|G|}\sum_{g\in G}[\rho(g)]_{ri}\left[\rho'(g^{-1})\right]_{js}=\begin{cases}\frac{1}{n} & \textit{if } i=j \textit{ and } r=s\\ 0 & \textit{otherwise}\end{cases}$$

where we use the notation $[T]_{ij}$ to refer to the ijth entry of the matrix of any $T\in \mathrm{GL}(n,\mathbb{C})$ with respect to the standard basis of $\mathbb{C}^n$.

Proof. Let $V=\mathbb{C}^n$ and $W=\mathbb{C}^m$ be the two simple $\mathbb{C}G$-modules corresponding to ρ and ρ' respectively. The idea is to define a linear map that will allow us to use Schur's Lemmas—specifically, those pertaining to finite groups over $\mathbb{C}$ (see Theorem 1.3.9).

Let $\phi_{ij}: W\to V$ be the $\mathbb{C}$-linear map given by the $n\times m$ matrix (with respect to the standard bases of V and W) with ijth entry 1 and all other entries 0. In other words, let ϕ_{ij} denote the ijth element of the standard basis of the space of linear maps from V to W. Define

$$\widehat{\phi_{ij}}:=\frac{1}{|G|}\sum_{g\in G}\rho(g)\circ\phi_{ij}\circ\rho'(g^{-1})$$

By Theorem 1.3.9, $\widehat{\phi_{ij}}$ is a $\mathbb{C}G$-module homomorphism from W to V. Indeed, we have that

$$\begin{aligned}\left[\widehat{\phi_{ij}}\right]_{rs}&=\left[\frac{1}{|G|}\sum_{g\in G}\rho(g)\circ\phi_{ij}\circ\rho'(g^{-1})\right]_{rs}\\&=\frac{1}{|G|}\sum_{g\in G}\left[\rho(g)\circ\phi_{ij}\circ\rho'(g^{-1})\right]_{rs}\\&=\sum_{k=1}^{n}\sum_{l=1}^{m}\frac{1}{|G|}\sum_{g\in G}[\rho(g)]_{rk}\,[\phi_{ij}]_{kl}\left[\rho'(g^{-1})\right]_{ls}\\&=\frac{1}{|G|}\sum_{g\in G}[\rho(g)]_{ri}\left[\rho'(g^{-1})\right]_{js}\end{aligned}$$

1. If $W\ncong V$, we have $\widehat{\phi_{ij}}=0$. In particular,

$$\frac{1}{|G|}\sum_{g\in G}[\rho(g)]_{ri}\left[\rho'(g^{-1})\right]_{js}=\left[\widehat{\phi_{ij}}\right]_{rs}=0$$

2. Similarly, if $W\cong V$, we have $m=n$. Now, by Theorem 1.3.9, we know that

$$\widehat{\phi_{ij}}=\frac{1}{n}\operatorname{Tr}(\phi_{ij})\cdot \mathrm{id}_V=\frac{1}{n}\delta_{ij}\cdot\mathrm{id}_V$$

We then have that

$$[\rho(g)]_{ri}\left[\rho'(g^{-1})\right]_{js}=\left[\widehat{\phi_{ij}}\right]_{rs}=\begin{cases}\frac{1}{n} & \text{if } i=j \text{ and } r=s\\ 0 & \text{otherwise}\end{cases}$$

□

Remark. As per Dr. Rizzoli, on the exam, it's more important to know the idea of such a proof than the specifics of *which index goes where*.

It turns out that by simply unfolding a few definitions and playing with the order of summations, we can use the above lemma to prove the Orthogonality Theorem.

Theorem 2.1.14 (Orthogonality Theorem). *Let S, T be irreducible $\mathbb{C}G$-modules.*

1. *If $S \ncong T$, then $\langle \chi_S, \chi_T \rangle = 0$.*
2. *If $S \cong T$, then $\langle \chi_S, \chi_T \rangle = 1$*

In other words, irreducible characters form an orthogonal system.

Proof. Let $P : G \to \mathrm{GL}(n, \mathbb{C})$ and $Q : G \to \mathrm{GL}(m, \mathbb{C})$ be the representations corresponding to S and T. We know that

$$\begin{aligned}\langle \chi_S, \chi_T\rangle &= \frac{1}{|G|}\sum_{G\in G}\chi_S(g)\chi_T(g^{-1})\\ &= \frac{1}{|G|}\sum_{g\in G}\mathrm{Tr}(P(g))\,\mathrm{Tr}(Q(g^{-1}))\\ &= \frac{1}{|G|}\sum_{g\in G}\left(\sum_{i=1}^{n}[P(g)]_{ii}\right)\left(\sum_{j=1}^{n}\left[Q(g^{-1})\right]_{jj}\right)\\ &= \sum_{i=1}^{n}\sum_{j=1}^{m}\frac{1}{|G|}\sum_{g\in G}[P(g)]_{ii}\left[Q(g^{-1})\right]_{jj}\end{aligned}$$

We can now use Lemma 2.1.13 to evaluate this sum.

1. If $S \ncong T$, then

$$\frac{1}{|G|}\sum_{g\in G}[P(g)]_{ii}\left[Q(g^{-1})\right]_{jj}=0$$

for all $1 \leq i \leq n$ and $1 \leq j \leq m$. Hence,

$$\langle \chi_S, \chi_T \rangle = \sum_{i=1}^{n} \sum_{j=1}^{m} 0 = 0$$

2. If $S \cong T$, then first of all, $n = m$. Indeed,

$$\frac{1}{|G|} \sum_{g \in G} [P(g)]_{ii} \left[Q\left(g^{-1}\right)\right]_{jj} = \begin{cases} \frac{1}{n} & \text{if } i = j \\ 0 & \text{otherwise} \end{cases}$$

for all $1 \leq i, j \leq n$. Hence,

$$\langle \chi_S, \chi_T \rangle = \sum_{i=1}^{n} \sum_{j=1}^{n} \frac{1}{n} \delta_{ij} = \sum_{i=1}^{n} \frac{1}{n} = 1$$

□

We have the following important corollary.

