NOTES ON REPRESENTATIONS OF FINITE GROUPS

AARON LANDESMAN

CONTENTS

1. Introduction 3
   1.1. Acknowledgements 3
   1.2. A first definition 3
   1.3. Examples 4
   1.4. Characters 7
   1.5. Character Tables and strange coincidences 8
2. Basic Properties of Representations 11
   2.1. Irreducible representations 12
   2.2. Direct sums 14
3. Desiderata and problems 16
   3.1. Desiderata 16
   3.2. Applications 17
   3.3. Dihedral Groups 17
   3.4. The Quaternion group 18
   3.5. Representations of $A_4$ 18
   3.6. Representations of $S_4$ 19
   3.7. Representations of $A_5$ 19
   3.8. Groups of order $p^3$ 20
   3.9. Further Challenge exercises 22
4. Complete Reducibility of Complex Representations 24
5. Schur’s Lemma 30
6. Isotypic Decomposition 32
   6.1. Proving uniqueness of isotypic decomposition 32
7. Homs and duals and tensors, Oh My! 35
   7.1. Homs of representations 35
   7.2. Duals of representations 35
   7.3. Tensors of representations 36
   7.4. Relations among dual, tensor, and hom 38
8. Orthogonality of Characters 41
   8.1. Reducing Theorem 8.1 to Proposition 8.6 41
   8.2. Projection operators 43
1. INTRODUCTION

Loosely speaking, representation theory is the study of groups acting on vector spaces. It is the natural intersection of group theory and linear algebra. In math, representation theory is the building block for subjects like Fourier analysis, while also the underpinning for abstract areas of number theory like the Langlands program. It appears crucially in the study of Lie groups, algebraic groups, matrix groups over finite fields, combinatorics, and algebraic geometry, just to name a few. In addition to great relevance in nearly all fields of mathematics, representation theory has many applications outside of mathematics. For example, it is used in chemistry to study the states of the hydrogen atom and in quantum mechanics to the simple harmonic oscillator.

To start, I’ll try and describe some examples of representations, and highlight some strange coincidences. Much of our goal through the course will be to prove that these “coincidences” are actually theorems.

1.1. Acknowledgements. I’d like to thank Noah Snyder for sending me some homework from a course he taught in representation theory. Many of his problems appear in these notes. In turn, some of those problems may have been taken from a class Noah took with Richard Taylor.

1.2. A first definition. To start, let’s begin by defining a representation so that we can hit the ground running. In order to define a representation, we’ll need some preliminary definitions to set up our notation.

Remark 1.1. Throughout these notes, we’ll adapt the following conventions:

1. Our vector spaces will be taken over a field \( k \). You should assume \( k = \mathbb{C} \) unless you are familiar with field theory, in particular the notion of characteristic and algebraically closed. (We will make explicit which assumptions we need on \( k \) when they come up. After a certain point, we will work over \( \mathbb{C} \).)

2. All vector spaces will be finite dimensional.

To start, we recall the definition of a group action.

Definition 1.2. For \( A \) and \( B \) two sets, we let \( \text{Hom}_{\text{sets}}(A, B) \) denote the set of maps from \( A \) to \( B \) and \( \text{Aut}_{\text{sets}}(A) := \text{Hom}_{\text{sets}}(A, A) \). For \( A \) and \( B \) two vector spaces over a field \( k \), we let \( \text{Hom}_{\text{vect}}(A, B) \) denote the set of linear maps from \( A \) to \( B \) and \( \text{Aut}_{\text{vect}}(A) := \text{Hom}_{\text{vect}}(A, A) \).

Remark 1.3. In general, \( A \) and \( B \) have extra structure, we will often let \( \text{Hom}(A, B) \) denote the set maps preserving that extra structure. In particular, when \( A \) and \( B \) are vector spaces, we will often use \( \text{Hom}(A, B) \) in place of \( \text{Hom}_{\text{vect}}(A, B) \) and similarly \( \text{Aut}(A) \) to denote \( \text{Aut}_{\text{vect}}(A) \).
Definition 1.4. Let $G$ be a group and $S$ be a set. An action of $G$ on $S$ is a map $\pi : G \to \text{Hom}(S, S)$ so that $\pi(e) = \text{id}_S$ and $\pi(g) \circ \pi(h) = \pi(g \cdot h)$, where $g, h \in G$, $s \in S$ and $e \in G$ is the identity.

Joke 1.5. Groups, like men, are judged by their actions.

We can now define a group representation.

Definition 1.6. Let $G$ be a group. A representation of $G$ (also called a $G$-representation, or just a representation) is a pair $(\pi, V)$ where $V$ is a vector space and $\pi : G \to \text{Hom}_{\text{vect}}(V, V)$ is a group action. I.e., an action on the set $V$ so that for each $g \in G$, $\pi(g) : V \to V$ is a linear map.

Remark 1.7. If you’re having trouble understanding the definition of a representation, a good way to think about it is an assignment of a matrix to every element of the group, in a way compatible with multiplication.

Exercise 1.8 (Easy exercise). If $g \in G$ has order $n$ so that $g^n = 1$, and $\pi : G \to \text{Aut}(V)$ is a representation, show that $\pi(g)$ is a matrix of order dividing $n$.

1.3. Examples. Let’s start by giving few examples of representations. The first one is rather trivial.

Example 1.9. Let $G$ be any group. Consider the representation $(\pi, V)$ where $V$ is a 1 dimensional vector space and every element of $G$ acts by the matrix (1). Formally, $\pi : G \to \text{Aut}(V)$ satisfies $\pi(g) = (1)$ for every $g \in G$. Said another way, $G$ acts as the identity map $V \to V$. This is a representation because for any $g, h \in G$,

$$\pi(g)\pi(h) = (1) \cdot (1) = (1) = \pi(gh).$$

This is called the trivial representation and we denote it by triv.

Let’s see a couple more examples of representations on a 1-dimensional vector space.

Remark 1.10. We refer to representations on an $n$-dimensional vector space as $n$-dimensional representations. Further, for $(\pi, V)$ a representation, we often refer to the representation simply as $\pi$ when or $V$ when clear from context. We call a representation $(\pi, V)$ a complex representation if $V$ is a vector space over the complex numbers. Similarly, we say the representation is a real representation if $V$ is a vector space is over the real numbers.

Example 1.11. Consider the 1-dimensional complex representation $(\pi, V)$ of the group $\mathbb{Z}/2 = \{i, \text{id}\}$ (with $i$ the nontrivial element $i \in \mathbb{Z}/2$) defined by $\pi(i) = \times(-1)$. In other words, $\pi(i)(v) = -v$. 
Exercise 1.12 (Easy exercise). Verify the representation of Example 1.11 is indeed a representation.

We refer to this as the sign representation and denote it by $\text{sgn}$.

Example 1.13. Consider the 1-dimensional representation of $\mathbb{Z}/3$ on the complex numbers defined as follows: Let $x$ be a generator for $\mathbb{Z}/3$ so that $\mathbb{Z}/3 = \{ x, x^2, \text{id} \}$. Define $(\pi, \mathbb{C})$ by $\pi(x) = (\omega)$ for $\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ a cube root of unity. This forces $\pi(x^2) = (\omega^2)$, and, as always, $\pi(\text{id}) = (1)$. Here we use parenthesis around a complex number to denote a $1 \times 1$ matrix, which is the element of $\text{Aut}(\mathbb{C})$ given by multiplication by the entry.

There is another representation, which we call given by $\pi(x) = \omega^2$ and $\pi(x^2) = \omega$.

Exercise 1.14. Generalizing Example 1.13 For $n$ an integer, construct $n$ different representations of $\mathbb{Z}/n$ on $\mathbb{C}$ (i.e., construct action maps $\pi : \mathbb{Z}/n \to \text{Aut}(\mathbb{C})$) and prove these are indeed representations. Hint: For each of the $n$ possible roots of unity $\zeta$ with $\zeta^n = 1$, send a generator of $\mathbb{Z}/n$ to the linear transformation $\mathbb{C} \to \mathbb{C}$ given by $x \mapsto \zeta \cdot x$.

The following example is more complicated, but prototypical.

Example 1.15. Let $V$ denote the complex numbers, considered as a 2-dimensional $\mathbb{R}$-vector space with basis $\{ 1, i \}$. Consider the triangle with vertices at the three cube roots of unity. Explicitly, vertex 1 is at $(1,0)$ vertex 2 is at $(-1/2, \sqrt{3}/2)$ and vertex 3 is at $(-1/2, -\sqrt{3}/2)$. See Figure 1 for a picture.

Then, there is a group action of the symmetric group on three elements, $S_3$, permuting the three vertices of the triangle. In fact, this action can be realized as the restriction of a representation of $S_3$ on $\mathbb{R}^2$ to the set $\{1,2,3\}$. Indeed, since the vectors corresponding to the vertices 1 and 2 are independent, any linear transformation is uniquely determined by where it sends 1 and 2. This shows the representation is unique. To show existence, we can write down the representation in terms of matrices. Explicitly, we let the elements of $S_3$ act by the following matrices. That is, we consider the map $\pi : S_3 \to \text{Aut}(V)$
To check this is a representation, we need to see that id maps to the identity and $\pi(g) \circ \pi(h) = \pi(g \cdot h)$. Let's check this in the case $g = (12), h = (23)$. 

Figure 1. Picture of a triangle with three labeled vertices, corresponding to the $S_3$ action.
Indeed, in this case,
\[
\pi(12) \pi(23) = \begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix} = \pi(123).
\]
Visually, this is saying that if one first flips the triangle flips 1 and 2, and then flips 2 and 3, this composition is the same as rotating 1 to 2.

**Exercise 1.16.** Verify that this is indeed a representation by checking that for all \( g, h \in S_3 \), \( \pi(g) \pi(h) = \pi(g \cdot h) \). (We checked \( g = (12), h = (23) \) above.)

*Hint:* It will probably be much easier to check this holds visually in terms of rotations and reflections than by writing out matrix multiplications.

The moral of this example is that a representation is an assignment of a matrix to each element of a group, in a way that respects composition of group elements.

We call this representation the **standard representation of** \( S_3 \) and denote it by std.

1.4. **Characters.** One useful piece of information which can be garnered from a representation is its character.

**Definition 1.17.** For \( M : V \to V \) a matrix, the **trace of** \( M \), denoted \( \text{tr}(M) \), is the sum of the diagonal elements of \( M \).

**Definition 1.18.** For \((\pi, V)\) a \( G \)-representation, define the **character** of \((\pi, V)\) by

\[
\chi_\pi : G \to k \\
g \mapsto \text{tr}(\pi(g)).
\]

**Example 1.19.** The character of the standard representation of \( S_3 \) from Example 1.15 is given by

\[
\begin{align*}
\text{id} & \mapsto 2 \\
(12) & \mapsto 0 \\
(23) & \mapsto 0 \\
(13) & \mapsto 0 \\
(123) & \mapsto -1 \\
(123) & \mapsto -1
\end{align*}
\]
Warning 1.20. The character is in no way a group homomorphism. This is already seen in Example 1.19.

Definition 1.21. Two elements \( g, h \in G \) are conjugate if there is some \( x \in G \) with \( xgx^{-1} = h \).

Exercise 1.22. Verify that the relation \( g \sim h \) if \( g \) is conjugate to \( h \) is an equivalence relation.

Definition 1.23. A conjugacy class of a group \( G \) is a maximal set of elements of \( G \) all conjugate to each other. That is, it is an equivalence class of \( G \) under the relation of conjugacy.

Lemma 1.24. For \((\pi, V)\) a \( G \)-representation, if \( g \) and \( h \) are conjugate in \( G \), then
\[
\chi_{\pi}(g) = \chi_{\pi}(h).
\]

Proof. Say \( h = kgk^{-1} \). We wish to verify \( \text{tr}(\pi(h)) = \text{tr}(\pi(kgk^{-1})) = \text{tr}(\pi(k)\pi(g)\pi(k)^{-1}) \). So, taking \( A = \pi(k) \) and \( B = \pi(g) \), it suffices to show
\[
\text{tr}(B) = \text{tr}(ABA^{-1}).
\]

Exercise 1.25. Verify this identity. Hint: Here are two possible approaches. (1) If you’ve seen generalized eigenvalues, use that the trace is the sum of generalized eigenvalues with multiplicity, and note that generalized eigenvalues are preserved under conjugation. (2) If you haven’t seen the notion of generalized eigenvalues, reduce to showing \( \text{tr}(CD) = \text{tr}(DC) \) and determine a formula for both of these in terms of the matrix entries of \( C \) and \( D \).

Remark 1.26. Let \( \text{Conj}(G) \) denote the set of conjugacy classes of \( G \). For \( c \in \text{Conj}(G) \) and \( g \) a representative for \( c \), and \( \pi \) as \( G \)-representation, define \( \chi_{\pi}(c) := \chi_{\pi}(g) \). This is independent of choice of \( g \) by Lemma 1.24.

1.5. Character Tables and strange coincidences. As promised, we now espouse the amazing coincidences associated with representations of groups. To see some of these coincidences, we look at the character table. Given a group \( G \) we can associate to \( G \) a character table, where in the rows we list certain representations (the irreducible representations, to be defined precisely later) and in the columns we list the conjugacy classes of \( G \). In the row associated to \((\pi, V)\) and column associated to the conjugacy class of \( g \), we put \( \chi_{\pi}(g) \) (which is independent of choice of \( g \) by Lemma 1.24). Let’s see a few examples.
Example 1.27. Let \( G = \mathbb{Z}/2 \), let \( t \) be the nontrivial element, and let \( \text{triv} \) and \( \text{sgn} \) be the representations discussed in Example 1.9 and Example 1.11. We can form the character table

<table>
<thead>
<tr>
<th></th>
<th>id</th>
<th>( t )</th>
</tr>
</thead>
<tbody>
<tr>
<td>triv</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>sgn</td>
<td>1</td>
<td>-1</td>
</tr>
</tbody>
</table>

Table 1. Character table for \( \mathbb{Z}/2 \)

Example 1.28. Let \( G = \mathbb{Z}/3 \) with elements \( x, x^2, \text{id} \), and let \( \pi_1, \pi_2 \) be the two representations discussed in Example 1.13 so \( \pi_i(x) = \omega^i \) for \( \omega \) a cube root of unity. We can form the character table

<table>
<thead>
<tr>
<th></th>
<th>id</th>
<th>( x )</th>
<th>( x^2 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>triv</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>( \pi_1 )</td>
<td>1</td>
<td>( \omega )</td>
<td>( \omega^2 )</td>
</tr>
<tr>
<td>( \pi_2 )</td>
<td>1</td>
<td>( \omega^2 )</td>
<td>( \omega )</td>
</tr>
</tbody>
</table>

Table 2. Character table for \( \mathbb{Z}/3 \)

Let’s do one more example:

Example 1.29. Let \( G = S_3 \) be the symmetric group on three elements. Let \( \text{std} \) denote the standard representation of Example 1.15. Let \( \text{sgn} \) denote the 1-dimensional representation where the transpositions \((12), (13), (23)\) act by \((-1)\) and all other elements act by \((1)\) (this is related to Example 1.11 by composing the map \( S_3 \to \mathbb{Z}/2 \), sending transpositions to the nontrivial element of \( \mathbb{Z}/2 \), with the sign representation for \( \mathbb{Z}/2 \)). Then, with some help from Example 1.19, \( S_3 \) has character table given as follows:

<table>
<thead>
<tr>
<th></th>
<th>id</th>
<th>(12)</th>
<th>(123)</th>
</tr>
</thead>
<tbody>
<tr>
<td>triv</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>sgn</td>
<td>1</td>
<td>-1</td>
<td>1</td>
</tr>
<tr>
<td>std</td>
<td>2</td>
<td>0</td>
<td>-1</td>
</tr>
</tbody>
</table>

Table 3. Character table for \( S_3 \)
Note that in the top row we use \((12)\) to denote the conjugacy class of \((12)\). So it really corresponds to the three elements \((12), (13), (23)\). Similarly, \((123)\) denotes the conjugacy class of \((123)\), which is \{\((123), (132)\}\).

Let \(\overline{x}\) denote the complex conjugate of \(x\). Recall that the dot product of two complex vectors \(v\) and \(w\) ∈ \(\mathbb{C}^n\) is by definition \(\langle v, w \rangle := \sum_{i=1}^{n} v_i \overline{w_i}\).