Corollary 2.1.15. *Up to isomorphism, there are finitely many irreducible $\mathbb{C}G$-modules.*

Proof. Suppose there exist infinitely many, pairwise nonisomorphic $\mathbb{C}G$-modules. Then, the (infinite) subset of $\mathcal{F}(G, \mathbb{C})$ consisting of all of their characters would be pairwise orthogonal (by Theorem 2.1.14). Since orthogonality implies linear independence, this set would need to be contained in a basis of $\mathcal{F}(G, \mathbb{C})$. However, by Proposition 2.1.4, such a basis would need to be finite, leading to a clear contradiction. Hence, there can only exist finitely many $\mathbb{C}G$-modules (up to isomorphism). □

2.1.4 Understanding Irreducible Characters

In this subsection, we will explore the properties of irreducible characters in more detail. In particular, we will see that they form a basis for the space of class functions on G. This is a very important result, which illustrates the power of character theory in understanding the properties of a group. We will begin by introducing some notation and stating a few basic properties of irreducible characters that will be useful in the proof of the main result.

Notation (Irreducible Characters)**.** Denote by $\mathrm{Irr}(G)$ the subset of $\mathcal{F}_C(G, \mathbb{C})$ consisting of irreducible characters of G.

The Orthogonality Theorem tells us the following facts about Irreducible Characters.

Proposition 2.1.16 (On the Behaviour of Irreducible Characters)**.**

1. $\mathrm{Irr}(G)$ *is a linearly independent set. In particular,* $|\mathrm{Irr}(G)| \leq |G|$.
2. *Let* $V = V_1 \oplus \cdots \oplus V_r$ *be a* $\mathbb{C}G$ *module, with* V_i *simple for* $1 \leq i \leq r$*. For any simple* $\mathbb{C}G$ *module* S*, the number of* V_i*s isomorphic to* S*, known as the* multiplicity *of* S*, is given by* $\langle \chi_V, \chi_S \rangle$.
3. *Let* V, V' *be simple* $\mathbb{C}G$*-modules. Then,* $V \cong V' \iff \chi_V = \chi_{V'}$.
4. *A* $\mathbb{C}G$*-module* V *is simple iff* $\langle \chi_V, \chi_V \rangle = 1$.

Proof.

1. The linear independence follows immediately from the fact that $\mathrm{Irr}(G)$ form an orthonormal system. The inequality follows from the fact that all central functions are class functions: they agree for all conjugate elements of G. This means that $\dim(\mathcal{F}_C(G, \mathbb{C}))$ is simply the number of conjugacy classes of G. Since $\dim(\mathcal{F}_C(G, \mathbb{C}))$ must be at least $|\mathrm{Irr}(G)|$ and the number of conjugacy classes of G must be at most $|G|$, we have the desired result.

2. We know, from Proposition 2.1.10, that $\chi_V = \chi_{V_1} + \cdots + \chi_{V_r}$. So,

$$\begin{aligned} \langle \chi_V, \chi_S \rangle &= \langle \chi_{V_1} + \cdots + \chi_{V_r}, \chi_S \rangle \\ &= \sum_{i=1}^{r} \langle \chi_{V_i}, \chi_S \rangle \end{aligned}$$

   Observe that for $1 \leq i \leq r$, $\langle \chi_{V_i}, \chi_S \rangle = 1$ if $V_i \cong S$ and 0 otherwise. Hence, the only nonzero terms in the summation are given by those i for which $V_i \cong S$. Since all of those terms are 1, the sum must evaluate to the multiplicity of S.

3. ($\implies$) This is true regardless of the simplicity of V and V' (cf. Proposition 2.1.10).

   ($\impliedby$) This turns out to be a straightforward application of the previous part. Let $W =$

$V \oplus V'$. Then, the multiplicity of V is given by

$$\langle \chi_W, \chi_V \rangle = \langle \chi_V + \chi_{V'}, \chi_V \rangle = \langle \chi_V, \chi_V \rangle + \langle \chi_{V'}, \chi_V \rangle = 2 \langle \chi_V, \chi_V \rangle = 2$$

This means that there are two terms in the decomposition $W = V \oplus V'$ that are isomorphic to V, which is only possible if $V \cong V'$.

4. ($\implies$) This follows immediately from the Orthogonality Theorem.

($\impliedby$) Let $\text{Irr}(G) = \{\chi_1, \dots, \chi_r\}$, with corresponding simple $\mathbb{C}G$-modules $\{V_1, \dots, V_r\}$. Denoting by a_i the multiplicity of each V_i in V, we have that

$$V = V_1^{\oplus a_1} \oplus \cdots \oplus V_r^{\oplus a_r}$$

where we use the notation $V_i^{\oplus a_i}$ to mean $\underbrace{V_i \oplus \cdots \oplus V_i}_{a_i \text{ times}}$, allowing $a_i = 0$.

We then have

$$\begin{aligned} \chi_V &= \sum_{i=1}^{r} a_i \chi_i \\ \implies \langle \chi_V, \chi_V \rangle &= \sum_{i=1}^{r} a_i^2 \end{aligned}$$

by the Orthogonality Theorem. Since $\langle \chi_V, \chi_V \rangle = 1$, it must be that only one of the a_is is nonzero, and equal to 1. Hence, $V = V_i$ for this i, making V simple.

□

We now have everything we need to prove the following important theorem.