**Remark 1.30.** Let us make some observations regarding the above two character tables:

1. The number of representations agrees with the number of conjugacy classes.
2. The size of the group is equal to the sum of the squares of the dimensions of the representations.
3. The dimensions of all representations divide \(\#G\).
4. The dot product of any two distinct columns is equal to 0.
5. The dot product of any column, corresponding to a conjugacy class \(c\), with itself is equal to \(\#G / \#c\).
6. Given two rows of a character table, corresponding to representations \(\pi\) and \(\rho\), define a weighted inner product by \(\langle \chi_\pi, \chi_\rho \rangle := \sum_{c \in \text{Conj}(G)} \#c \chi_\pi(c) \overline{\chi_\rho(c)}\). Then, this weighted inner product of any row with itself takes value \(\#G\) and the weighted inner product of any two distinct rows is 0.

**Exercise 1.31** (Crucial exercise).

1. Verify all claims of **Remark 1.30** for the groups \(\mathbb{Z}/2, \mathbb{Z}/3, S_3\) as in examples Example 1.27, Example 1.28, and Example 1.29.
2. Write down the character table for the representations of \(\mathbb{Z}/n\) constructed in Example 1.14. Verify the claims of **Remark 1.30** for those representations.

It turns out these amazing coincidences hold for all finite groups. Much of the rest of the course will be devoted to proving this.
2. Basic Properties of Representations

Having seen a preview of coming attractions yesterday, we’ll begin solidifying basic notions today.

As is ubiquitous in mathematics, once one has defined the objects of a category, one should define the maps. For example, in the category of groups, the objects are groups and the maps are group homomorphisms. In the category of \( k \)-vector spaces, the objects are \( k \)-vector spaces and the maps are linear transformations. We next define the maps in the category of \( G \)-representations.

**Definition 2.1.** Let \((\pi, V)\) and \((\rho, W)\) be two \( G \)-representations. A **map of representations** is a linear map of vector spaces \( T : V \to W \) so that for all \( g \in G \),

\[
T \circ \pi(g) = \rho(g) \circ T.
\]

Said another way, the diagram

\[
\begin{array}{ccc}
V & \xrightarrow{\pi(g)} & V \\
\downarrow T & & \downarrow T \\
W & \xrightarrow{\rho(g)} & W
\end{array}
\]

(2.1)

commutes.

**Definition 2.2.** A map of \( G \)-representations \( T : (\pi, V) \to (\rho, W) \) is an **isomorphism** if there is an inverse map of \( G \)-representations \( S : (\rho, W) \to (\pi, V) \) so that \( S \circ T : (\pi, V) \to (\pi, V) \) is the identity on \( V \) and \( T \circ S : (\rho, W) \to (\rho, W) \) is the identity on \( W \). We say two \( G \)-representations are **isomorphic** if there exists an isomorphism between them.

**Exercise 2.3** (Optional Exercise). Show that a map of \( G \)-representations \( T \) is an isomorphism if and only if \( T : V \to W \), when viewed simply as a linear transformation of vector spaces, is an isomorphism. **Hint:** Show that the inverse map to \( T \) is automatically a map of representations.

Let’s see an example of a map of representations.

**Example 2.4.** Take \( G = \mathbb{Z}/2 \) and define the 2-dimensional representation \((\pi, V)\) by

\[
\pi(\iota) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}
\]

for \( \iota \) the nontrivial element of \( \mathbb{Z}/2 \). In other words, \( \iota \) swaps the basis vectors of \( V \). Let \( e_1 \) and \( e_2 \) denote the two basis vectors of \( V \). Then, we have a map

\[
T : (\text{triv}, k) \to (\pi, V)
\]
Defined by \( T(1) = e_1 + e_2 \).

Let’s check this is a map of representations. We have to check that for all \( g \in G, v \in V \), \( T \text{triv}(g)v = \pi(g)Tv \). Pictorially, we want to check

\[
\begin{array}{cc}
k & \xrightarrow{\text{id}} & k \\
\downarrow T & & \downarrow T \\
V & \xrightarrow{\pi(g)} & V
\end{array}
\]

commutes.

In equations, since \( \text{triv}(g) = (1) \), we only need to check \( Tv = \pi(g)Tv \). In other words, we just need to check that all elements \( g \in G \) fix the image of \( T \). However, the image of \( T \) is the span of \( e_1 + e_2 \). The identity in \( Z/2 \) fixes everything and \( \pi(\iota)(e_1 + e_2) = e_2 + e_1 \), so it is indeed fixed.

**Exercise 2.5.** Define a nonzero map of \( Z/2 \) representations from \((\text{sgn}, \mathbb{C})\) to \((\pi, V)\) with \( \text{sgn} \) the sign representation and \((\pi, V)\) the representation given in Example 2.4. Show your map of representations is unique up to scaling.

2.1. **Irreducible representations.** We next introduce irreducible representations, which are essentially the building blocks of representation theory.

**Definition 2.6.** For \((\pi, V)\) a representation, a **subrepresentation** is a subspace \( W \subset V \) which is stable under the action of all \( g \in G \) (i.e., \( \pi(g)(W) \subset W \) for all \( g \in G \)). Such a \( W \) has the structure of a representation given by \((\pi|_W, W)\) where \( \pi|_W(g) := \pi(g)|_W \). I.e., viewing \( \pi(g) \) as a map \( V \to V \), \( \pi(g)|_W \) is the induced map \( W \to W \), which has the correct target because \( \pi(g)(W) \subset W \).

**Exercise 2.7.** Show that for \((\pi, V)\) a representation and \( g \in G \), if \( W \subset V \) is subrepresentation then the inclusion \( \pi(g)(W) \subset W \) is automatically an equality. (Recall: All representations are finite dimensional.)

**Example 2.8.** For any representation \((\pi, V)\), both 0 and \( V \) define subrepresentations.

**Definition 2.9.** A representation \((\pi, V)\) is **irreducible** if its only subrepresentations are the 0 subspace and all of \( V \). If a representation is not irreducible, we say it is **reducible**. For brevity, we sometimes refer to an irreducible representation as an **irrep**.

**Exercise 2.10** (Easy exercise). Show that all 1-dimensional representations are irreducible.

**Example 2.11.** The standard representation of \( S_3 \) from Example 1.15 is irreducible. To see this, if it were reducible, it would have some 1-dimensional
subrepresentation, spanned by a nonzero vector \( v \). But then, \( \pi((123))(v) \) is a vector not in the span of \( v \), because it is related to \( v \) by rotation by \( 120^\circ \) which is not in the span of \( v \). Therefore, \( (\text{std}, \mathbb{R}^2) \) cannot be reducible, so it is irreducible.

**Exercise 2.12.** Let \( S_n \) denote the symmetric group on \( n \) elements. Define the permutation representation of \( S_n \) as the representation \( (\pi, V) \) where \( V \) has basis \( e_1, \ldots, e_n \) and \( \sigma \in S_n \) acts by \( \pi(\sigma)(e_i) = e_{\sigma(i)} \). This is called the permutation representation, which we denote \( \text{perm} \). Show that \( V \) has two subrepresentations given by the subspaces \( W_1, W_2 \) where

\[
W_1 := \left\{ \sum_{i=1}^{n} a_i e_i \in V : \sum_{i} a_i = 0 \right\}
\]

and

\[
W_2 := \left\{ \sum_{i=1}^{n} a_i e_i \in V : a_1 = a_2 = \cdots = a_n \right\}.
\]

For the remainder of this exercise, assume the characteristic of \( k \) does not divide \( n \). If you have not seen the notion of characteristic, feel free to assume \( k = \mathbb{C} \).

1. Determine the dimensions of \( W_1 \) and \( W_2 \).
2. Show that \( W_1 \) and \( W_2 \) are independent and span \( V \).
3. In the case \( n = 3 \), show \( W_1 \) is isomorphic to \( \text{std} \) the standard representation of \( S_3 \) by Example 1.15 (in fact, this holds for \( n > 3 \), but we haven’t yet defined the standard representation for higher \( n \)).
4. Determine which 1-dimensional representation \( (\pi|_{W_2}, W_2) \) is isomorphic to. **Hint:** It is one we have already seen, and we haven’t seen very many!

**Definition 2.13.** We call the representation \( W_1 \) from Exercise 2.12 the standard representation of \( S_n \), and denote it by \( \text{std} \).

Note that Definition 2.13 is not a conflict of notation with our definition of the standard representation for \( S_3 \) by Exercise 2.12(3).

If you are assuming \( k = \mathbb{C} \) skip the following exercise.

**Exercise 2.14** (Optional tricky exercise for those familiar with the characteristic of a field). In the setup of Exercise 2.12, assume \( n = 3 \) and \( \text{char}(k) = 3 \). What is the dimension of \( W_2 \)? Are \( W_1 \) and \( W_2 \) independent? Is \( W_1 \) irreducible?

**Exercise 2.15** (Important exercise). Let \( T : (\pi, V) \to (\rho, W) \) be a map of representations. Show that \( \ker T \subset V \) is a subrepresentation of \( V \) and \( \text{im} T \subset W \) is a subrepresentation of \( W \).
Lemma 2.16. A representation is irreducible if and only if for all nonzero $v \in V$, the set $\{g \cdot v\}_{g \in G}$ spans $V$.

Proof. Observe that for any $v \in V$, $\text{Span}\{\pi(g)v\}_{g \in G}$ is a $G$-stable subspace because for any fixed $h \in G$,

$$\{\pi(g)v\}_{g \in G} = \{\pi(h)\pi(g)v\}_{g \in G}.$$

Therefore, if the representation is irreducible, $\text{Span}\{\pi(g)v\}_{g \in G}$ must either be all of $V$ or 0. In other words, if $v \neq 0$, $\text{Span}\{\pi(g)v\}_{g \in G} = V$.

Conversely, if the representation is reducible, let $W \subset V$ be a subrepresentation and take some nonzero $w \in W$. Then $\{\pi(g)w\}_{g \in G} \subset W$ does not span $V$, as desired. □

Exercise 2.17. In the setup of Exercise 2.12 (still assuming $\text{char}(k) \nmid n$), show that $V$ is reducible and $W_1, W_2$ are irreducible subrepresentations. Show that these are the only nonzero proper subrepresentations. Hint: If $W$ is a third subrepresentation, pick $w = \sum_{i=1}^{n} a_i e_i \in W$ nonzero and look at the span of $\{gw\}_{g \in G}$. Depending on whether $a_1 = \cdots = a_n$ and whether $\sum_i a_i = 0$, show that this span is either $W_1, W_2$, or all of $V$.

2.2. Direct sums. We now recall a construction from linear algebra.

Definition 2.18. For $V$ and $W$ two vector spaces, the direct sum, denoted $V \oplus W$, is defined by

$$V \oplus W := \{(v, w) : v \in V, w \in W\}.$$

Addition is given by $(v_1, w_1) + (v_2, w_2) = (v_1 + v_2, w_1 + w_2)$ and scalar multiplication is given by $c(v, w) = (cv, cw)$. This makes $V \oplus W$ into a vector space. More generally, one can define $\oplus_{i=1}^{n} V_i$ as the set of tuples $(v_1, \ldots, v_n)$ with $v_i \in V_i$, and give it the structure of a vector space analogously.

Remark 2.19. Sometimes, the object defined above as $V \oplus W$ is also referred to as $V \times W$.

Example 2.20. The vector space $\mathbb{R}^2 = \mathbb{R} \oplus \mathbb{R}$. Also, $\mathbb{R}^{12} = \mathbb{R}^7 \oplus \mathbb{R}^3 \oplus \mathbb{R}^2$. Further, $\mathbb{R}^n = \oplus_{i=1}^{n} \mathbb{R}$.

Just as we often construct new vector spaces by taking direct sums of vector spaces we have already constructed, we can also construct new representations by taking direct sums of representations we have already constructed. We now formalize this notion.
Definition 2.21. If \((\pi, V)\) and \((\rho, W)\) are two \(G\)-representations, the direct sum is the representation \((\pi \oplus \rho, V \oplus W)\) defined by

\[
(\pi \oplus \rho)(g) : V \oplus W \to V \oplus W
\]

\[
(v, w) \mapsto (\pi(g)v, \rho(g)w).
\]

Exercise 2.22. Check that the direct sum of two representations \((\pi, V)\) and \((\rho, W)\) is indeed a representation. Check that \((\pi, V)\) and \((\rho, W)\) are both subrepresentations of \((\pi \oplus \rho, V \oplus W)\). In particular, deduce that the direct sum of two nonzero representations is never irreducible. Hint: Choose bases for \(V\) and \(W\), and write out the matrix \(\pi(g)\) as a block matrix with blocks corresponding to the maps \(V \to V\) and \(W \to W\).

Exercise 2.23. Show that the representation \((\pi, V)\) of \(\mathbb{Z}/2\) from Example 2.4 can be written as

\[
(\pi, V) \simeq (\text{triv}, \mathbb{C}) \oplus (\text{sgn}, \mathbb{C}).
\]

Exercise 2.24. For \((\pi, V)\) a representation, recall \(\chi_{\pi}(g) = \text{tr}(\pi(g))\). Show that for \((\pi, V), (\rho, W)\) two representations, we have \(\chi_{\pi \oplus \rho}(g) = \chi_{\pi}(g) + \chi_{\rho}(g)\).
3. DESIDERATA AND PROBLEMS

In this section, we’ll state the main results we’ll prove later in the course, and use them to compute lots of examples and fun problems. To start, we recall the main things we want to prove about representations of finite groups, which were essentially already stated in [Remark 1.30]. In order to temporarily state our desiderata, we need to define certain inner products on the rows and columns of a character table. We recommend you jump to the exercises in [subsection 3.2] and come back to read [subsection 3.1] as needed.

3.1. Desiderata. Given a group $G$ and its associated character table (where we think of the character table as a matrix with rows corresponding to irreducible representations $\pi$, columns corresponding to conjugacy classes $c$ and entries given by $\text{tr} \pi(c)$) we define the following inner products: Given two rows of the character table $v$ and $w$ (thought of as vectors with entries $v_c$, $c \in \text{Conj}(G)$), define

$$\langle v, w \rangle_{\text{row}} := \sum_{c \in \text{Conj}(G)} \#c \cdot v_c w_c.$$  

Let $\text{Irrep}(G)$ denote the set of isomorphism classes of complex irreducible representations of $G$. Given two columns of the character table $x$ and $y$ (thought of as vectors with entries $x_\pi$, $\pi \in \text{Irrep}(G)$) define

$$\langle x, y \rangle_{\text{column}} := \sum_{\pi \in \text{Irrep}(G)} x_\pi y_\pi.$$  

(These notations are temporary for this section only, we will re-introduce the relevant inner products later in a broader context.)

Desiderata 3.1. Let $G$ be a finite group. Then, the following hold:

**Maschke’s theorem** Every complex representation is a direct sum of irreducible representations.

**Isotypic decomposition** The direct sum decomposition of the previous part is unique in the sense that any two such decompositions have the same multiset of irreducible components. That is, each irreducible representation which appears in one decomposition appears in the other with the same multiplicity.

**Sum of squares** $\#\text{Irrep}(G)$ is finite, and in fact $\#G = \sum_{\pi \in \text{Irrep}(G)} (\dim \pi)^2$.

**Conjugacy and irreps** $\#\text{Conj}(G) = \#\text{Irrep}(G)$

**Dimensions of irreps** For $\pi \in \text{Irrep}(G)$, $\dim \pi \mid \#G$.

**Orthogonality of rows** For $G$ a group, the rows of the character table are orthogonal in the sense that for any two rows $v$ and $w$, $\langle v, w \rangle_{\text{row}} = 0$ if $v \neq w$ and $\langle v, w \rangle_{\text{row}} = \#G$ if $v = w$.

**Orthogonality of columns** The columns of the character table are orthogonal in the sense that for any two columns $x$ and $y$, $\langle x, y \rangle_{\text{column}} = 0$ if $x \neq y$ and $\langle x, y \rangle_{\text{column}} = \frac{\#G}{\#c}$ for $x = y$. 