Theorem 2.1.17. $\text{Irr}(G)$ *is a basis for* $\mathcal{F}_C(G, \mathbb{C})$.

Proof. As $\text{Irr}(G)$ is linearly independent, we only need to show that it spans $\mathcal{F}_C(G, \mathbb{C})$. To that end, let $W = \text{Span}(\text{Irr}(G)) \leq \mathcal{F}_C(G, \mathbb{C})$, with orthogonal complement $W^\perp$ with respect to the inner-product (2.1.1). Since $V = W \oplus W^\perp$, if we can show that $W^\perp = \{0\}$, we would have that $V = W$, proving the desired result.

Fix $f \in W^{\perp}$, and consider the element $\widehat{f} \in \mathbb{C}G$ given by

$$\widehat{f} = \sum_{g \in G} \overline{f(g)} \cdot g$$

First, we show that $\widehat{f} \in \mathrm{Z}(\mathbb{C}G)$—ie, that $\widehat{f}$ commutes (multiplicatively) with all elements of $\mathbb{C}G$. To show this, it suffices to show that $h^{-1}\widehat{f}h = \widehat{f}$ for all $h \in G$ (ie, that $\widehat{f}$ commutes with all elements of G). To that end, fix $h \in G$. Then,

$$\begin{aligned} h^{-1}\widehat{f}h &= \sum_{g \in G} \overline{f(g)} \cdot h^{-1}gh \\ &= \sum_{g \in G} \overline{f(h^{-1}gh)} \cdot h^{-1}gh \\ &= \widehat{f} \end{aligned}$$

where the first equality follows from the fact that $\overline{f(g)} \in \mathbb{C}$, thereby commuting with all elements of g in $\mathbb{C}G$; the second equality from the fact that f is central (recall that $W, W^{\perp} \leq \mathcal{F}_C(G, \mathbb{C})$); and last equality from a change of variables in the summation, replacing g with hgh^{-1}.

Now, let S be any simple $\mathbb{C}G$-module. One can show that the map

$$\phi : S \to S : v \mapsto \widehat{f} \cdot v$$

is a $\mathbb{C}G$-module homomorphism. Now, in the notation of (1.3.1), consider the map $\widehat{\phi} : S \to S$. Since $\widehat{f} \in \mathrm{Z}(\mathbb{C}G)$, we have that for all $v \in V$,

$$\begin{aligned} \widehat{\phi}(v) &= \frac{1}{|G|} \sum_{g \in G} g \cdot \phi(g^{-1} \cdot v) \\ &= \frac{1}{|G|} \sum_{g \in G} g\widehat{f}g^{-1} \cdot v \\ &= \frac{1}{|G|} \sum_{g \in G} \widehat{f} \cdot v \\ &= \widehat{f} \cdot v = \phi(v) \end{aligned}$$

proving that $\widehat{\phi} = \phi$. Then, by Theorem 1.3.9, we have that

$$\phi = \widehat{\phi} = \frac{\mathrm{Tr}(\phi)}{\dim(S)} \cdot \mathrm{id}$$

Indeed,

$$\begin{aligned}\mathrm{Tr}(\phi) &= \dim(S)\cdot\mathrm{Tr}\left(\sum_{g\in G}\overline{f(g)}\cdot g|_S\right)\\ &= \sum_{g\in G}\overline{f(g)}\chi_S(g)\\ &= |G|\left\langle \underbrace{\chi_S}_{\in W}, \underbrace{f}_{\in W^\perp}\right\rangle = 0\end{aligned}$$

proving that in fact, $\widehat{f}|_S = 0$.

`sorry` □

2.2 Character Tables

2.2.1 The Orthogonality Relations

For the purposes of this subsection, let $C_1, \dots, C_k$ be the conjugacy classes of G with representatives $g_1, \dots, g_k$ respectively. Recall that by the Orbit-Stabiliser Theorem,

$$|C_i| = \frac{|G|}{|C_G(g_i)|}$$

where $C_G(\cdot)$ refers to the centraliser[2] of an element in G. Now, let $\mathrm{Irr}(G) = \{\chi_1, \dots, \chi_k\}$.

Definition 2.2.1 (Character Table)**.** A character table is a $k \times k$ table whose columns are the conjugacy classes (or their representatives) and whose rows are the irreducible characters. In other words, it is a table whose (i, j)th entry is $\chi_i(g_j)$.

We now have the following important result that lets us check orthogonality as we go across the columns.

[2] Recall that the centraliser of a group element is the set of all elements that commute with it.

Proposition 2.2.2 (First Orthogonality Relation). *Given $1 \leq r, s \leq k$, we have*

$$\frac{1}{|G|}\sum_{j=1}^{k} |C_j|\, \chi_r(g_j)\, \chi_s(g_j^{-1}) = \delta_{rs}$$

Proof. Observe that

$$\begin{aligned}\delta_{rs} &= \langle \chi_r, \chi_s \rangle \\ &= \frac{1}{|G|}\sum_{g\in G} \chi_r(g)\chi_s(g^{-1}) \\ &= \frac{1}{|G|}\sum_{j=1}^{k}\left(\sum_{g\in C_i} \chi_r(g)\chi_s(g^{-1})\right) \\ &= \frac{1}{|G|}\sum_{j=1}^{k} |C_j|\, \chi_r(g_j)\, \chi_s(g_j^{-1})\end{aligned}$$

where the last inequality follows from the fact that characters are central (ie, they are equal for all elements of a conjugacy class). □

We can use this to prove an important result about the regular representation.

Theorem 2.2.3. *Let χ_{reg} denote the character of the regular representation of G over $\mathbb{C}$. Then,*

$$\chi_{\text{reg}} = \sum_{j=1}^{k} \chi_j(1)\, \chi_j$$

Proof. `sorry` □

Corollary 2.2.4. $\sum_{i=1}^{k} (\chi_i(1))^2 = |G|$.