NOTES ON REPRESENTATIONS OF FINITE GROUPS

Multiplicity If \((\pi, V)\) is a representation with some irreducible representation \((W, \rho)\) appearing with multiplicity \(n\) inside \(\pi\) (that is, \(\pi \simeq \rho^\oplus n \oplus \rho'\) where \(\rho'\) has no subrepresentations isomorphic to \(\rho\)) then \(\sum_{c \in \text{Conj}(G)} \# \chi_\pi(c) \chi_\rho(c) = \#G \cdot n\). Recall that, for any \(g \in c\), we have defined \(\chi_\pi(c) := \text{tr} \pi(g)\).

The items above will be proven in Theorem 4.5, Theorem 6.3, Theorem 10.1 Corollary 11.6, Theorem 12.1, Theorem 9.2, and Corollary 10.8 below.

3.2. Applications. We now get to apply our desiderata with great effect. In what follows in this subsection, we will assume Desiderata 3.1 throughout (and we may avoid stating explicitly when we are using it). We also assume all representations are over the complex numbers so that we can apply Desiderata 3.1 freely.

Exercise 3.2. (1) If you haven’t yet finished Exercise 1.31 (which asked you to compute the character tables of \(S_3\) and \(\mathbb{Z}/n\)) now is your chance! Do it!
(2) Show that all the representations you write down are irreducible.
(3) Show that every irreducible of the relevant group appears in your list using Desiderata 3.1 [Sum of squares].

Exercise 3.3. Using orthogonality of characters, show that two irreducible complex representations of a finite group \(G\) have equal characters if and only if they are isomorphic.

3.3. Dihedral Groups. In this section, we work out the character tables of dihedral groups.

Definition 3.4. The dihedral group of order \(2n\), denoted \(D_{2n}\), is the finite nonabelian group generated by \(r\) and \(s\) and satisfying the relations \(r^n = s^2 = 1, sr = r^{-1}s\).

Remark 3.5. The dihedral group \(D_{2n}\) can be thought of as the symmetries of the \(n\)-gon with \(r\) acting by rotation by \(2\pi/n\) and \(s\) acting as a reflection. In particular, \(D_6 \simeq S_3\).

Exercise 3.6. (1) If \(n\) is odd, construct two distinct 1-dimensional representations of \(D_{2n}\).
(2) If \(n\) is even, construct four distinct 1-dimensional representations of \(D_{2n}\). Hint: Allow \(r\) and \(s\) to act by \(\pm1\).

Exercise 3.7. (1) If \(n\) is odd, construct \(\frac{n-1}{2}\) distinct 2-dimensional irreducible representations of \(D_{2n}\). Hint: Consider the action on the \(n\)-gon where \(r\) acts by rotation by \(j \cdot 2\pi/n\) for \(1 \leq j < n/2\). Compute characters to show they are distinct.
(2) If $n$ is even, construct $\frac{n-2}{2}$ distinct 2-dimensional irreducible representations of $D_{2n}$.

**Exercise 3.8.** Show that the representations constructed in Exercise 3.6 and Exercise 3.7 are all irreducible representations of $D_{2n}$. *Hint:* Use Desiderata 3.1 [Sum of squares]

**Exercise 3.9.** Determine the character table for the group $D_{2n}$. Check its rows and columns are orthogonal in the sense of Desiderata 3.1.

### 3.4. The Quaternion group

In this subsection, we work out the character table of the Quaternion group.

**Definition 3.10.** The Quaternion group, $Q$, is a group of size 8 with elements $\pm 1, \pm i, \pm j, \pm k$ with the relations $i^2 = j^2 = k^2 = -1$ and $ij = k, ji = -k, ki = j, ik = -j, kj = i, jk = -i$.

**Exercise 3.11.** Construct an irreducible 2-dimension complex representation of the Quaternion group and prove it is irreducible. *Hint:* Consider the 2-dimensional vector space $V$ over $\mathbb{C}$ with basis vectors 1, $j$, which is a 4-dimensional $\mathbb{R}$-vector space $V$ with basis 1, $i, j, i \cdot j$. Identifying $k = ij \in Q$, define an action of $Q$ on $\{\pm 1, \pm i, \pm j, \pm i \cdot j\} \in V$, and extend this to an action on $V$.

**Exercise 3.12.** Construct 4 1-dimensional representations of $Q$ and prove they are pairwise non-isomorphic. *Hint:* To construct them, allow $i$ and $j$ to act by either 1 or $-1$. To show they are distinct, use Exercise 3.3.

**Exercise 3.13.** Compute a complete character table for $Q$. It turns out there are only two order 8 nonabelian groups up to isomorphism: $Q$ and $D_8$. Can you distinguish these two groups using their character tables?

### 3.5. Representations of $A_4$

In this section, we determine the character table for the alternating group $A_4$.

**Exercise 3.14.** (1) Show that the Klein-4 subgroup consisting of permutations $e, (12)(34), (13)(24), (14)(23) \in A_4$ (isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/2$) is a normal subgroup of $A_4$.

(2) Show that the quotient $A_4/K_4 \simeq \mathbb{Z}/3$.

(3) Use the projection $A_4 \rightarrow \mathbb{Z}/3$ to define 3 irreducible 1-dimensional representations of $A_4$, coming from the three irreducible representations of $\mathbb{Z}/3$.

**Exercise 3.15.** Identify the rotations of the tetrahedron in $\mathbb{R}^3$ with the alternating group $A_4$. *Hint:* Here, $A_4$ acts as a subgroup of the permutations of the 4-points on the tetrahedron.

Exercise 3.17. Show that the 3 1-dimensional representations of $A_4$ constructed in Exercise 3.14, together with the 3-dimensional representation constructed in Exercise 3.16 are all irreducible representations of $A_4$. Compute the character table of $A_4$. *Hint:* After determining these are all the representations, to avoid computing angles of rotation of the tetrahedron, you can use the orthogonality properties of the character table to compute the character for the 3-dimensional representation.

3.6. Representations of $S_4$. In this section, we determine the character for $S_4$.

Exercise 3.18. (1) Show that the Klein-4 subgroup consisting of permutations $e, (12)(34), (13)(24), (14)(23) \in S_4$ (isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/2$) is a normal subgroup of $S_4$.
(2) Show that the quotient $S_4/K_4 \cong S_3$.
(3) Use the projection $S_4 \to S_4/K_4 \cong S_3$ construct irreducible representations of $S_4$ corresponding to the three irreducible representations of $S_3$ (triv, sgn, and std).

Exercise 3.19. Show that $S_4$ can be realized as the automorphisms of the cube. *Hint:* Stare at the four long diagonals of the cube.

Exercise 3.20. Use Exercise 3.19 to construct an irreducible 3-dimensional representation of $S_4$.

Exercise 3.21. (1) Show that altogether, $S_4$ has 5 irreducible representations: 3 were constructed in Exercise 3.18, one was constructed in Exercise 3.20, and there is one more, call this last one we have not yet constructed $(\pi, V)$.
(2) Determine the dimension of $V$ from the previous part.
(3) Even though we have not constructed the representation $V$, compute the character table of $S_4$.
(4) Using the character table as a guide, can you construct the representation $V$ explicitly. *Hint:* Can you figure out the relation between $V$, the sgn representation (coming from sgn on $S_3$ via Exercise 3.18), and the 3-dimensional representation of $S_3$? This is a first example of the “tensor product” of representations, which we will see more of later.

3.7. Representations of $A_5$. In this section, we compute character table of $A_5$. 

Exercise 3.22. Compute the conjugacy classes of $A_5$. *Hint:* There are 5 conjugacy classes.

Exercise 3.23. Using the inclusion $A_5 \to S_5$ construct a 4-dimensional irreducible representation of $A_5$ (which we again call std for $A_5$) by composing $A_5 \to S_5 \xrightarrow{\text{std}} \text{Aut}(V)$, where the latter map is the standard representation $(\text{std}, V)$ (as defined in *Definition 2.13*) of $S_5$.

Exercise 3.24. Identify $A_5$ as the group of rotations of the dodecahedron. Use this to construct an irreducible 3-dimensional representation of $A_5$. Compute the character of this representation. *Hint:* To compute the character, find automorphisms of the dodecahedron of orders 2, 3, and 5. The conjugacy classes are almost determined by their orders, with the exception that there are 2 conjugacy classes of order 5. Note that all but one of the conjugacy classes act by rotation. If they rotate an angle of $\theta$ about the third basis vector (which we choose to be the angle of rotation), the action of these elements can be expressed as

$$
\begin{pmatrix}
\cos \theta & -\sin \theta & 0 \\
\sin \theta & \cos \theta & 0 \\
0 & 0 & 1
\end{pmatrix}.
$$

It may be helpful to know $\cos \frac{2\pi}{5} = \frac{1}{4}(-1 + \sqrt{5})$.

Exercise 3.25. (1) Construct an automorphism $S_5 \to S_5$ by sending $\sigma \mapsto (12)\sigma(12)$. Show that this restricts to an automorphism $\phi : A_5 \to A_5$.

(2) Let $(\pi, V)$ denote the 3-dimensional representation of $A_5$ constructed in Exercise 3.24. Compose the automorphism $\phi : A_5 \to A_5$ constructed in the previous part with the representation $\pi : A_5 \to \text{Aut}(V)$ to obtain another 3-dimensional representation $(\rho, W)$ of $A_5$. Show $(\rho, W)$ is irreducible, but is not isomorphic to $(\pi, V)$. *Hint:* To show it is not isomorphic, show that it flips the actions of the two conjugacy classes consisting of order 5 elements.

(3) Compute the character of $(\rho, W)$.

Exercise 3.26. Show that $A_5$ has 5 irreducible representations: triv, the 4-dimensional std from Exercise 3.23, the two 3-dimensional representations fromExercise 3.24 and Exercise 3.25, and one more. Compute the dimension of this last representation.

Exercise 3.27. Compute the character table of $A_5$.

3.8. **Groups of order** $p^3$. In this subsection, we guide the reader in determining the number of conjugacy classes of any group of order $p^3$ for $p$ a prime. This is carried out in Exercise 3.44.
Definition 3.28. Let $G$ be a group. Define the center of $G$, denoted $Z(G)$ by
$$Z(G) := \{ g \in G : gh = hg \text{ for all } g \in G \}.$$ 

Remark 3.29. The center is the set of elements that commute with all other elements, so $G$ is abelian if and only if $G = Z(G)$.

Exercise 3.30. Show $Z(G) \subset G$ is a normal subgroup.

Exercise 3.31. Suppose $p$ is a prime and $G$ is a $p$-group (meaning $\#G = p^n$ for some $n$). Suppose $G$ acts on a finite set $S$. Let $\text{Fix}_G(S) \subset S$ denote the set of $s \in S$ with $g \cdot s = s$ for all $g \in G$. I.e., $\text{Fix}_G(S)$ is the set of fixed points under the $G$-action. Show $\#\text{Fix}_G(S) \equiv S \pmod{p}$. Hint: Use the orbit stabilizer theorem.

Exercise 3.32. Let $p$ be a prime. If $G$ is a $p$-group show $Z(G)$ is nontrivial. \(\text{Exercise 3.31}\)

Exercise 3.33. Suppose that $G$ is a group with $G/Z(G) \cong \mathbb{Z}/n\mathbb{Z}$. Show that in fact $G = Z(G)$ (so $n = 1$).

Exercise 3.34. For $G$ a nonabelian group of order $p^3$ for $p$ prime, show $\#Z(G) = p$. Hint: Rule out the possibilities that $\#Z(G) = 1, p^2, p^3$.

Definition 3.35. For $G$ a group, define the commutator subgroup, denoted $[G, G]$ to be the subgroup of $G$ generated by all elements of the form $xyx^{-1}y^{-1}$ for $x, y \in G$. That is, $[G, G]$ consists of all products of elements of the form $xyx^{-1}y^{-1}$.

Exercise 3.36. For $G$ a group, show that $[G, G] \subset G$ is a normal subgroup.

Exercise 3.37. Show there are no nonabelian groups of order $p^2$. \(\text{Exercise 3.32 and Exercise 3.33}\)

Exercise 3.38. Let $G$ be a non-abelian group of order $p^3$ for some prime $p$. Show $[G, G] = Z(G)$ and both have size $p$ in the following steps

1. Let $q : G \to G/[G, G]$ denote the quotient map. Show that if we have a map $f : G \to H$ for $H$ an abelian group then there is a unique map $\phi : G/[G, G] \to H$ so that $\phi \circ q = f$.
2. Show that $[G, G]/Z(G)$ is abelian using \(\text{Exercise 3.37}\). Conclude from the previous part that if $f : G \to G/Z(G)$ is the quotient map, there is a unique map $\phi : G/[G, G] \to G/Z(G)$ so that $\phi \circ q = f$.
3. Show that for $H$ and $K$ groups, and $N \subset H$ a normal subgroup, the set of maps $H/N \to K$ are in bijection with maps $H \to K$ sending $N$ to the identity element of $K$.
4. Conclude from the previous two parts that $[G, G] \subset Z(G)$.
5. Show that $[G, G] \neq 1$
(6) Conclude \([G, G] = Z(G)\) and both have size \(p\). \textit{Hint:} Use Exercise 3.34.

**Exercise 3.39.** Suppose \(G\) is a non-abelian group of order \(p^3\) for some prime \(p\). Show that \(G / [G, G] = \mathbb{Z} / p \times \mathbb{Z} / p\). \textit{Hint:} Show \(G / [G, G]\) is abelian of order \(p^2\), but not cyclic. For this, use Exercise 3.37 and Exercise 3.38.

**Exercise 3.40.** For \(G\) any finite group, show that if \(g \in [G, G]\), then for any 1-dimensional \((\pi, k)\) of \(G\), \(\pi(g) = \text{id}\). Use this to show there is a bijection between the 1-dimensional representations of \(G\) and 1-dimensional representations of \(G / [G, G]\).

**Exercise 3.41.**

1. Construct \(p^2\) distinct irreducible 1-dimensional representations of \(\mathbb{Z} / p \times \mathbb{Z} / p\) and show these are all of them. \textit{Hint:} Send generators to multiplication by roots of unity, as in Exercise 1.31.
2. If you are so inclined, generalize this to arbitrary finite abelian groups (which are necessarily a product of cyclic groups by the fundamental theorem for finitely generated abelian groups).

**Exercise 3.42.** Suppose \(G\) is a non-abelian group of order \(p^3\) for some prime \(p\). Find all 1-dimensional representations of \(G\). \textit{Hint:} Combine Exercise 3.39, Exercise 3.40, and Exercise 3.41.

**Exercise 3.43.** Let \(G\) be a nonabelian group of order \(p^3\) for \(p\) prime. Show that \(G\) has \(p^2\) irreps of dimension 1 and \(p - 1\) irreps of dimension \(p\). \textit{Hint:} Use that the dimension of any irrep must divide the order of the group, together with the previous exercises.

**Exercise 3.44.** Let \(p\) be a prime and \(G\) a nonabelian group of order \(p^3\). Show that \(G\) has \(p^2 + p - 1\) conjugacy classes. \textit{Hint:} Use Exercise 3.43.

### 3.9. Further Challenge exercises.

**Exercise 3.45.** Consider the regular representation of \(S_3\), \(\text{Reg}(S_3)\), defined as the 6-dimensional representation spanned by basis vectors \(\{e_g\}_{g \in S_3}\) with action given by \(\sigma \cdot e_g = e_{\sigma \cdot g}\). Calculate the character of the regular representation and use the multiplicity criterion from Desiderata 3.1 to find the number of copies of the three irreducible representations of \(S_3\) (triv, sgn, std) inside \(\text{Reg}(S_3)\). (Note, this calculation is done for an arbitrary group in the proof of the sum of squares formula.) Then, describe an explicit decomposition of \(\text{Reg}(S_3)\) as a direct sum of irreducible subrepresentations.

**Exercise 3.46** (Tricky exercise). In this exercise, we explore the possible number of even and odd dimensional irreducible representations of a group \(G\). A priori, there are four possibilities either \(G\) has
(1) an even number of odd dimensional irreducible representations and an even number of even dimensional irreducible representations
(2) an odd number of odd dimensional irreducible representations and an even number of even dimensional irreducible representations
(3) an even number of odd dimensional irreducible representations and an odd number of even dimensional irreducible representations
(4) an odd number of odd dimensional irreducible representations and an odd number of even dimensional irreducible representations

For which of (1), (2), (3), and (4) does there exist a finite group \(G\) with such a number of odd and even dimensional irreducible representations? Either given an example of such a \(G\) or prove no such \(G\) exist.

Here are two problems, which can be solved both by elementary methods and using representation theory.

**Exercise 3.47.** Let \(S_n\) act on \([n] := \{1, \ldots, n\}\) by permuting the elements. For \(g \in S_n\), let \(\text{Fix}(g)\) denote the set of \(x \in [n]\) so that \(g(x) = x\). That is, \(\text{Fix}(g)\) is the set of \(x\) fixed by \(g\).

1. Show using elementary methods (without representation theory) that \(\sum_{g \in S_n} \# \text{Fix}(g) = n!\).
2. Show using representation theory \(\sum_{g \in S_n} \# \text{Fix}(g) = n!\). **Hint:** Consider the permutation representation of \(S_n\) as defined in Exercise 2.12 and recall it decomposes as a direct sum of triv and std, two irreducible representations, as shown in Exercise 2.12 and Exercise 2.17. Let \(\chi_{\text{perm}}\) be the associated character and relate \(\sum_{g \in S_n} \# \text{Fix}(g)\) to \(\langle \chi_{\text{perm}}, \chi_{\text{triv}} \rangle\).

**Exercise 3.48.** Let \(S_n\) act on \([n] := \{1, \ldots, n\}\) by permuting the elements. Show that \(\sum_{g \in S_n} (\# \text{Fix}(g))^2 = 2n!\). See if you can do it both using representation theory, and via elementary means.

**Exercise 3.49.** Show that \(G\) is abelian if and only if all irreducible representations are 1-dimensional.

**Exercise 3.50.** Fix a group \(G\). Show that \(G\) is abelian if and only if it is possible to reorder the irreps and conjugacy classes of \(G\) so that the character table of \(G\) is symmetric about the diagonal line from the upper left to lower right.

**Exercise 3.51.** Let \(D_\infty\) be the “infinite dihedral group” generated by \(r\) and \(s\) with the relations that \(s^2 = 1\) and \(sr = r^{-1}s\). (If we imposed \(r^n = 1\), we would get the usual dihedral group \(D_{2n}\).) Find a 2-dimensional representation of \(D_\infty\) which is not irreducible, but cannot be written as a direct sum of irreducible representations. Note this does not contradict Maschke’s theorem because \(D_\infty\) is infinite.
4. COMPLETE REDUCIBILITY OF COMPLEX REPRESENTATIONS

We begin the saga of proving Desiderata 3.1. To start, we next introduce a notion of complete reducibility. Just as every vector space breaks up as a direct sum of copies of the base field (by choosing a basis), in many nice cases, every representation breaks up as a direct sum of irreducible representations.

We next codify the notion of complete reducibility:

**Definition 4.1.** A $G$-representation $(\pi, V)$ is **completely reducible** if $V$ can be written as a direct sum of irreducible $G$-representations. That is, one can find a collection of irreducible subrepresentations $V_i \subset V$ which have trivial pairwise intersection and span $V$.

We’d like to give a criterion for when every $G$-representation is completely reducible, so it can always be broken down into irreducible pieces. This is done in [Theorem 4.5]. In particular, we will see this is always true over $\mathbb{C}$ or more generally any field of characteristic 0.

To set this up, we define quotient representations. Recall that for $W \subset V$ a subspace, the quotient $V/W$ is the quotient of $V$ by the equivalence relation $v_1 \sim v_2$ if $v_1 - v_2 \in V$. The following exercise is crucial, especially if you haven’t seen quotients:

**Exercise 4.2 (Important Exercise).** Let $W \subset V$ be a subspace.

1. Verify that the relation $v_1 \sim v_2$ if $v_1 - v_2 \in W$ is an equivalence relation.
2. Give the set $V/W$ the structure of a vector space by declaring $c[v] := [cv]$ and $[v_1] + [v_2] := [v_1 + v_2]$. Check that this is well defined (i.e., independent of the choice of representative for $v \in V$).
3. Check that $\dim V/W = \dim V - \dim W$. Hint: Choose a basis $e_1, \ldots, e_m$ for $W$ and extend it to a basis $e_1, \ldots, e_n$ for $V$. Check the images $[e_{m+1}], \ldots, [e_n]$ in $V/W$ form a basis for $V/W$.
4. Let

$$q : V \to V/W$$
$$v \mapsto [v]$$

denote the projection map. Verify that there is a map of vector spaces $s : V/W \to V$ so that $q \circ s = \text{id}_{V/W}$. Hint: Choose bases as in the previous part and define $s$ by sending $[e_{m+j}] \in V/W$ to $e_{m+j} \in V$.
5. Let $i : W \to V$ denote the given inclusion. Show that for any such map $s$ as in the previous part, the map $(i, s) : W \oplus V/W \to V$ is an
isomorphism. Here, \((i, s)\) denotes the map
\[
(i, s): W \oplus V/W \to V
\]
\[
(w, x) \mapsto i(w) + s(x).
\]

**Definition 4.3.** For \((\pi, V)\) a \(G\)-representation and \(W \subset V\) a subrepresentation, define the **quotient representation** \((\overline{\pi}, V/W)\) to be the representation with vector space \(V/W\) and action given by \(\overline{\pi}(g)[v] := [\pi(g)(v)]\) where for \(x \in V\), \([x]\) denotes the image under the map \(V \to V/W\) taking the equivalence class in the quotient.

**Exercise 4.4.**
1. Check definition [Definition 4.3](#) is well defined. That is, check that if \(v_1, v_2\) are two representatives for \([v]\) then \([\pi(g)(v_1)] = [\pi(g)(v_2)]\).
2. Verify that \(V/W\) is indeed a \(G\)-representation.
3. Show \(q: V \to V/W\) is a map of representations.

If you are assuming \(k = \mathbb{C}\), then ignore the assumption on \(\text{char}(k)\) everywhere that follows, as it is automatically satisfied.

**Theorem 4.5** (Maschke’s Theorem). Suppose \(\text{char}(k) \nmid \#G\). Then every \(G\)-representation is completely reducible.

Before continuing with the proof, we include a couple illustrative exercises.

**Exercise 4.6.** Let \((\text{perm}, V)\) be the permutation representation for \(S_3\), as discussed in Exercise 2.12. Recall this was the 3-dimensional representation with basis \(e_1, e_2, e_3\) so that \(\text{perm}(\sigma)(e_i) = e_{\sigma(i)}\). Let \((\text{triv}, W) \subset (\text{perm}, V)\) denote the 1-dimensional subrepresentation spanned by \(e_1 + e_2 + e_3\). Find a \(T \in \text{Hom}(\text{perm}, \text{perm})\) with \(T^2 = T\) and \(\text{im} T = W\). Compute the subrepresentation \(\ker T\). *Hint:* You might guess what \(T\) and \(\ker T\) have to be via your solution to Exercise 2.12.

**Exercise 4.7.**
1. Let \((\pi, V)\) denote the 2-dimensional \(\mathbb{Z}/2\) representation defined in Example 2.4 where the nontrivial element \(i\) acts by \(\pi(i)(e_0) = e_1, \pi(i)(e_1) = e_0\). Write \((\pi, V)\) as a direct sum of irreducible representations. *Hint:* We already did this in Exercise 2.23.
2. Similarly, for this part, let \((\pi, V)\) denote the 3-dimensional representation of \(\mathbb{Z}/3 = \{0, 1, 2\}\) with basis \(e_1, e_2, e_3\) satisfying \(\pi(j)e_i = e_{i+j \mod 3}\). Write \((\pi, V)\) as a direct sum of irreducible \(\mathbb{Z}/3\) representations.
3. Can you generalize the previous part replacing \(\mathbb{Z}/3\) with \(\mathbb{Z}/n\)?

**Proof of Theorem 4.5** Let \((\pi, V)\) be a \(G\)-representation. Let \(i: (\pi|_W, W) \subset (\pi, V)\) be a nonzero proper subrepresentation and \((\overline{\pi}, V/W)\) be the quotient...
representation defined in Definition 4.3. Let \( q : (\pi, V) \to (\overline{\pi}, V/W) \) denote the quotient map.

We claim \((\pi, V) \simeq (\pi|_W, W) \oplus (\overline{\pi}, V/W)\). Indeed, once we show this, by induction on the dimension of \( V \), we will be done, because \( \pi|_W \) and \( \overline{\pi} \) are smaller dimensional representations. Therefore, by induction on the dimension, we can write \((\pi|_W, W) = \bigoplus_{i=1}^n (\pi_i, W_i) \) and \((\overline{\pi}, V/W) = \bigoplus_{j=1}^m (\overline{\pi}_j, V'_j) \) for irreducible \( \pi_i \) and \( \overline{\pi}_j \). Then,

\[
(\pi, V) \simeq (\pi|_W, W) \oplus (\overline{\pi}, V/W) \simeq \left( \bigoplus_{i=1}^n (\pi_i, W_i) \right) \oplus \left( \bigoplus_{j=1}^m (\overline{\pi}_j, V'_j) \right).
\]

So, to conclude, it suffices to show \((\pi, V) \simeq (\pi|_W, W) \oplus (\overline{\pi}, V/W)\). To prove this, we claim there is a map of representations \( \iota : (\pi, V/W) \to (\pi, V) \) so that \( q \circ \iota = \text{id}_{V/W} \). This is shown next in Proposition 4.9. Let’s see why this concludes the proof, and then we’ll come back to prove Proposition 4.9.

To conclude the proof, by Exercise 4.2(5) the resulting map \((i, \iota) : W \oplus V/W \to V\) is an isomorphism of vector spaces. Further, since \( \iota \) and \( i \) are both maps of representations, it is also a map of representations.

Exercise 4.8 (Easy exercise). Check for yourself that \((i, \iota)\) is indeed a map of representations.

Hence \((i, \iota)\) is an isomorphism of representations, which is what we needed to check.

So, to conclude the proof of Theorem 4.5, we only need to prove the following proposition.

**Proposition 4.9.** Let \( \text{char}(k) \not| \#G \). Let \((\pi, V)\) be a representation, \( W \subset V \) a subrepresentation, \( V/W \) the corresponding quotient representation with quotient map \( q : V \to V/W \). Then there is a map of representations \( \iota : V/W \to V \) so that \( q \circ \iota = \text{id}_{V/W} \).

**Proof.** First, we know there exists a map \( f : V/W \to V \) of vector spaces so that \( q \circ f = \text{id}_{V/W} \), as shown in Exercise 4.2(4). However, this may not be a map of representations (as there is no reason that \( f \circ \pi(g) \) should equal \( \pi(g) \circ f \)). We rectify this by an averaging trick: Define

\[
\iota : V/W \to V \quad x \mapsto \frac{1}{\#G} \sum_{g \in G} \pi(g)f(\pi(g^{-1})x).
\]
We claim $\iota$ is a map of representations and satisfies $q \circ \iota = \text{id}_{V/W}$. Once we check these two facts, we will be done. First, let’s check $\iota$ is a map of representations. Pictorially, this means we have to check

\[
\begin{array}{cccc}
V/W & \xrightarrow{\pi(h)} & V/W \\
\downarrow \iota & & \downarrow \iota \\
V & \xrightarrow{\pi(h)} & V
\end{array}
\]

(4.1)

commutes.

Indeed, for $x \in V/W$,

\[
\iota(\pi(h)x) = \frac{1}{\#G} \sum_{g \in G} \pi(g)f(\pi(g^{-1})\pi(h)x)
\]

\[
= \frac{1}{\#G} \sum_{g \in G} \pi(h^{-1}g)f(\pi(g^{-1}h)x)
\]

\[
= \frac{1}{\#G} \sum_{g \in G} \pi(h)\pi(h^{-1}g)f\left(\pi\left((h^{-1}g)^{-1}\right)x\right)
\]

\[
= \pi(h)\frac{1}{\#G} \sum_{h^{-1}g \in G} \pi(h^{-1}g)f\left(\pi\left((h^{-1}g)^{-1}\right)x\right)
\]

\[
= \pi(h)\iota(x)
\]

as desired.
To conclude, we check \( q \circ i = \text{id}_{V/W} \). Indeed, for \( x \in V/W \),
\[
q \circ i(x) = q \left( \frac{1}{\#G} \sum_{g \in G} \pi(g) f(\pi(g^{-1})x) \right)
\]
\[
= \frac{1}{\#G} \sum_{g \in G} q \left( \pi(g) f(\pi(g^{-1})x) \right)
\]
\[
= \frac{1}{\#G} \sum_{g \in G} \pi(g) q \left( f(\pi(g^{-1})x) \right)
\]
\[
= \frac{1}{\#G} \sum_{g \in G} \pi(g) \pi(g^{-1})x
\]
\[
= \frac{1}{\#G} \sum_{g \in G} \pi(gg^{-1})x
\]
\[
= \frac{1}{\#G} \sum_{g \in G} \pi(e)x
\]
\[
= \frac{1}{\#G} \sum_{g \in G} x
\]
\[
= x.
\]
\( \square \)

This concludes the proof of Maschke’s theorem.

We note that the assumption that \( \text{char}(k) \nmid \#G \) is crucial to Theorem 4.5. (Again, ignore this if you are assuming \( k = \mathbb{C} \).) We give an exercise exhibiting of a representation that is not completely reducible when \( \text{char}(k) \mid \#G \). This is essentially spelling out the solution to Exercise 2.14. Again, skip this if you are assuming \( k = \mathbb{C} \).

**Exercise 4.10** (Optional exercise for those familiar with characteristic). Let \( k \) be a field of characteristic 2. Consider the action of \( \mathbb{Z}/2 \) on the two dimensional vector space \( V \) with basis \( e_1, e_2 \) given by
\[
\pi(i)(e_1) := e_1,
\]
\[
\pi(i)(e_2) := e_1 + e_2.
\]

1. Verify that \( (\pi, V) \) is a representation. *Hint:* You will need to use \( \text{char}(k) = 2 \).
2. Check that \( \text{Span}(e_1) \) is a subrepresentation, so \( V \) is reducible.
3. Check that \( \text{Span}(e_1) \) is the only subrepresentation, so \( V \) is not completely reducible. *Hint:* Show that for any \( v \in V - \text{Span}(e_1) \), \( v \) and \( \pi(i)(v) \) are independent and use Lemma 2.16.
Remark 4.11. Theorem 4.5 will be psychologically useful for us, as it lets us think of any representation as a sum of irreducible constituents. As we shall see next, these irreducible constituents (and their multiplicities) are in fact uniquely determined.
5. Schur’s Lemma

Our next main result is proving isotypic decomposition. In order to show this, we will need Schur’s lemma, which we prove in this section. This is one of the most important results toward setting up the basic theory of representations of finite groups. Recall that a field $k$ is algebraically closed if every monic polynomial with coefficients in $k$ has a root. (Again, feel free to assume $k = \mathbb{C}$ if it is helpful.) Here is the statement for Schur’s lemma.

**Theorem 5.1** (Schur’s lemma). If $(\pi, V)$ and $(\rho, W)$ are two $G$-representations over an algebraically closed field,

$$\dim \text{Hom}(\pi, \rho) = \begin{cases} 1 & \text{if } \pi \simeq \rho \\ 0 & \text{if } \pi \not\simeq \rho \end{cases}.$$

To prove Schur’s lemma, we will need two lemmas.

**Lemma 5.2.** Let $T : (\pi, V) \to (\rho, W)$ be a nonzero map of representations.

1. If $(\pi, V)$ is irreducible, $T$ is injective.
2. If $(\rho, W)$ is irreducible, $T$ is surjective.
3. If $(\pi, V)$ and $(\rho, W)$ are both irreducible, $T$ is an isomorphism.

**Proof.** We prove the parts in order.

1. Consider $\ker T \subset V$. Since $V$ is irreducible, and $\ker T$ is a subrepresentation by Exercise 2.13, we either have $\ker T = V$ or $\ker T = 0$. The former cannot occur because $T \neq 0$. So, $\ker V = 0$ and $T$ is injective.
2. Consider $\text{im } T \subset W$. Since $W$ is irreducible, and $\text{im } T$ is a subrepresentation by Exercise 2.13, either $\text{im } T \subset W = 0$ or $\text{im } T = W$. But we cannot have $\text{im } T = 0$ because $T \neq 0$, so $\text{im } T = W$ and $T$ is surjective.
3. This follows from the first two parts.