Proof. $\chi_{\text{reg}}(1) = \sum_{i=1}^{k} (\chi_i(1))^2 = |G|$. □

We now have a similar result about going down the rows.

Proposition 2.2.5 (Second Orthogonality Relation). *Given $1 \leq r, s \leq k$, we have*

$$\sum_{i=1}^{k} \chi_i(g_r)\, \chi_i(g_s^{-1}) = \begin{cases} 0 & \text{if } r \neq s \\ |C_G(g_r)| & \text{if } r = s \end{cases}$$

Proof. Let A be the matrix $(A_{ij})_{ij}$, where $A_{ij} := \chi_i(g_j)$. Similarly, let B be the matrix $(B_{ij})_{ij}$, where $B_{ij} := \frac{|C_i|}{|G|}\chi_j(g_i^{-1})$. Then, writing $AB = (AB)_{pq}$, we have

$$\begin{aligned} (AB)_{pq} &= \sum_{l=1}^{k} A_{pl}B_{lq} \\ &= \sum_{l=1}^{k} \chi_p(g_l)\, \frac{|C_l|}{|G|} \chi_q(g_l^{-1}) \\ &= \langle \chi_p, \chi_q \rangle = \delta_{pq} \end{aligned}$$

This proves that in fact, $AB = I$, the identity matrix. This, in particular, means that $BA = I$ as well. It turns out that setting $\delta_{pq} = (BA)_{pq}$ gives us the desired result. □

2.2.2 Character Tables of Symmetric Groups

Example 2.2.6 (S_3). S_3 has precisely three conjugacy classes C_1, C_2 and C_3 with representatives $g_1 = 1$, $g_2 = (12)$ and $g_3 = (123)$. We then have the following character table for S_3:

	1	(12)	(123)
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

Here, χ_1 corresponds to the trivial representation (of degree 1), χ_2 to the sign representation (of degree 1), and χ_3 to the subrepresentation $W = \operatorname{Span}(e_1 - e_2, e_1 - e_3)$ (of degree 2) of the permutation representation on $\mathbb{C}^3$. Note that all of these representations are irreducible, the first two because their degrees are 1, and the third because we can show $\langle \chi_W, \chi_W \rangle$ to be equal to 1 (cf. the fourth point of Proposition 2.1.16).

Example 2.2.7 (S_4)**.** Observe that the conjugacy classes C_i, $i = 1, \dots, 5$, of S_4 correspond precisely to the various possible cycle shapes. They therefore have representatives $g_1 = 1$, $g_2 = (12)$, $g_3 = (123)$, $g_4 = (12)(34)$, and $g_5 = (1234)$. The conjugacy classes have sizes 1, 6, 8, 3 and 6 respectively.

We then have the following character table for S_4:

	1	(12)	(123)	(12)(34)	(1234)
χ_1	1	1	1	1	1
χ_2	1	-1	1	1	-1
χ_3	3	1	0	-1	-1
χ_4	2	0	-1	2	0
χ_5	a	b	c	d	e

where the characters χ_i are as follows:

1. χ_1 is the trivial character.
2. χ_2 is the sign character[a].
3. χ_3 is the deleted permutation character given by the subrepresentation of the permutation representation[b] of S_4 corresponding to $\mathrm{Span}(e_1 - e_2, e_2 - e_3, e_3 - e_4)$, an S_4-invariant subspace of $\mathbb{C}^4$.
4. χ_4 is given by the following construction. Consider

$$N = \{1, (12)(34), (13)(24), (14)(23)\} \trianglelefteq S_4$$

One can show that ${}^{S_4}\!/_{N} \cong S_3$. Let $\pi : S_4 \twoheadrightarrow S_3$ be the associated quotient map. Then, if $\rho : S_3 \to \mathrm{GL}(2, \mathbb{C})$ is a 2-dimensional irreducible representation of S_3, then the map $\rho' := \rho \circ \pi : S_4 \to \mathrm{GL}(2, \mathbb{C})$ is also irreducible. We take χ_4 to be the associated character.

5. χ_5 is the regular character[c]. We can actually solve for a, b, c, d, e using the Orthogonality Relations. From Corollary 2.2.4, we know that

$$1 + 1 + 9 + 4 + a^2 = 24 = |S_4|$$

from which we can conclude that $a = 3$. Then, using the First Orthonality Relation

(Proposition ??), we can see that

$$1 - 1 + 3 + 0 + ab = 0$$

from which we can conclude that $b = -1$.

`sorry`

[a] ie, that corresponding to the sign representation
[b] ie, that corresponding to its action on $\mathbb{C}^4$ by permuting the standard basis
[c] ie, that corresponding to the regular representation

Note that the number of irreducible characters of degree 1 of any group G is $|G| / |G'|$, where G' is the derived subgroup of G. Indeed, there is a one-to-one correspondence between degree 1 irreducible characters of G and those of ${}^{G}\!/\!{}_{G'}$.

It turns out that we can glean even more information about groups from their characters, for which we will need the properties of the algebraic integers.

2.3 Integrality

2.3.1 The Algebraic Integers

First, we recall the notion of integrality over an integral domain.

Definition 2.3.1 (Integrality). Let R be an integral domain, and $S \supset R$ an extension. We say that $s \in S$ is integral over R if one of the following equivalent conditions is satisfied:

- s is a root of a monic polynomial in $R[X]$.
- The minimal polynomial of s over $\mathrm{Frac}(R)$ is actually in $R[X]$.

We now define what it means for a complex number to be an algebraic integer.

Definition 2.3.2 (Algebraic Integer). We say that a number $\alpha \in \mathbb{C}$ is an algebraic integer if it is integral over $\mathbb{Z}$.

Notation. Given a conjugacy class C of G, we define

$$\widehat{C} := \sum_{g \in C} g \tag{2.3.1}$$

to be an element of $\mathbb{C}G$.

Lemma 2.3.3. *Let $g \in G$ and let $C = g^G$ Let S be a simple $\mathbb{C}G$-module. Then, for all $s \in S$, we have an action by scalar multiplication*

$$\widehat{C} \cdot s = \lambda s$$

where $\lambda = \dfrac{|C|}{|C_G(g)|} \dfrac{\chi(g)}{\chi_s(1)} = |C| \dfrac{\chi_s(g)}{\chi_s(1)}$.

Proof. Define a function $\phi : S \to S : s \mapsto \widehat{C} \cdot s$. Since $\widehat{C} \in \mathrm{Z}(\mathbb{C}G)$, we have that $\forall x \in G$, $x \cdot \phi(s) = \phi(x \cdot s)$. This makes ϕ a $\mathbb{C}G$-module homomorphism. Then, by Schur's Lemmas, we know that $\phi = \lambda \, \mathrm{id}$. This means that... □

Lemma 2.3.4. *Let $r = \sum_{g \in G} \alpha_g g$ for some $\alpha_g \in \mathbb{Z}$. Suppose that $\exists \lambda, v \in \mathbb{C}G \setminus \{0\}$ such that $rv = \lambda v$. Then, λ is an algebraic integer.*

Proof. Let $G = \{g_1, \ldots, g_n\}$. For all $1 \leq i \leq n$,

$$rg_i = \sum_{j=1}^{n} \alpha_{ij} g_j$$

The key observation here is that $\alpha_{ij} \in \mathbb{Z}$ for all $1 \leq i, j \leq n$. Then, if $rv = \lambda v$, we have that λ is an eigenvalue of the matrix $A := (\alpha_{ij})_{1 \leq i,j \leq n} \in \mathrm{M}_{n \times n}(\mathbb{Z})$. This makes λ a root of the characteristic polynomial of A (over $\mathbb{Z}$), which is monic and of degree n. □

The point of lemmas 1 and 2 is the following Corollary, the proof of which is trivial:

Corollary 2.3.5. *For any $\chi \in \mathrm{Irr}(G)$ and $g \in G$, the quantity $\lambda = \frac{|G|}{|C_G(g)|} \frac{\chi(g)}{\chi(1)}$ is an algebraic integer.*

This leads us to the following important connection between algebraic integers and irreducible representations.

Theorem 2.3.6. *For all $\chi \in \operatorname{Irr}(G)$, $\chi(1) \mid |G|$.*

Proof. `Check phone` □

2.3.2 The *n*th Roots of Unity

Lemma 2.3.7. *Let w be an nth root of unity in $\mathbb{C}$. Then,*

$$\sum_{1 \leq i \leq m, (i,n)=1} w^i \in \mathbb{Z}$$

Proof. EXERCISE. Hint: induction on n. □

Proposition 2.3.8. *Let $g \in G$ be of order n. Suppose that g^i is conjugate to g for all $1 \leq i \leq n$ such that $(i, n) = 1$. Then, for all characters χ of G, $\chi(g)$ is an integer.*

Proof. Let χ be a character of G, with associated representation (V, ρ) of degree m over $\mathbb{C}$. We know that $\chi(g) = \sum_{i=1}^m w_i$, where each w_i is an nth root of unity (cf. Proposition 2.1.10). Indeed, the idempotent linear map $\rho(g)$ is diagonalisable, with matrix $\operatorname{diag}(w_1, \ldots, w_m)$ with respect to an appropriate basis. Hence, we have that $\rho(g^i) = \operatorname{diag}\big(w_1^i, \ldots, w_m^i\big)$, meaning that $\chi(g^i) = \sum_{j=1}^m w_j^i$. But this is nothing but $\sum_{1 \leq i \leq m, (i,n)=1} w^i$, by assumption. Hence, $\chi(g)$ is an integer, by Lemma 2.3.7. □

Lemma 2.3.9. *Fix $g \in G$, and let p be a prime number. Then, $\exists! x, y \in G$ such that*

1. $g = xy = yx$
2. $\operatorname{ord}(x) = p^k$ *for some* $k \in \mathbb{N}$
3. $(\operatorname{ord}(y), p) = 1$

Proof. Let $\operatorname{ord}(g) = up^v$, where $(u, v = 1)$. By Bézout's Lemma, we know that $\exists a, b \in \mathbb{Z}$ such that $au + bp^v = 1$. Then, we can define $x = g^{au}$ and $y = g^{bp^v}$. This satisfies all the conditions:

1. $g = xy = g^{au} g^{bp^v} = g^{bp^v} g^{au} = yx$.

2. $x^{p^v} = 1$.

3. $y^v = 1$.

One can also show x and y to be the only elements of G satisfying these conditions. □

Definition 2.3.10 (The p- p'-parts of g)**.** For any $g \in G$, call x and y from Lemma 2.3.9 the p- and p'-parts of g respectively.

For the remainder of this subsection, let $n = |G|$, and let $\zeta = e^{\frac{2\pi i}{n}}$ be a primitive nth root of unity. Define $\mathbb{Z}[\zeta]$ to be the subring of $\mathbb{C}$ generated by $\mathbb{Z}$ and ζ. Let p be a prime number and $p\mathbb{Z}[\zeta]$ be the principal ideal of $\mathbb{Z}[\zeta]$ generated by p. By the Correspondence Theorem, the ideals of $\mathbb{Z}[\zeta]$ containing $p\mathbb{Z}[\zeta]$ are in bijection with the ideals of ${\mathbb{Z}[\zeta]}\big/{p\mathbb{Z}[\zeta]}$. Since the latter object is finite, it contains finitely many ideals, meaning that only finitely many of the ideals of $\mathbb{Z}[\zeta]$ contain $p\mathbb{Z}[\zeta]$. We can then look at the maximal (proper) ideal amongst these, which is a maximal ideal of $\mathbb{Z}[\zeta]$. Denote it by P. Indeed, we can show that $P \cap \mathbb{Z} = p\mathbb{Z}$.