**Lemma 5.3.** Suppose $k$ is algebraically closed and $V$ is a $k$ vector space with $(\pi, V)$ a finite dimensional irreducible $G$-representation. Then, any map of representations $T : (\pi, V) \to (\pi, V)$ is necessarily multiplication by a scalar. That is, $T = c \cdot \text{id}$ for $c \in k$.

**Proof.** Let $T$ be some such map. Note that $T$ has an eigenvalue since eigenvalues are the same as roots of the characteristic polynomial, and by assumption $k$ is algebraically closed so the characteristic polynomial has a root in $k$. (If you are pretending $k = \mathbb{C}$, this is just saying that every polynomial over $\mathbb{C}$ has a root, which is the fundamental theorem of algebra.)

Let $\lambda$ denote the resulting eigenvalue and $x$ the corresponding eigenvector, so $Tx = \lambda x$. Let

$$W := \{w \in V : Tw = \lambda w\}.$$
Observe that $W$ is nonzero since $0 \neq x \in W$ (and by definition of eigenvector, $x \neq 0$). To conclude, it suffices to show $W = V$, because that will imply $Tv = \lambda v$ for all $v \in V$ so $T = \lambda \cdot \text{id}$.

Because $V$ is irreducible, in order to show $W = V$, it suffices to show $W$ is a subrepresentation. To check this, we just need to know that for $g \in G$, $T(W) \subset W$. But indeed, for any $w \in W$, $T w = \lambda w \in \text{Span}(w) \subset W$, as desired. \[ \square \]

Using the above two results, we can easily prove Schur’s lemma.

**Proof of Theorem 5.1** From Lemma 5.2 we know that if $\rho \ncong \pi$ then the only map between $\rho$ and $\pi$ is 0. So, it suffices to show that if $\pi \cong \rho$ then, $\dim \text{Hom}(\pi, \rho) = 1$. This is precisely the content of Lemma 5.3 \[ \square \]

**Exercise 5.4** (Irreducible representations of abelian groups). Let $G$ be an abelian group and $(\pi, V)$ an irreducible representation over an algebraically closed field $k$. For this exercise, you are not allowed to use Desiderata 3.1 and

1. Show that $\pi(g) : (\pi, V) \to (\pi, V)$ defines a map of representations. 
   **Hint:** You need to show $\pi(g)$ commutes with $\pi(h)$ for any $h \in G$.
2. Show that for every $g \in G$, there is some nonzero $c \in k$ such that $\pi(g) = c \cdot \text{id}$ **Hint:** Schur’s lemma!
3. Conclude that $V$ is 1-dimensional.

If you are working over $\mathbb{C}$, skip the following exercise.

**Exercise 5.5** (Optional exercise for those familiar with algebraically closed fields). Let $G$ be an abelian group and $(\rho, V)$ an irreducible representation. Show that if $k$ is not algebraically closed then $V$ may have dimension more than 1 via the following example: Take $k = \mathbb{R}$, $G = \mathbb{Z}/3$ and let $\rho$ be the representation on the 2-dimensional vector space $\mathbb{R}^2$ so that the generator of $\mathbb{Z}/3$ acts by rotation by $2\pi/3$. Show that this representation is irreducible.
6. ISOTYPIC DECOMPOSITION

We next introduce a notion of isotypic decomposition of a representation. This essentially says that a representation breaks into irreducibles in an almost unique way.

First, we introduce notation for repeated direct sums:

**Definition 6.1.** For \((\rho, W)\) a \(G\)-representation, define 
\[
(\rho, W)^{\oplus n} := \bigoplus_{i=1}^{n} (\rho, W).
\]

We shall often denote \((\rho, W)\) simply as \(\rho\), in which case we let \(\rho^{\oplus n}\) denote \((\rho, W)^{\oplus n}\).

**Definition 6.2.** Let \((\pi, V)\) be a \(G\)-representation. An **isotypic decomposition** for \(\pi\) is an isomorphism 
\[
(\pi, V) \cong \bigoplus_{i=1}^{n} \left(\pi_i, V_i\right)^{\oplus n_i}
\]
so that each \((\pi_i, V_i)\) is irreducible and for any \(i \neq j\), \(\pi_i \not\cong \pi_j\).

The main result is that isotypic decomposition is essentially unique:

**Theorem 6.3.** Suppose \((\pi, V)\) is a \(G\)-representation and \((\pi, V) \cong \bigoplus_{i=1}^{n} (\pi_i, V_i)^{\oplus n_i}\) and \((\pi, V) \cong \bigoplus_{j=1}^{m} (\rho_j, W_j)^{\oplus m_j}\) are two isotypic decompositions. Then isotypic decomposition is unique in the following sense:

1. \(m = n\)
2. For each \(i\) there is a unique \(j\) so that \((\pi_i, V_i) \cong (\rho_j, W_j)\) and \(n_i = m_j\).

**Remark 6.4.** Note that this does not say there is a unique isomorphism between two isotypic decompositions. For example, if \((\pi, V) = (\text{triv}, \mathbb{C})^{\oplus 2}\) then any invertible \(2 \times 2\) matrix will define an isomorphism between \(V\) and itself. In general, isotypic decomposition says we can determine the irreducible subrepresentations and their respective multiplicities.

Before proving Theorem 6.3, let’s deduce a quick but useful corollary.

**Corollary 6.5.** Suppose \((\pi, V)\) is a \(G\)-representation over a field with \# \not\mid \text{char}(k). Then \((\pi, V)\) has a unique isotypic decomposition (where by unique, we mean unique in the sense of Theorem 6.3).

**Proof.** The existence is precisely the content of Theorem 4.5. Uniqueness is precisely Theorem 6.3. \(\square\)

6.1. Proving uniqueness of isotypic decomposition. We next aim toward proving Theorem 6.3. The following lemma is key.

**Lemma 6.6.** Let \(\pi \cong \bigoplus_{i=1}^{n} \pi_i\) and \(\rho \cong \bigoplus_{j=1}^{m} \rho_j\) be two \(G\)-representations. Then 
\[
\text{Hom}(\pi, \rho) \cong \bigoplus_{i=1}^{n} \bigoplus_{j=1}^{m} \text{Hom}(\pi_i, \rho_j).
\]
Proof. We define maps both ways, and check that these define a bijection. First, we define a map

\[ f : \text{Hom}(\pi, \rho) \to \bigoplus_{i=1}^{n} \bigoplus_{j=1}^{m} \text{Hom}(\pi_i, \rho) . \]

This is given by sending a map \( \phi : \pi \to \rho \), to the tuple of composite maps

\[ \phi_{ij} : \pi_i \to \pi \xrightarrow{\phi} \rho \to \rho_j . \]

Similarly, we define a map

\[ g : \bigoplus_{i=1}^{n} \bigoplus_{j=1}^{m} \text{Hom}(\pi_i, \rho) \to \text{Hom}(\pi, \rho) \]

by sending a tuple of maps \( (\phi_{ij})_{1 \leq i \leq n, 1 \leq j \leq m} \) to the map \( \phi \) defined as follows. If \( v = \sum_{i=1}^{n} v_i \) with \( v_i \) in the vector space \( V_i \) on which \( \pi_i \) acts, then

\[ \phi(v) = \sum_{i=1}^{n} \sum_{j=1}^{m} \phi_{ij}(v_i) . \]

Exercise 6.7. Verify that the maps \( f \) and \( g \) above are maps of \( G \)-representations and are inverse of each other, completing the proof of Lemma 6.6.

From Lemma 6.6, we can easily deduce the following:

Lemma 6.8. If \( \pi \) and \( \rho_1, \ldots, \rho_m \) are two irreducible \( G \)-representations with \( \pi \) not isomorphic to \( \rho_j \) for any \( j \), \( \text{Hom}(\pi \oplus a, \bigoplus_{j=1}^{m} \rho_j \oplus b_j) = 0 \).

Proof. Lemma 6.6 allows us to reduce to the case \( m = 1 \) and then further to the case \( a = b_1 = 1 \). This case is then settled by Lemma 5.2.

Using Lemma 6.8 we can now prove Theorem 6.3.

Proof of Theorem 6.3. Pick some \( i, 1 \leq i \leq n \). If there is no \( \rho_j \) with \( \pi_i \simeq \rho_j \), then by Lemma 6.8 any map

\[ \bigoplus_{i=1}^{n} \pi_i \oplus n_i \to \bigoplus_{j=1}^{m} \rho_j \oplus m_j \]

must be 0 on \( V_i \), and hence cannot be an isomorphism. Therefore, there is some \( j \) so that \( \pi_i \simeq \rho_j \). Furthermore, \( j \) is unique because by definition of isotypic decomposition, no two \( \rho_j \) are isomorphic. By reasoning similarly
with \( \rho_j \), we find that for each \( j \) there is a unique \( i \) with \( \rho_j \simeq \pi_i \). Therefore, there is a bijection between the set of \( \pi_i \) and the set of \( \rho_j \), so \( m = n \).

It only remains to show that when \( \pi_i \simeq \rho_j \), \( n_i = m_j \). We will show \( n_i \leq m_j \), and the reverse inequality will follow by symmetry (interchanging the roles of the \( \pi_i \) and \( \rho_j \)).

To conclude, we show \( n_i \leq m_j \). Composing the isomorphism (6.1) with the inclusion \( \pi_{i}^{\oplus n_i} \to \bigoplus_{i=1}^{n} \pi_{i}^{\oplus n_i} \) we obtain an injection

\[
\pi_{i}^{\oplus n_i} \to \bigoplus_{i=1}^{m} \rho_{i}^{\oplus m_i}.
\]

If \( \pi_i \simeq \rho_j \), then by Lemma 6.8, we know the composite map \( \pi_{i}^{\oplus n_i} \to \bigoplus_{i=1}^{m} \rho_{i}^{\oplus m_i} \to \rho_{s}^{\oplus n_s} \) must be 0 whenever for \( s \neq j \). Therefore, we even have an injection \( V_{i}^{\oplus n_i} \to W_{j}^{\oplus m_j} \). Therefore,

\[
n_i \cdot \dim V_i = \dim V_{i}^{\oplus n_i} \leq \dim W_{j}^{\oplus m_j} = m_j \cdot \dim W_j.
\]

Since \( V_i \simeq W_j \), \( \dim V_i = \dim W_j \), so \( n_i \cdot \dim V_i \leq m_j \cdot \dim V_i \) which implies \( n_i \leq m_j \) as claimed. \( \square \)
In order to prove orthogonality of characters, we will need to introduce several new constructions of representations from old ones. Namely homs, duals, and tensors. For each of homs, duals, and tensor products, we first explain them in the context of linear algebra, and then upgrade them to representation theoretic constructions.

7.1. Homs of representations. We next define the notions of duals, tensor products, and homs in the setting of linear algebra.

**Definition 7.1** (homs). Let $V$ and $W$ be two vector spaces. Then $\text{Hom}(V, W)$ denotes the set of linear maps $T : V \to W$. Then, $\text{Hom}(V, W)$ can be given the structure of a vector space as follows: If $T, S : V \to W$ are linear maps and $c \in k$, define $(T + S)(v) := T(v) + S(v)$ and define $(c \cdot T)(v) := c \cdot (T(v))$.

**Definition 7.2** (homs of representations). Let $(\pi, V)$ and $(\rho, W)$ be two representations. This can be given the structure of a $G$-representation $(\text{Hom}_{\pi, \rho}, \text{Hom}(V, W))$ by declaring

$$\text{Hom}_{\pi, \rho}(g) : \text{Hom}(V, W) \to \text{Hom}(V, W)$$

$$T \mapsto \rho(g)T\pi(g^{-1}).$$

**Lemma 7.3.** For $(\pi, V)$ and $(\rho, W)$ two representations, the object $(\text{Hom}_{\pi, \rho}, \text{Hom}(V, W))$ constructed in [Definition 7.2] is indeed a $G$-representation.

**Proof.** The crux of the matter is to check that for $g, h \in G$, we have $\text{Hom}_{\pi, \rho}(g) \circ \text{Hom}_{\pi, \rho}(h) = \text{Hom}_{\pi, \rho}(gh)$. Indeed,

$$(\text{Hom}_{\pi, \rho}(g) \circ \text{Hom}_{\pi, \rho}(h))T = \text{Hom}_{\pi, \rho}(g)\left(\text{Hom}_{\pi, \rho}(h)T\right)$$

$$= \text{Hom}_{\pi, \rho}(g)\left(\rho(h)T\pi(h^{-1})\right)$$

$$= \rho(g)\rho(h)T\pi(h^{-1})\pi(g^{-1})$$

$$= \rho(gh)T\pi((gh)^{-1})$$

$$= \text{Hom}_{\pi, \rho}(gh)T.$$

7.2. Duals of representations.

**Definition 7.4** (Duals). For $V$ a $k$-vector space, let $V^\vee$, the dual of $V$, denote the set of linear maps $V \to k$. Note that $V^\vee = \text{Hom}(V, k)$, so this can be given the structure of a vector space as in [Definition 7.1].
Exercise 7.5. If \( e_1, \ldots, e_n \) is a basis for \( V \) then we can form a dual basis \( e_1^\vee, \ldots, e_n^\vee \) for \( V^\vee \) defined by

\[
e_i^\vee : V \to k,
\quad e_j \mapsto \delta_{ij},
\]

where \( \delta_{ij} = 1 \) if \( i = j \) and 0 if \( i \neq j \). Check this is a basis for \( V^\vee \). In particular, conclude \( \dim V^\vee = \dim V \). Hint: Show any linear map \( V \to k \) is determined by where it sends the basis elements \( e_1, \ldots, e_n \). Show that a linear map \( V \to k \) can be expressed uniquely as a linear combination of the \( e_i^\vee \).

Definition 7.6 (Duals of representations). For \((\pi, V)\) a \( G \)-representation, let \((\pi^\vee, V^\vee)\) denote the dual representation of \( \pi \), which is defined as

\[
(\pi^\vee, V^\vee) := (\text{Hom}_{\pi, \text{triv}}, \text{Hom}(V, C))
\]

using the notation from Definition 7.2.

Exercise 7.7. Verify that for \((\pi, V)\) a representation, and \( g \in G, \xi \in V^\vee, v \in V \), we have \((\pi^\vee(g)\xi)(v) = \xi(\pi(g^{-1})v)\). Hint: Thinking of \( \xi \) as a map \( \xi : V \to k \), use that \( \text{Hom}_{\pi, \text{triv}}(g)(\xi) = \text{triv}(g) \circ \xi \circ \pi(g^{-1}) \).

Exercise 7.8. Let \((\pi, C)\) be the representation of \( \mathbb{Z}/3 = \{e, x, x^2\} \) with \( x \) acting by \( \omega \), for \( \omega^3 = 1, \omega \neq 1 \). Compute \((\pi^\vee, C^\vee)\). Hint: We know \((\pi^\vee, C^\vee)\) is a 1-dimensional representation of \( \mathbb{Z}/3 \), and it is determined by whether \( \pi^\vee(x) = 1, \omega, \text{or} \omega^2 \).

Remark 7.9. We will see later in Lemma 8.11 that over the complex numbers, the dual representation essentially corresponds to taking the complex conjugate. Technically, Lemma 8.11 only makes a statement about the character of the dual representation being the conjugate of the character of the representation. This is true more generally on the level of representations (not just on characters). If you’re interested, try to define what is meant by the conjugate of a complex representation, and show that the conjugate representation is isomorphic to the dual representation.