Theorem 2.3.11. *Let $g \in G$, and let y be the p'-part of g for some p prime. For all characters χ of G, $\chi(g) - \chi(y)$ lies in the maximal ideal P.*

Proof. Let $m = \operatorname{ord}(g) = up^v$. Let $a, b \in \mathbb{Z}$ be such that $au + bp^v = 1$ (as in the proof of Lemma 2.3.9). We have that $y = g^{bp^v}$. We know that $\chi(g), \chi(y) \in \mathbb{Z}[\zeta]$.

Now, let w be an mth root of unity. Since $m|n$ (by Lagrange's Theorem), we know that $w \in \mathbb{Z}[\zeta]$. We have that $w = w^{au+bp^v}$. Raising both sides to the p^vth power, we get that $w^{p^v} = w^{aup^v} w^{bp^{2v}}$. Since $w^{up^v} = w^m = 1$, we have that $w^{p^v} = w^{bp^{2v}}$.

Now, consider the binomial expansion of $\left(w - w^{bp^v}\right)^{p^v}$. Some blah blah, use fact that P is a prime ideal (since it is maximal). □

This theorem has several important consequences.

Corollary 2.3.12. *Let $g \in G$ and y be the p'-part of g for some prime p. Let χ be a character of G.*

1. *If $\chi(g), \chi(y) \in \mathbb{Z}$, then $\chi(g) \equiv \chi(y) \pmod{p}$.*

2. *If* $\mathrm{ord}(g) = p^k$ *for some* $k \in \mathbb{N}$, *then* $\chi(g) \equiv \chi(1) \pmod{p}$.

Lemma 2.3.13. *Let* $g, h \in G$. *Then,* g *is conjugate to* h *iff for all characters* χ *of* G, $\chi(g) = \chi(h)$.

Proof.

$(\implies)$ Seen Before

$(\impliedby)$ As we know, $\mathrm{Irr}(G)$ is an orthonormal basis for $\mathcal{F}_C(G, \mathbb{C})$. Let f be the indicator function on g^G. Then, $f(g) = 1 \implies f(h) = 1 \implies h \in g^G$.

□

Corollary 2.3.14. *Let* $g \in G$. *Then,* g *is conjugate to* g^{-1} *iff for all characters* χ *of* G, $\chi(g) \in \mathbb{R}$.

Example 2.3.15 (Constructing the Character Table of $G = \mathrm{PSL}(2, 7)$). First, note that $|G| = 168$ and that G has 6 conjugacy classes. Denote them by $C_1, \ldots, C_6$ with representatives $g_1, \ldots, g_6$, with $g_1 = 1$. It turns out we have exactly 6 irreducible characters of G.

We begin filling the table as follows.

$C_G(g_i)$	168	8	4	3	7	7
$\mathrm{ord}(g_i)$	1	2	4	3	7	7
g_i	g_1	g_2	g_3	g_4	g_5	g_6
χ_1	1	1	1	1	1	1
χ_2						
χ_3						
χ_4						
χ_5						
χ_6						

We can then fill in the first column by applying Corollary 2.2.4.

$C_G(g_i)$	168	8	4	3	7	7
$\text{ord}(g_i)$	1	2	4	3	7	7
g_i	g_1	g_2	g_3	g_4	g_5	g_6
χ_1	1	1	1	1	1	1
χ_2	7					
χ_3	8					
χ_4	3					
χ_5	3					
χ_6	6					

Observe that since the orders are unique for the first four columns, they contain all elements of their respective orders. We can then fill in the third column by applying the Column Orthogonality Relation and the first Lemma from today.

$C_G(g_i)$	168	8	4	3	7	7
$\text{ord}(g_i)$	1	2	4	3	7	7
g_i	g_1	g_2	g_3	g_4	g_5	g_6
χ_1	1	1	1	1	1	1
χ_2	7		-1			
χ_3	8		0			
χ_4	3		1			
χ_5	3		1			
χ_6	6		0			

We can then fill in the fourth column using the second point of Corollary 2.3.11.

$C_G(g_i)$	168	8	4	3	7	7
$\text{ord}(g_i)$	1	2	4	3	7	7
g_i	g_1	g_2	g_3	g_4	g_5	g_6
χ_1	1	1	1	1	1	1
χ_2	7		-1	1		
χ_3	8		0	-1		
χ_4	3		1	0		
χ_5	3		1	0		
χ_6	6		0	0		

We now have four possibilities for the second column.

$C_G(g_i)$	168	8	4	3	7	7
$\mathrm{ord}(g_i)$	1	2	4	3	7	7
g_i	g_1	g_2	g_3	g_4	g_5	g_6
χ_1	1	1	1	1	1	1
χ_2	7		-1	1		
χ_3	8		0	-1		
χ_4	3		1	0		
χ_5	3		1	0		
χ_6	6		0	0		

$C_G(g_i)$	168	8	4	3	7	7
$\mathrm{ord}(g_i)$	1	2	4	3	7	7
g_i	g_1	g_2	g_3	g_4	g_5	g_6
χ_1	1	1	1	1	1	1
χ_2	7		-1	1		
χ_3	8		0	-1		
χ_4	3		1	0		
χ_5	3		1	0		
χ_6	6		0	0		

For the last two columns of the table, we use row orthogonality, in combination with the fact that $g_5 = g_6^{-1}$.