7.3. Tensors of representations.

Definition 7.10 (Tensors). For \( V \) and \( W \) two finite dimensional \( k \)-vector spaces, let \( e_1, \ldots, e_n \) be a basis of \( V \) and \( f_1, \ldots, f_m \) be a basis of \( W \). Then the tensor product of \( V \) and \( W \), denoted \( V \otimes_k W \) (often denoted \( V \otimes W \) when \( k \) is understood) is the \( k \)-vector space with basis \( \{e_i \otimes f_j\}_{1 \leq i \leq n, 1 \leq j \leq m} \). For \( v = \sum_i a_i e_i \in V, w = \sum_j b_j f_j \in W \) let \( v \otimes w \in V \otimes W \) denote the simple tensor given by

\[
v \otimes w = \sum_{i,j} a_i \cdot b_j (e_i \otimes f_j).
\]
Remark 7.11. Here the symbols $e_i \otimes f_j$ are merely formal symbols to keep track of indexing, and $V \otimes_k W$ is a vector space of dimension $\dim V \cdot \dim W$. If one thinks of direct sum of vector spaces as adding vector spaces, one may think of tensor product as multiplying them.

Remark 7.12. One can alternatively define the tensor product of $V$ and $W$ as the vector space generated by all pairs $v \otimes w$ for $v \in V, w \in W$, subject to the bilinearity relations that

\[
(v + v') \otimes w = v \otimes w + v' \otimes w, \\
v \otimes (w + w') = v \otimes w + v \otimes w', \\
(aw) \otimes w = a(v \otimes w) = v \otimes (aw).
\]

One issue with this is that it is not obvious from this definition that this is finite dimensional. The way to prove it is finite dimensional is to show it agrees with the definition given in Definition 7.10. There is a further (in many ways “better”) definition given in terms of a universal property, which we do not go into here.

Exercise 7.13. For $V$ any $k$-vector space, verify $V \simeq V \otimes_k k$ with the isomorphism given by $v \mapsto v \otimes 1$.

Example 7.14. Consider the vector space $V \otimes_k W$ where $V$ has basis $e_1, e_2$ and $W$ has basis $f_1, f_2$. Then, $V \otimes W$ is a 4-dimensional vector space with basis $e_1 \otimes f_1, e_2 \otimes f_1, e_1 \otimes f_2, e_2 \otimes f_2$. In particular, viewing $\mathbb{C}$ as a 2-dimensional vector space over $\mathbb{R}$ with basis $\{1, i\}$, conclude that $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ has basis given by $1 \otimes 1, 1 \otimes i, i \otimes 1, i \otimes i$.

Exercise 7.15 (Not all tensors are simple). Consider the vector space $V \otimes_k W$ where $V$ has basis $e_1, e_2$ and $W$ has basis $f_1, f_2$. Show that the element $e_1 \otimes f_2 + e_2 \otimes f_1$ cannot be expressed as a simple tensor $a \otimes b$ for $a \in V, b \in W$. Hint: Expand a general element of the form $(ae_1 + be_2) \otimes (cf_1 + df_2)$.

Exercise 7.16. Show that for vector spaces $U, V,$ and $W$, a linear map $T : V \otimes_k W \to U$ is uniquely determined by its values on simple tensors. That is $T$ is determined by its values on elements of the form $v \otimes w$. That is, show that if we have two such maps $T$ and $S$ where $T(v \otimes w) = S(v \otimes w)$ for all simple tensors $v \otimes w$ then $T = S$.

Exercise 7.17. For $V, W$ two finite dimensional vector spaces, show

1. $\dim \text{Hom}(V, W) = \dim V \cdot \dim W$,
2. $\dim V^\vee = \dim V$,
3. $\dim V \otimes W = \dim V \cdot \dim W$,
4. $\dim V^\vee \otimes W = \dim \text{Hom}(V, W)$.
**Definition 7.18** (Tensors of representations). For \((\pi, V)\) and \((\rho, W)\) two \(G\)-representations, Define the **tensor representation** \((\pi \otimes \rho, V \otimes W)\) by

\[ (\pi \otimes \rho)(g) : V \otimes W \to V \otimes W \]

\[ v \otimes w \mapsto \pi(g)v \otimes \rho(g)w. \]

**Example 7.19.** Let \(G = \mathbb{Z}/2\) and consider the representation \((\text{sgn}, k)\) as defined in **Example 1.11**. This is the unique nontrivial representation of \(\mathbb{Z}/2\). When one tensors two 1-dimensional representations, one multiplies the corresponding characters. In particular, we claim that the representation \(\text{sgn} \otimes \text{sgn}\) is isomorphic to the trivial representation because 

\[ -1 \cdot -1 = 1, \quad 1 \cdot 1 = 1. \]

That is, we have an isomorphism

\[ \phi : (\text{triv}, k) \simeq (\text{sgn} \otimes \text{sgn}, k \otimes k) \]

given by sending \(a \mapsto a \otimes 1\) for \(a \in k\). We have seen in **Exercise 7.13** that this defines an isomorphism of vector spaces, so we only need to check this is a map of representations. That is, we need to check that for \(v \in k\),

\[ \phi \circ \text{triv}(g)v = ((\text{sgn} \otimes \text{sgn})(g) \circ \phi)v. \]

As always, this holds for \(g = \text{id}\) tautologically, so we only need to check it in the case \(g\) is the nontrivial element of \(\mathbb{Z}/2\). Indeed, in this case, we have \(\phi \circ \text{triv}(g)v = \phi(v) = v \otimes 1\). So, we really just need to check \(((\text{sgn} \otimes \text{sgn})(g) \circ \phi)v = v \otimes 1\). Indeed,

\[ ((\text{sgn} \otimes \text{sgn})(g) \circ \phi)v = (\text{sgn} \otimes \text{sgn})(g)(v \otimes 1) \]

\[ = (-v) \otimes (-1) \]

\[ = (-1)^2 \cdot (v \otimes 1) \]

\[ = v \otimes 1. \]

**Remark 7.20.** **Example 7.19** illustrates a general procedure for computing tensors of a representation with a 1-dimensional representation. The reason \(\text{sgn} \otimes \text{sgn} \simeq \text{triv}\) is because 

\[ (-1) \cdot (-1) = 1. \]

In general, the tensor product of two 1-dimensional representations acts as the product of the two 1-dimensional representations. The situation is similar when only one of the representations is 1-dimensional (you multiply the higher dimensional representation by the scalar coming from the 1-dimensional representation).

**Exercise 7.21.** For \((\pi, V)\) a \(G\)-representation, verify that there is an isomorphism of representations \((\pi, V) \simeq (\pi \otimes \text{triv}, V \otimes_k k)\) defined on the underlying vector spaces by sending \(v \mapsto v \otimes 1\).

7.4. **Relations among dual, tensor, and hom.** Having defined dual, tensor, and hom, both as vector spaces and representations, we next explain how they relate to each other. Let’s start with their relation within linear algebra and then upgrade it to a statement in representation theory.
Lemma 7.22. For $V$ and $W$ $k$-vector spaces, the map
\[
\phi : V^\vee \otimes W \rightarrow \text{Hom} \,(V,W)
\]
\[
(\xi \otimes w) \mapsto (v \mapsto \xi(v) \cdot w).
\]
is an isomorphism.

Proof. The map $\phi$ is a map between two vector spaces of the same dimension by Exercise 7.17(4). So, to show it is an isomorphism, it suffices to show it is injective.

Let $e_1, \ldots, e_n$ denote a basis for $V$ and let $e_1^\vee, \ldots, e_n^\vee$ denote the dual basis given by $e_i^\vee(e_j) := \delta_{ij}$, see Exercise 7.5. Here $\delta_{ij} = 1$ if $i = j$ and 0 if $i \neq j$. Let $f_1, \ldots, f_m$ be a basis for $W$. Then, observe that $\phi$ is given by
\[
\phi \left( \sum_{i,j} a_{ij} e_i^\vee \otimes f_j \right) = \left( v \mapsto \sum_{i,j} a_{ij} e_i^\vee(v) f_j \right).
\]

To show $\phi$ is injective, we only need to check that if not all $a_{ij}$ are 0, then the map $v \mapsto \sum_{i,j} a_{ij} e_i^\vee(v) f_j$ is nonzero. Indeed, if some $a_{k\ell}$ is nonzero, then $e_k \mapsto \sum_{i,j} a_{ij} e_i^\vee(e_k) f_j = \sum_j a_{kj} f_j \neq 0$ since the $f_j$ form a basis. Hence, the linear transformation takes $e_k$ to something nonzero, so is nonzero. \qed

We now give a representation theoretic upgrade of the previous lemma.

Lemma 7.23. If $(\pi, V)$ and $(\rho, W)$ are two $G$-representations, then the map $\phi$ from Lemma 7.22 gives is an isomorphism of $G$-representations
\[
(\pi^\vee \otimes \rho, V^\vee \otimes W) \simeq (\text{Hom}_{\pi,\rho}, \text{Hom} \,(V,W)).
\]

Proof. We know from Lemma 7.22 that the underlying vector spaces are isomorphic via the map $\phi$. So it suffices to show this map $\phi$ is in fact a map of representations. This is now a routine calculation. For $g \in G$ we need to check $(\phi \circ (\pi^\vee \otimes \rho))(g) = \text{Hom}_{\pi,\rho}(g) \circ \phi$. That is, we need the following diagram to commute:

\[
\begin{array}{ccc}
V^\vee \otimes W & \overset{(\pi^\vee \otimes \rho)(g)}{\longrightarrow} & V^\vee \otimes W \\
\downarrow \phi & & \downarrow \phi \\
\text{Hom}(V,W) & \overset{\text{Hom}_{\pi,\rho}(g)}{\longrightarrow} & \text{Hom}(V,W).
\end{array}
\]

(7.1)
Indeed,
\[
(\phi \circ (\pi^\vee) \otimes \rho(g))(\xi \otimes w) = \phi(\pi^\vee \otimes \rho(g)(\xi \otimes w)) \\
= \phi(\pi^\vee(g)(\xi) \otimes \rho(g)(w)) \\
= (x \mapsto (\pi^\vee(g)(\xi))(x) \otimes \rho(g)w) .
\]

On the other hand, we also see
\[
\text{Hom}_{\pi,\rho}(g) \circ \phi(\xi \otimes w) = \text{Hom}_{\pi,\rho}(g) \ (x \mapsto \xi(x) \otimes w) \\
= \rho(g) \circ (x \mapsto \xi(x)\rho(g)w) \circ \pi(g^{-1}) \\
= (x \mapsto \xi(x)\rho(g)w) \circ \pi(g^{-1}) \\
= (x \mapsto \xi(\pi(g^{-1})x)\rho(g)w) \\
= (x \mapsto (\pi^\vee(g)(\xi))(x)\rho(g)w) \text{ Exercise 7.7}
\]

Therefore,
\[
(\phi \circ (\pi^\vee) \otimes \rho(g)) = \text{Hom}_{\pi,\rho}(g) \circ \phi
\]
8. ORTHOGONALITY OF CHARACTERS

In this section, we work over the field $\mathbb{C}$. We will assume this in what follows without comment.

Recall from Definition 1.18 that if $(\pi, V)$ is a complex $G$-representation then $\chi_\pi : G \to \mathbb{C}$ is the function sending $g \mapsto \text{tr}(\pi(g))$. Let $\bar{x}$ denote the complex conjugate of $x \in \mathbb{C}$. The main result is the following:

**Theorem 8.1.** Suppose $(\pi, V)$ and $(\rho, W)$ are two irreducible complex $G$-representations. Then

$$
\sum_{g \in G} \chi_\pi(g) \cdot \bar{\chi}_\rho(g) = \begin{cases} 
\#G & \text{if } \pi \simeq \rho \\
0 & \text{if } \pi \not\simeq \rho
\end{cases}
$$

The idea of the proof will be to realize $\sum_{g \in G} \chi_\pi(g) \cdot \bar{\chi}_\rho(g)$ as the character of the representation $\text{Hom}_{\pi, \rho}$, to reduce it to the Proposition 8.6. In order to state Proposition 8.6, we need the following definition:

**Definition 8.2.** For $(\pi, V)$ a $G$-representation, the $G$-invariants, denoted $V^G$, are defined as

$$
V^G := \{ v \in V : \pi(g)v = v \text{ for all } g \in G \}.
$$

In other words, $V^G$ is the set of $G$-invariant vectors in $V$.

**Exercise 8.3.** Verify that $V^G \subset V$ is a subspace.

**Definition 8.4.** For $(\pi, V)$ and $(\rho, W)$ two $G$-representations, let $\text{Hom}(\pi, \rho)$ denote the vector space of maps or representations.

**Exercise 8.5.** Suppose $(\pi, V)$ and $(\rho, W)$ are two $G$-representations and let $(\text{Hom}_{\pi, \rho}, \text{Hom}(V, W))$ be the corresponding hom representation. Show that the $G$-invariants of $\text{Hom}_{\pi, \rho}$ on the vector space $\text{Hom}(V, W)$ are exactly the maps of $G$-representations $\text{Hom}(\pi, \rho)$.

**Proposition 8.6.** For $(\pi, V)$ an irreducible $G$-representation over $\mathbb{C}$,

$$
\sum_{g \in G} \chi_\pi(g) = \#G \cdot \dim V^G.
$$

8.1. Reducing Theorem 8.1 to Proposition 8.6. Let’s first see why Proposition 8.6 implies Theorem 8.1. For this, we will need to understand how characters behave with respect to tensor products and duals.

**Lemma 8.7.** For $(\pi, V)$ and $(\rho, W)$ two representations, $\chi_{\pi \otimes \rho}(g) = \chi_\pi(g) \cdot \chi_\rho(g)$.
Proof. Choosing a basis $e_i$ for $V$ and $f_j$ for $W$, we see that $e_i \otimes f_j$ is a basis for $V \otimes W$. Therefore, if $\pi(g)(e_i) = \sum_k a^i_k e_k$ and $\rho(g)(f_j) = \sum \ell b^j_\ell f_\ell$, it follows from the definition of the tensor of two representations that

$$((\pi \otimes \rho)(g))(e_i \otimes f_j) = \sum_{k, \ell} a^i_k b^j_\ell (e_k \otimes f_\ell).$$

In particular, the diagonal element of the matrix corresponding to $\pi \otimes \rho$ acting on the basis vector $e_i \otimes f_j$ is $a^i_i b^j_j$. It follows that

$$\text{tr}((\pi \otimes \rho)(g)) = \sum_{i, j} a^i_i b^j_j$$

as desired. \[\Box\]

Exercise 8.8 (Important exercise). For $(\pi, V)$ a representation, show $\chi_{\pi^\vee}(g) = \chi_\pi(g^{-1})$. 

Hint: Let $e_i$ be a basis for $V$ and $e_i^\vee$ be the dual basis for $V^\vee$ (meaning $e_i^\vee(e_j) = \delta_{ij}$).

1. Check that $\pi^\vee(g^{-1})(e_i^\vee)$ is the functional sending $e_j \mapsto e_i^\vee(\chi_\pi(g^{-1})e_j)$.

2. Verify $\text{tr} \pi(g) = \sum_{i=1}^{\dim V} e_i^\vee(\pi(g)e_i)$

3. Use the previous two parts to deduce the result.

Exercise 8.9. For $(\pi, V)$ a representation, show that every eigenvalue of $\pi(g)$ has complex norm 1. 

Hint: Use that $G$ is finite.

Exercise 8.10. Verify that if $M$ is a matrix of finite order over $C$, then $M$ is diagonalizable. 

Hint: Say $M^n = \text{id}$. Then the characteristic polynomial of $M$ divides $x^n - 1$, and use that the latter splits as a product of distinct linear factors over $C$ to conclude that $V$ has a basis of eigenvectors for $M$, so $M$ is diagonalizable.

Lemma 8.11. For $(\pi, V)$ a representation, we have $\chi_{\pi^\vee}(g) = \chi_\pi(g^{-1})$.

Proof. By Exercise 8.10, $\pi(g)$ is diagonalizable. Say its eigenvalues are $\lambda_1, \ldots, \lambda_n$. Then the eigenvalues of $\pi(g^{-1})$ are $\frac{1}{\lambda_1}, \ldots, \frac{1}{\lambda_n}$. By Exercise 8.9 (using that $\overline{x} = x^{-1}$ for $x \in C$ of norm 1), we obtain

$$\frac{1}{\lambda_i} = \overline{\lambda_i}.$$
It follows that the eigenvalues of $\pi(g^{-1})$ are $\lambda_1, \ldots, \lambda_n$ so

$$\text{tr } \pi(g^{-1}) = \sum_{i=1}^{n} \lambda_i = \sum_{i=1}^{n} \lambda_i = \text{tr } \pi(g)$$

\[ \square \]

We can combine the above observations to show the following:

**Corollary 8.12.** For $(\pi, V)$ and $(\rho, W)$ two representations, we have

$$\chi_{\text{Hom}(\pi, \rho)} = \overline{\chi_{\pi}} \cdot \chi_{\rho}$$

**Proof.** Indeed,

$$\chi_{\text{Hom}(\pi, \rho)}(g) = \chi_{\pi} \otimes \rho(g) = \chi_{\pi}(g) \cdot \chi_{\rho}(g) = \chi_{\pi}(g^{-1}) \cdot \chi_{\rho}(g) = \overline{\chi_{\pi}(g)} \cdot \chi_{\rho}(g)$$

\[ \square \]

We’re finally ready to show why Proposition 8.6 implies Theorem 8.1.

**Proof that Proposition 8.6 implies Theorem 8.1.** Let $(\pi, V)$ and $(\rho, W)$ be as in Theorem 8.1. Apply Proposition 8.6 to the representation $\text{Hom}(\pi, \rho)$. We find

$$\sum_{g \in G} \chi_{\rho}(g) \overline{\chi_{\pi}(g)} = \sum_{g \in G} \chi_{\text{Hom}(\pi, \rho)}(g)$$

**Corollary 8.12**

$$= \#G \cdot \dim \text{Hom}(V, W)^G$$

**Proposition 8.6**

$$= \#G \cdot \dim \text{Hom}(\pi, \rho)$$

**Exercise 8.5**

$$= \begin{cases} \#G & \text{if } \pi \simeq \rho \\ 0 & \text{if } \pi \not\simeq \rho \end{cases}$$

**Lemma 5.2.**

\[ \square \]

### 8.2. Projection operators.

We next want to prove Proposition 8.6. For this, we first review some linear algebra involving projection operators.

**Definition 8.13.** Let $V$ be a vector space and $W \subset V$ a subspace. A map $T : V \to V$ is a projection onto $W$ if $T|_{W} = \text{id}$ and $T(V) \subset W$.

**Exercise 8.14.** Show that $T : V \to V$ is a projection onto $\text{im } T$ if and only if $T \circ T = T$, viewed as linear maps $V \to V$. 


Exercise 8.15. If \( T : V \rightarrow V \) is a projection operator onto \( W \), show \( \text{tr}(T) = \dim W \). *Hint:* Write \( T \) as a block matrix with blocks corresponding to \( W \) and a complement of \( W \). Show one of the diagonal blocks is \( \text{id} \) and the other is \( 0 \).

The point of introducing projection operators is to prove the following, which will be used to relate the trace of the averaging operator to \( \dim V^G \) in the statement of Proposition 8.6 by Exercise 8.15.

**Lemma 8.16.** Let \((\pi, V)\) be a representation. The averaging map \( \text{Av}_\pi : \frac{1}{\#G} \sum_{g \in G} \pi(g) : V \rightarrow V \) is a projection onto \( V^G \).

**Proof.** First, if \( v \in V^G \) then then
\[
\text{Av}_\pi(v) = \frac{1}{\#G} \sum_{g \in G} \pi(g)v
\]
\[
= \frac{1}{\#G} \sum_{g \in G} v
\]
\[
= \frac{1}{\#G} \#G v
\]
\[
= v,
\]
so \( \text{Av}_\pi |_{V^G} = \text{id} \). In particular, we see \( V^G \subset \text{im Av}_\pi \).

So, to show \( \text{Av}_\pi \) is a projection operator, we only need to check \( V^G \supset \text{im Av}_\pi \). To this end, let \( v \in \text{im Av}_\pi \). We want to show \( v \in V^G \), meaning that for any \( h \in G \), \( \pi(h)v = v \). By the assumption \( v \in \text{im Av}_\pi \), we can write \( v = \frac{1}{\#G} \sum_{g \in G} \pi(g)w \) for some \( w \in V \). Then, we see
\[
\pi(h)v = \pi(h) \frac{1}{\#G} \sum_{g \in G} \pi(g)w
\]
\[
= \frac{1}{\#G} \sum_{g \in G} \pi(h)\pi(g)w
\]
\[
= \frac{1}{\#G} \sum_{g \in G} \pi(hg)w
\]
\[
= \frac{1}{\#G} \sum_{t \in G} \pi(t)w \quad \text{setting } t := hg
\]
\[
= v.
\]

\( \Box \)

8.3. **Proving Proposition 8.6** We are now equipped to prove Proposition 8.6 which will also complete the proof of Theorem 8.1.
Proof of Proposition 8.6. By Lemma 8.16, we know \( A_{\pi} = \frac{1}{\#G} \sum_{g \in G} \pi(g) \) is a projection onto \( V^G \). It follows from Exercise 8.15 that \( \text{tr} A_{\pi} = \dim V^G \). Therefore,

\[
\dim V^G = \text{tr} A_{\pi} \\
= \text{tr} \left( \frac{1}{\#G} \sum_{g \in G} \pi(g) \right) \\
= \frac{1}{\#G} \sum_{g \in G} \text{tr} \pi(g) \\
= \frac{1}{\#G} \sum_{g \in G} \chi_{\pi}(g)
\]

as we wished to show. \( \Box \)
9. ORTHOGONALITY OF CHARACTER TABLES

We discuss how the rows of a character table are, in an appropriate sense, orthogonal. We then discuss how the columns are also orthogonal. Again, in this section we work over \( \mathbb{C} \). We state and prove this now, but the proof depends on knowing that the number of conjugacy classes equals the number of irreducible representations, as shown later in Corollary 11.6.

**Definition 9.1.** Let \( \text{Irrep}(G) \) denote the set of all irreducible complex representations of \( G \), up to isomorphism.

**Theorem 9.2** (Orthogonality of character tables). For \( G \) a group, the rows of the character table are orthogonal in the sense that, for \( \pi, \rho \in \text{Irrep}(G) \),

\[
\sum_{c \in \text{Conj}(G)} \#c \chi_{\pi}(c) \overline{\chi_{\rho}(c)} = \begin{cases} \#G & \text{if } \pi \simeq \rho \\ 0 & \text{if } \pi \not\simeq \rho \end{cases}
\]

(where \( \chi_{\pi}(c) \) denotes the value of \( \chi_{\pi} \) on a conjugacy class, well defined by Lemma 1.24). The columns of of the character table are orthogonal in the sense that for \( c, d \) any two conjugacy classes

\[
\sum_{\pi \in \text{Irrep}(G)} \chi_{\pi}(c) \overline{\chi_{\pi}(d)} = \begin{cases} \frac{\#G}{\#c} & \text{if } c = d \\ 0 & \text{if } c \neq d \end{cases}
\]

**Proof assuming Corollary 11.6** The orthogonality claim on the rows is the content of Theorem 9.2.

It remains to prove the column orthogonality. We deduce this from row orthogonality via a clever trick of changing the order of matrix multiplication. Let \( A \) denote the matrix indexed by pairs \( (\pi, c) \in \text{Irrep}(G) \times \text{Conj}(G) \) defined by

\[
A_{\pi,c} := \frac{\sqrt{\#c}}{\sqrt{\#G}} \chi_{\pi}(c).
\]

Let \( \overline{A} \) denote the entry-wise conjugate matrix (so \( \overline{A}_{\pi,c} = \overline{A_{\pi,c}} \)).

**Exercise 9.3.** Verify that column orthogonality is precisely the statement that \( A \cdot \overline{A}^T = \text{id} \), where for \( M \) a matrix, \( M^T \) denotes the transpose of \( M \).

To conclude column orthogonality, we need the following elementary fact from linear algebra.

**Exercise 9.4.** For \( M, N \) two \( n \times n \) matrices with \( MN = \text{id} \), verify that \( NM = \text{id} \) as well. *Hint:* Observe that \( M(NM - \text{id}) = MNM - M = 0 \). Use that \( M : V \rightarrow V \) is bijective to conclude \( NM - \text{id} = 0 \).
So, knowing $A \cdot \overline{A} = \text{id}$, it follows from Exercise 9.4 that $\overline{A} \cdot A = \text{id}$. Here we are using that $A$ is a square matrix, which follows since the number of conjugacy classes equals the number of irreps (proved later in Corollary 11.6). However, expanding out this product, we see that multiplying the row of $\overline{A}$ indexed by a conjugacy class $c$ containing $g$ and the column of $A$ indexed by a conjugacy class $d$ containing $h$, we have that

$$(\overline{A} \cdot A)_{c,d} = \sum_{\pi \in \text{Irrep}(G)} \frac{\sqrt{\# c}}{\sqrt{\# G}} \chi_{\pi}(g) \chi_{\pi}(h).$$

On the other hand, since $\overline{A} \cdot A = \text{id}$, it follows that the right hand side expression is 0 if $c \neq d$ and 1 if $c = d$. In the latter case, we obtain

$$1 = \sum_{\pi \in \text{Irrep}(G)} \frac{\# c}{\# G} \chi_{\pi}(g) \chi_{\pi}(h).$$

Therefore,

$$\frac{\# G}{\# c} = \sum_{\pi \in \text{Irrep}(G)} \frac{\# c}{\# G} \chi_{\pi}(g) \chi_{\pi}(h),$$

as claimed. □
10. THE SUM OF SQUARES FORMULA

In this section, we work over $\mathbb{C}$, so in particular we may apply Schur’s lemma, Maschke’s theorem, and orthogonality of characters. The main goal is to prove that the sum of the squares of the dimensions of all irreducible representations of $G$ is equal to $\#G$. Along the way, we will need to introduce the inner product between characters and the regular representation.

Theorem 10.1 (Sum of Squares Formula). For $G$ any finite group,

$$\sum_{\rho \in \text{Irrep}(G)} (\dim \rho)^2 = \#G.$$ 

Remark 10.2. Note that this follows immediately from Theorem 9.2 applied to the column corresponding to the conjugacy class of the identity, since $\dim \rho = \chi_\rho(e)$. However, this proof relies on the fact the the number of conjugacy classes equals the number of irreducible representations, which takes quite some work as we will later see. We now give an alternate proof, as it gives us the opportunity to introduce the regular representation and see more representation theory techniques in action.

Exercise 10.3. Assuming Theorem 10.1 show that there are only finitely many isomorphism classes of irreducible representations. Further verify that if $(\pi, V)$ is an irreducible $G$-representation, $\dim \pi \leq \sqrt{\#G}$ with equality if and only if $\#G = 1$.

10.1. The inner product on characters. We define an “inner product” on characters of representations. For now this is just notation as we have not yet described the space on which it is an inner product. It will turn out that characters are actually a basis for the space of class functions, to be defined later in Definition 11.1.

Definition 10.4. For $(\pi, V), (\rho, W)$ two complex representations, define

$$\langle \chi_\pi, \chi_\rho \rangle := \frac{1}{\#G} \sum_{g \in G} \chi_\pi(g) \overline{\chi_\rho(g)}.$$ 

Lemma 10.5. If $(\pi, V)$ and $(\rho, W)$ are irreducible then

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

Furthermore, the number above is equal to $\dim \text{Hom}(\pi, \rho)$.

Proof. The first claim is simply a rephrasing of the statement of Theorem 8.1. The second claim follows from Schur’s lemma Theorem 5.1. \qed


We wish to generalize Lemma 10.5 which computes the dimension of maps of representations to arbitrary representations, instead of just irreducible ones. For this, we will need the following result on how characters commute with direct sums:

**Exercise 10.6.** Verify that for \( \pi \cong \bigoplus_{i=1}^{n} \pi_i \), we have
\[
\chi_{\pi} = \sum_{i=1}^{n} \chi_{\pi_i}.
\]
*Hint:* Recall Exercise 2.24 which showed this in the case \( n = 2 \).

**Proposition 10.7.** For \((\pi, V), (\rho, W)\) two complex \( G \)-representations (not necessarily irreducible) we have
\[
\langle \chi_{\pi}, \chi_{\rho} \rangle = \dim \text{Hom}(\pi, \rho).
\]

**Proof.** We have already proven this holds in the case \( \rho \) and \( \pi \) are irreducible in Lemma 10.5. In general, by Maschke's theorem Theorem 4.5 we can write \( \rho \) and \( \pi \) as \( \pi \cong \bigoplus_{i=1}^{n} \pi_i, \rho \cong \bigoplus_{j=1}^{m} \rho_j \). for \( \pi_i, \rho_j \) all irreducible representations. Then, by Lemma 6.6 we find
\[
\text{Hom}(\pi, \rho) = \bigoplus_{i=1}^{n} \bigoplus_{j=1}^{m} \text{Hom}(\pi_i, \rho_j).
\]
Taking dimensions of both sides we find
\[
\dim \text{Hom}(\pi, \rho) = \dim \left( \bigoplus_{i=1}^{n} \bigoplus_{j=1}^{m} \text{Hom}(\pi_i, \rho_j) \right).
\]

\[
= \sum_{i=1}^{n} \sum_{j=1}^{m} \dim \text{Hom}(\pi_i, \rho_j)
\]
\[
= \sum_{i=1}^{n} \sum_{j=1}^{m} \langle \chi_{\pi_i}, \chi_{\rho_j} \rangle
\]
\[
= \langle \sum_{i=1}^{n} \chi_{\pi_i}, \sum_{j=1}^{m} \chi_{\rho_j} \rangle
\]
\[
= \langle \chi_{\bigoplus_{i=1}^{n} \pi_i}, \chi_{\bigoplus_{j=1}^{m} \rho_j} \rangle
\]
\[
= \langle \chi_{\pi}, \chi_{\rho} \rangle.
\]

\( \square \)

The following corollary is crucial for proving Theorem 10.1. Note this is essentially Desiderata 3.1[Multiplicity].
Corollary 10.8. Let \((\pi, V)\) be a representation and \(\pi \simeq \oplus_{i=1}^{n} \pi_{i}^{n_i}\) an isotypic decomposition. Then
\[
\langle \chi_{\pi_i}, \chi_{\pi} \rangle = n_i.
\]

Proof. We know from Proposition 10.7 that
\[
\langle \chi_{\pi_i}, \chi_{\pi} \rangle = \dim \text{Hom}(\pi_{i}, \pi).
\]

Therefore,
\[
\langle \chi_{\pi_i}, \chi_{\pi} \rangle = \dim \text{Hom}(\pi_{i}, \pi)
= \dim \text{Hom}\left(\pi_{i}, \bigoplus_{j=1}^{n} \pi_{j}^{n_j}\right)
= \dim \bigoplus_{i=1}^{n} \text{Hom}(\pi_{i}, \pi_{j}^{n_j}) \quad \text{Lemma 6.6}
= \sum_{j=1}^{n} \dim \text{Hom}(\pi_{i}, \pi_{j}^{n_j}) 
= \sum_{j=1}^{n} n_j \cdot \dim \text{Hom}(\pi_{i}, \pi_{j}) \quad \text{Lemma 6.6}
= \sum_{j=1}^{n} n_j \cdot \delta_{ij} \quad \text{Theorem 5.1}
= n_i.
\]
\[\square\]

10.2. The Regular Representation. We will apply the above inner product of Definition 10.4 to deduce Theorem 10.1. We will apply it to the regular representation, which we now define. It may be helpful to note that you have already encountered the regular representation for \(\mathbb{Z}/n\) in Exercise 4.7.

Definition 10.9. For \(G\) a group define the regular representation \((\text{Reg}(G), V)\) as follows: Take \(V\) to be a vector space with basis \(\{e_{g}\}_{g \in G}\) (so \(\dim V = \#G\)). Let \(\text{Reg}(G)\) act on \(V\) by \((\text{Reg}(G)(h))(e_{g}) := e_{hg}\).

Exercise 10.10 (Easy Exercise). Verify \(\text{Reg}(G)\) is indeed a \(G\)-representation.