$C_G(g_i)$	168	8	4	3	7	7
$\mathrm{ord}(g_i)$	1	2	4	3	7	7
g_i	g_1	g_2	g_3	g_4	g_5	g_6
χ_1	1	1	1	1	1	1
χ_2	7		1	-1	0	0
χ_3	8		-1	0	1	1
χ_4			0	1	z	$\overline{z}$
χ_5	3		0	1	$\overline{z}$	z
χ_6	6		0	0	t	$\overline{t}$

FINAL COMMENTS. Also use the results on p groups, since G is a 7-group.

Chapter 3

Applications to the Study of Groups

Welcome to the third chapter.

3.1 First Examples

3.1.1 A Word on Simple Groups

First, we have an interesting result on p-groups.

Lemma 3.1.1. *Assume that $|G| = p^n$ for some p prime and $n \in \mathbb{N}$. Then, $\forall \chi \in \mathrm{Irr}(G)$, $\chi(1)$ is a power of p.*

Proof. Let $\mathrm{Irr}(G) = \{\chi_1, \dots, \chi_k\}$, with χ_1 being the trivial character. `sorry` □

Corollary 3.1.2. *If $|G| = p^2$ for some p prime, then $\forall \chi \in \mathrm{Irr}(G)$, $\chi(1) = 1$. In particular, G is abelian.*

Proof. `sorry` □

We now have an interesting result on the characters of simple groups.

Lemma 3.1.3. *If G is simple, G does not admit an irreducible character of degree 2.*

Proof. Suppose, for contradiction, that G is simple but admits an irreducible representation $\rho : G \to \mathrm{GL}(2, \mathbb{C})$. Since G is simple, we must have that $\ker(\rho) = \{1\}$.

If G is nonabelian, then $G' = G$. This tells us that there are no nontrivial characters of degree 1. Since the map $\rho \mapsto \det(\rho(g))$ a linear character (ie, has degree 1), we can conclude that $\det(\rho(g)) = 1$ for all $g \in G$. By Theorem 2.3.6, we know that $2 \mid |G|$. Then, by Cauchy's Theorem, $\exists g \in G$ such that $g \neq 1$ but $g^2 = 1$. This tells us that $\rho(g) = -\mathrm{id} \in Z(G)$, which is absurd, since G is simple. □

3.2 Burnside's Theorem

3.2.1 The Algebraic Numbers

In this subsection, we investigate a generalisation of the algebraic integers, whose properties will be useful in the proof of Burnside's Theorem. We begin with the following definition.

Definition 3.2.1 (Algebraic Numbers). An algebraic number is a complex number that is a root of a non-zero polynomial in $\mathbb{Q}[X]$.

Remark (A few recollections on the notion of a minimal polynomial). For any algebraic number x,

- There exists a *unique* monic polynomial of minimal degree over $\mathbb{Q}$ that annihilates x. This polynomial, denoted m_x, is called the *minimal polynomial* of x.

- m_x is irreducible.

- m_x divides any polynomial over $\mathbb{Q}$ for which x is a root.

Definition 3.2.2 (Conjugates of an Algebraic Number). Let x be an algebraic number. The conjugates of x are the roots of its mimimal polynomial, m_x.

Example 3.2.3. Fix $n \in \mathbb{N}$, and let ω be an nth root of unity. The minimal polynomial of ω divides $X^n - 1$, meaning that all of its roots are also nth roots of unity, and therefore, have modulus 1.

Indeed, it turns out that if a number is an algebraic integer, then its minimal polynomial actually has integer coefficients.

Lemma 3.2.4. *Let α, β be algebraic numbers, and let $r \in \mathbb{Q}$. Then,*

1. *The conjugates of $\alpha + \beta$*[1] *are all of the form $\alpha' + \beta'$, where α' and β' are conjugates of α and β respectively.*
2. *The conjugates of $r\alpha$, where $r \in \mathbb{Q}$, are all of the form $r\alpha'$, where α' is a conjugate of α.*

Proof sketch. Let L denote the splitting field over $\mathbb{Q}$ of m_α, m_β and $m_{\alpha+\beta}$. This is a normal extension of $\mathbb{Q}$ `[JUSTIFY]`. Now, let $G = \mathrm{Aut}(L/\mathbb{Q})$. One can show the action of G on the conjugates of α to be transitive `[JUSTIFY]`. For instance, one can show that $\mathbb{Q}(\alpha) \cong \mathbb{Q}(\alpha')$ `[relevance?]`. Then, for all $g \in G$, we have that $g(\alpha + \beta) = g(\alpha) + g(\beta)$, and $g(x)$ is a conjugate of x for any $x \in L$ (by transitivity). *I* think the transitivity/normality comes from the fact that L is the splitting field of irreducible polynomials. □

Lemma 3.2.5. *Let G be a finite group, and let χ be a character of G. Then, $\left|\frac{\chi(g)}{\chi(1)}\right| \leq 1$, and if $0 < \left|\frac{\chi(g)}{\chi(1)}\right| < 1$, then $\chi(g)/\chi(1)$ is not an algebraic integer.*

Proof. Let $\gamma = \frac{\chi(g)}{\chi(1)}$ and $d = \chi(1)$. Then, $\chi(g) = w_1 + \cdots + w_d$, where $|w_i| = 1$ for all i. This then gives us that $|\gamma| \leq 1$. Now, suppose that γ *is* an algebraic integer and that $|\gamma| < 1$. We show show that $\chi(g) = 0$.

Let m_γ be the minimal polynomial of γ. Then, $m_\gamma(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_0$. Since γ is an algebraic integer, we have that $a_i \in \mathbb{Z}$ for all i. By the previous lemma, we know that the conjugates of γ are of the form $\frac{w_1' + \cdots + w_d'}{d}$, where w_i' are conjugates of w_i. Since $|w_i| = 1$, we have that $|w_i'| = 1$ for all i.

Now, let z be the product of all the conjugates of γ—ie, the product of all the roots of m_γ. Then, $|z| < 1$. Indeed, $z = a_0$, and hence, in particular, $z \in \mathbb{Z}$. Therefore, it must be that $z = 0$. Hence, it must be that $m_\gamma(X) = X$, as it is irreducible. This gives us that $\gamma = 0$, and hence, $\chi(g) = 0$. □

[1] It is easy to see that $\alpha + \beta$ is algebraic.

3.2.2 The Three Versions of Burnside's Theorem

Theorem 3.2.6 (Burnside's Theorem for Simple Groups). *Let p be a prime number, and let $r \in \mathbb{Z}$ be greater than or equal to 1. Let G be a finite group which a conjugacy class of size p^r. Then, G is not simple.*

Proof. Let $g \in G$ be such that $\left|g^G\right| = p^r$. Note that since G contains a conjugacy class of size greater than 1, G cannot be abelian. Now, let $\mathrm{Irr}(G) = \{\chi_1, \dots, \chi_k\}$. The idea is to apply column orthogonality between the g-column and the 1-column of G.

By Proposition **??**, we have that

$$\begin{aligned} 0 &= \frac{1}{|G|}\sum_{i=1}^{k} \chi_i(g)\chi_i(1) \\ &= 1 + \frac{1}{|G|}\sum_{i=2}^{k} \chi_i(g)\chi_i(1) \end{aligned}$$

Dividing both sides by p, we get that

$$\sum_{i=2}^{k} \chi_i(g)\frac{\chi_i(1)}{p} = -\frac{1}{p}$$

Since $-1/p$ is not an algebraic integer, this implies that for some $2 \leq j \leq k$, $\chi_j(g)\frac{\chi_j(1)}{p}$ is not an algebraic integer. However, since $\chi_j(g)$ is necessarily an algebraic integer, it must be that $\chi_j(1)/p$ is not an algebraic integer. Since $\chi_j(1) \in \mathbb{Z}$ (as it is the degree of the associated representation) and p is prime, this is equivalent to saying that $p \nmid \chi_j(1)$. Since $\left|g^G\right| = p^r$, this means that $\chi_j(1)$ and $\left|g^G\right|$ are coprime.

We know, by Bézout's Lemma, that there exist integers a, b such that $a\left|g^G\right| + b\chi_j(1) = 1$. Multiplying by the character ratio $\gamma = \chi_j(g)/\chi_j(1)$, we have that

$$a\left|g^G\right|\gamma + b\chi_j(g) = \gamma$$

By Lemma 2.3.3 `(make reference more precise)`, we know that $a\left|g^G\right|\gamma$ is an algebraic integer. This means that γ must be an algebraic integer too, giving us that $|\gamma| = 1$ (by Lemma 3.2.5).

Now, let ρ be the representation wich character χ_j. Then, by Lemma 2.3.3, we have that $\rho(g) = \lambda I$, where $\lambda = \left|g^G\right| \gamma$. `Finish using picture on iPad.` □

Theorem 3.2.7 (Burnside's Theorem for Groups of Order $p^a q^b$). *Let G be a finite group of order $p^a q^b$, where p, q are prime numbers and $a, b \in \mathbb{N}$. Then, G is simple only if $|G| \in \{p, q\}$.*

Proof. First, suppose that $b = 0$. Then, G is a p-group, and hence, has a nontrivial centre.[2] This means that G is not simple unless $|G| = p$. One can prove similarly that if $a = 0$ then $|G| = q$.

Now, suppose that $a, b > 0$. Then, G has a normal Sylow p-subgroup P of order p^a for some $a \in \mathbb{N}$. Since P is a p-group, its centre is nontrivial, and therefore, there exists some $g \in Z(P) \setminus \{1\}$. Indeed,

$$\begin{aligned} P &\leq C_G(g) \\ \implies |P| &\mid |C_G(g)| = \frac{|G|}{|g^G|} \\ \implies p^a \left|g^G\right| &\mid p^a q^b \\ \implies \left|g^G\right| &\mid q^b \end{aligned}$$

where we justify the first inclusion by writing it out `[DO IT!]`.

Since G is simple, $Z(G) = \{1\}$, meaning that $\left|g^G\right| = q^r$ for some $r \geq 1$. This contradicts the simplicity of G. `[JUSTIFY!]` □

`Insert definition of solvable`

Theorem 3.2.8 (Burnside's Theorem for Solvable Groups). *Let G be a finite group. If G has order $p^a q^b$, where p, q are prime and $a, b \geq 0$, then G is solvable.*

Proof. We argue by induction on $|G|$. If $|G| = 1$, then G is trivially solvable. Now, suppose that

[2] Recall that the sizes of the conjugacy classes of a p-group are prime powers. One can then use the Class Equation to arrive at this result.

$|G| = p^a q^b$, where $a, b \geq 0$. If $a = 0$ or $b = 0$, then G is a p-group or a q-group, and hence, solvable.[3] Else, if $a, b \geq 1$, then by Theorem 3.2.7, we know that G is not simple. It then contains a nontrivial normal subgroup N. By the Induction Hypothesis, both N and ${}^{G}\!/_{N}$ are solvable, making G solvable as well. □

3.2.3 Applications of Burnside's Theorem

Lemma 3.2.9. *There are no nonabelian simple groups of order less than* 30.

[3] Give/link a proof of this!