Theorem 10.11. We have an isotypic decomposition of \(\text{Reg}(G)\) given by
\[
\text{Reg}(G) \simeq \oplus_{\pi \in \text{Irrep}(G)} \pi \oplus \dim \pi \quad \text{(10.1)}
\]
Before proving Theorem 10.11 let’s see why it implies Theorem 10.1.
Theorem 10.11 implies Theorem 10.1. Simply compute dimensions of both sides of Equation 10.1. By construction, \( \dim \text{Reg}(G) = |G| \). On the other hand,

\[
\dim \left( \bigoplus_{\pi \in \text{Irrep}(G)} \pi \oplus \dim \pi \right) = \sum_{\pi \in \text{Irrep} G} \dim(\pi \oplus \dim \pi)
\]

\[
= \sum_{\pi \in \text{Irrep} G} (\dim \pi)^2.
\]

Therefore, \( |G| = \sum_{\pi \in \text{Irrep} G} (\dim \pi)^2 \), as desired. \( \Box \)

It remains only to prove Theorem 10.11. For this, we will need the following concrete description of the character of the regular representation.

Lemma 10.12. We have

\[
\chi_{\text{Reg}(G)}(g) = \begin{cases} 
|G| & \text{if } g = \text{id} \\
0 & \text{if } g \neq \text{id} 
\end{cases}
\]

Proof. Choose the basis of the vector space underlying the regular representation given by \( \{e_g\}_{g \in G} \). Then, since \((\text{Reg}(G)(h))(e_g) = e_{gh}\), observe that \( \text{tr} \text{Reg}(G)(h) \) is precisely \( \{g \in G : gh = g\} \) (make sure you understand why for yourself!). But if \( gh = g \) then necessarily \( h = \text{id} \). So, this number is 0 if \( h \neq \text{id} \). If \( h = \text{id} \), then \( \text{Reg}(G)(\text{id}) = \text{id} \). Since the vector space underlying \( \text{Reg}(G) \) is \( |G| \) dimensional, we obtain \( \text{tr} \text{Reg}(G)(\text{id}) = |G| \). \( \Box \)

Proof of Theorem 10.11. By Corollary 10.8, it suffices to prove that for \((\pi, V)\) any irreducible representation, we have

\[
\langle \chi_{\text{Reg}(G)}, \chi_{\pi} \rangle = \dim \pi_i.
\]

To see this, recall that for any representation \( \pi, \chi_{\pi}(\text{id}) = \dim \pi \), and so

\[
\langle \chi_{\text{Reg}(G)}, \chi_{\pi} \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_{\text{Reg}(G)}(g) \cdot \overline{\chi_{\pi}}(g)
\]

\[
= \frac{1}{|G|} \left( \chi_{\text{Reg}(G)}(\text{id}) \cdot \overline{\chi_{\pi}}(\text{id}) + \sum_{g \neq \text{id}} \chi_{\text{Reg}(G)}(g) \cdot \overline{\chi_{\pi}}(g) \right)
\]

\[
= \frac{1}{|G|} \left( |G| \cdot \dim \pi + \sum_{g \neq \text{id}} 0 \cdot \overline{\chi_{\pi}}(g) \right) \tag{Lemma 10.12}
\]

\[
= \frac{1}{|G|} (|G| \cdot \dim \pi)
\]

\[
= \dim \pi.
\]

\( \Box \)
11. THE NUMBER OF IRREDUCIBLE REPRESENTATIONS

Throughout this section, we work over \( \mathbb{C} \). In this section, among other things, we show that the number of irreducible representations is equal to the number of conjugacy classes. In order to do this, we will need to define a notion of class function, which are functions constant on conjugacy classes. It will be evident that the dimension of the space of class functions is equal to the number of conjugacy classes. We will show that characters of irreducible representations form a basis for the space of class functions, and therefore the number of irreducible representations equals the number of conjugacy classes.

**Definition 11.1.** A class function is a map of sets \( f : G \to \mathbb{C} \) so that \( f(g) = f(h) \) if \( g \) and \( h \) are conjugate in \( G \). Let \( \text{Class}(G) \) denote the set of class functions on \( G \).

**Remark 11.2.** By Lemma 1.24 we see that for any \( G \)-representation \( (\rho, V) \), the character \( \chi_\rho \in \text{Class}(G) \).

**Remark 11.3.** Because addition and scalar multiplication preserves class functions, \( \text{Class}(G) \) can be given the structure of a \( \mathbb{C} \) vector space. Explicitly, if \( f \) and \( h \in \text{Class}(G) \), \( a \in \mathbb{C} \) and \( g \in G \), then \((f + h)(g) := f(g) + h(g)\) and \((a \cdot f)(g) = a \cdot (f(g))\).

**Exercise 11.4.** For \( c \in \text{Conj}(G) \) a conjugacy class, define
\[
f_c : G \to \mathbb{C} \quad g \mapsto \begin{cases} 1 & \text{if } g \in c \\ 0 & \text{if } g \notin c. \end{cases}
\]
Show the set of functions \( \{f_c\}_{c \in \text{Conj}(G)} \) form a basis for \( \text{Class}(G) \). Conclude \( \dim \text{Class}(G) = \# \text{Conj}(G) \).

As mentioned above, the main result we will show in this section is the following:

**Theorem 11.5.** For \( G \) a finite group, the set of class functions \( \{\chi_\pi\}_{\pi \in \text{Irrep}(G)} \) form a basis for \( \text{Class}(G) \).

**Proof.** Since a set is a basis if and only if it is independent and a spanning set, this follows from Lemma 11.10 and Proposition 11.11 below. \( \square \)

Let’s deduce our motivating consequence:

**Corollary 11.6.** For \( G \) a finite group,
\[
\# \text{Irrep}(G) = \# \text{Conj}(G).
\]
Proof. By Theorem 11.5, the set of characters or irreducible representations form a basis for Class(G). Therefore, \( \dim \text{Class}(G) = \# \text{Irrep}(G) \).

However, by Exercise 11.4, we know \( \dim \text{Class}(G) = \# \text{Conj}(G) \). Hence, \( \# \text{Irrep}(G) = \dim \text{Class}(G) = \# \text{Conj}(G) \). □

11.1. Proving characters are independent. We prove Theorem 11.5 by showing characters of irreducible representations are independent and span Class(G). Let’s start by showing they are independent. For this, we begin by upgrading the temporarily defined pairing in Definition 10.4 to a bona fide pairing on Class(G).

Definition 11.7. Define an inner product on the space of class functions as follows: If \( f, h \in \text{Class}(G) \) define the pairing

\[
\langle f, h \rangle := \frac{1}{\#G} \sum_{g \in G} f(g) \overline{h(g)}.
\]

Remark 11.8. Note that in particular if we take \( f = \chi_\pi, h = \chi_\rho \), then \( \langle f, h \rangle \) defined as in Definition 11.7 agrees with \( \langle \chi_\pi, \chi_\rho \rangle \) as defined in Definition 10.4.

Exercise 11.9 (Properties of the inner product on class functions). For \( f, g, h \in \text{Class}(G) \) and \( a \in \mathbb{C} \), check the following properties of the inner product on class functions (usually a map \( V \times V \to \mathbb{C} \) is called an inner product on \( V \) if it satisfies these properties):

\[
\begin{align*}
(1) \quad \langle f, g + h \rangle &= \langle f, h \rangle + \langle f, g \rangle \\
(2) \quad \langle f + g, h \rangle &= \langle f, h \rangle + \langle g, h \rangle \\
(3) \quad \langle af, h \rangle &= a \langle f, h \rangle \\
(4) \quad \langle f, ah \rangle &= \bar{a} \langle f, h \rangle \\
(5) \quad \langle f, f \rangle &\in \mathbb{R}_{\geq 0} \\
(6) \quad \langle f, f \rangle = 0 \iff f = 0.
\end{align*}
\]

Lemma 11.10. The set of class functions \( \{ \chi_\pi \}_{\pi \in \text{Irrep}(G)} \) are independent.

Proof. Suppose there are some constants \( a_\pi \in \mathbb{C} \) so that \( \sum_{\pi \in \text{Irrep}(G)} a_\pi \chi_\pi = 0 \). We want to show that \( a_\pi = 0 \) for all \( \pi \in \text{Irrep}(G) \). In order to pick out the coefficient \( a_\rho \), we take the inner product with \( \chi_\rho \). More precisely, for
\[\rho \in \text{Irrep}(G),\]
\[0 = \langle 0, \chi_\rho \rangle\]
\[= \left\langle \sum_{\pi \in \text{Irrep}(G)} a_\pi \chi_\pi, \chi_\rho \right\rangle\]
\[= \sum_{\pi \in \text{Irrep}(G)} a_\pi \langle \chi_\pi, \chi_\rho \rangle\] \hspace{1cm} \text{(Exercise 11.9)}
\[= \sum_{\pi \in \text{Irrep}(G)} a_\pi \delta_{\pi\rho}\] \hspace{1cm} \text{(Lemma 10.5)}
\[= a_\rho.\]
So \(a_\pi = 0\) for all \(\pi \in \text{Irrep}(G)\), as we wanted to show. \(\square\)

11.2. **Proving characters form a basis for class functions.** In order to prove the set of characters of irreps form a basis for the space of class functions, we only need to show they span all class functions.

**Proposition 11.11.** The set of class functions \(\{\chi_\pi\}_{\pi \in \text{Irrep}(G)}\) span the space of all class functions.

**Assuming Proposition 11.13.** Suppose \(f : G \to \mathbb{C}\) is some class function. To see that \(f\) lies in the span of the \(\chi_\pi\). We are free to modify it by linear combinations of the \(\chi_\pi\). Define \(\tilde{f} := f - \sum_{\pi \in \text{Irrep}(G)} \langle f, \chi_\pi \rangle \chi_\pi\). We claim \(\langle \tilde{f}, \chi_\pi \rangle = 0\) for all \(\pi \in \text{Irrep}_G\). Once we verify this, it will follow from Proposition 11.13 below that \(\tilde{f} = 0\) and therefore
\[f = \sum_{\pi \in \text{Irrep}(G)} \langle f, \chi_\pi \rangle \chi_\pi \in \text{Span} \langle \chi_\pi \rangle.\]

So, conditional on Proposition 11.13, we only need to check \(\langle \tilde{f}, \chi_\pi \rangle = 0\).

**Exercise 11.12.** Verify this, completing the proof. \textit{Hint:} expand out the definition of \(\tilde{f}\) and use Exercise 11.9. \(\square\)

To complete the proof of Theorem 11.5 we have reduced to showing the following:

**Proposition 11.13.** If \(f\) is a class function so that \(\langle f, \chi_\pi \rangle = 0\) for all \(\pi \in \text{Irrep}(G)\) then \(f = 0\).

**Proof.** The proof of this is a bit tricky, so we subdivide it into steps. For \((\pi, V)\) a \(G\)-representation, we consider the \(T_{f,\pi} := \sum_{g \in G} f(g) \pi(g^{-1}) : V \to V\). The motivation for considering this is that it is closely related to the inner product \(\langle f, \chi_\pi \rangle\), which we are assuming is 0.
11.2.1. Step 1: $T_{f,\pi}$ is a map of representations. We first claim $T_{f,\pi} : (\pi, V) \to (\pi, V)$ is a map of representations. That is, we want to check

\[
\begin{array}{c}
\pi(h) \circ T_{f,\pi} = T_{f,\pi} \circ \pi(h)
\end{array}
\]

commutes. This follows from the following computation:

\[
\pi(h)T_{f,\pi} = \pi(h) \left( \sum_{g \in G} f(g)\pi(g^{-1}) \right)
\]

\[
= \sum_{g \in G} f(g)\pi(hg^{-1})
\]

\[
= \sum_{a \in G} f(h^{-1}ah)\pi \left( h \left( h^{-1}ah \right)^{-1} \right)
\]

setting $g := h^{-1}ah$

\[
= \sum_{a \in G} f(a)\pi(h^{-1}a^{-1}h)
\]

since $f$ is a class function

\[
= \sum_{a \in G} f(a)\pi(a^{-1}h)
\]

\[
= \left( \sum_{a \in G} f(a)\pi(a^{-1}) \right)\pi(h)
\]

\[
= T_{f,\pi} \circ \pi(h)
\]

11.2.2. Step 2: $T_{f,\pi} = 0$ for $\pi$ irreducible. We saw in the previous step $T_{f,\pi}$ defines a map of representations. If $\pi$ is irreducible, it follows from Schur’s lemma [Theorem 5.1] that $T_{f,\pi}$ must be $a \cdot \text{id}$ for some scalar $a \in \mathbb{C}$. Therefore, it only remains to prove $a = 0$. Since $\text{tr} T_{f,\pi} = \text{tr}(c \cdot \text{id}) = \dim \pi \cdot a$, it suffices to show $\text{tr} T_{f,\pi} = 0$. Indeed, by our assumption on $f$,

\[
\text{tr} T_{f,\pi} = \text{tr} \left( \sum_{g \in G} f(g)\pi(g^{-1}) \right)
\]

\[
= \sum_{g \in G} f(g) \text{tr} \pi(g^{-1})
\]

\[
= \langle f, \chi_{\pi} \rangle
\]

\[
= 0
\]
11.2.3. Step 3: $T_{f,\pi} = 0$ for all representations $\pi$. By Maschke’s theorem [Theorem 4.5], we can write $\pi \sim \bigoplus_{i=1}^{n} \pi_i$ for $\pi_i$ irreducible representations. It follows that $T_{f,\pi} = \bigoplus_{i=1}^{n} T_{f,\pi_i}$. Here, if $T_i : V_i \to V_i$ are linear maps,
\[
\bigoplus_{i=1}^{n} T_i : \bigoplus_{i=1}^{n} V_i \to \bigoplus_{i=1}^{n} V_i
\]
denotes the “block diagonal” linear map defined by
\[
\left( \bigoplus_{i=1}^{n} T_i \right)(v_1, \ldots, v_n) = (T_1(v_1), \ldots, T_n(v_n)).
\]
It follows from the previous step that each $T_{f,\pi_i} = 0$ and hence $T_{f,\pi} = 0$.

11.2.4. Step 4: Concluding the proof. We apply the previous step in the case that $\pi = \text{Reg}(G)$. We have $T_{f,\text{Reg}(G)} = 0$, meaning that for $V$ the underlying vector space of $\text{Reg}(G)$ with basis $\{e_g\}_{g \in G}$, the function
\[
\sum_{g \in G} f(g) \pi(g^{-1}) : V \to V
\]
is the 0 map. We wish to show this means $f(g) = 0$ for all $g \in G$. Indeed,
\[
0 = \left( \sum_{g \in G} f(g) \pi(g^{-1}) \right)(e_{\text{id}}) = \sum_{g \in G} f(g)e_{g^{-1}}.
\]
Since the set $\{e_{g^{-1}}\}_{g \in G}$ form a basis of $V$, and $\sum_{g \in G} f(g)e_{g^{-1}}$ is a dependence relation between these basis elements, we must have $f(g) = 0$ for all $g \in G$, as desired. \(\square\)
12. Dimensions of Irreps Divide the Order of the Group

In this section, we work over \( \mathbb{C} \). Via a series of exercises, we prove that the dimension of any irreducible representation divides the order of the group. This section assumes familiarity with the notion of integral extensions of rings and algebraic integers, or at least the willingness to take on faith that a sum and product of integral elements is integral. For the remainder of this section, we fix a group \( G \).

The main result is the following, whose proof is concluded below in \red{Exercise 12.10}.

**Theorem 12.1.** Let \( \rho \) be an irreducible complex representation of \( G \). Then \( \dim \rho \mid \#G \).

To prove this, we will need the notion a ring element being integral. We now recall this.

**Definition 12.2.** Let \( R \to S \) be a map of rings. An element \( s \in S \) is integral over \( R \) if \( s \) is a root of some monic polynomial \( \sum_{i=1}^{n} r_i x^i \) with \( r_i \in R \) (where monic means \( r_n = 1 \)). We say \( S \) is integral over \( R \) if every \( s \in S \) is integral over \( R \).

We now state the main result on integral elements which we will need, but do not prove it.

**Theorem 12.3.** If \( R \to S \) is a map of rings and \( a, b \in S \) are integral then so are \( a + b \) and \( a \cdot b \).

We now outline how to prove \red{Theorem 12.1} using \red{Theorem 12.3}.

**Exercise 12.4.** Fix an irreducible complex representation \( (\rho, V) \) of \( G \). The purpose of this exercise is to show \( \chi_{\rho}(g) \) is an integral over \( \mathbb{Z} \).

1. Show that all eigenvalues of \( \rho(g) \) are integral over \( \mathbb{Z} \). \textit{Hint:} Use \red{Exercise 8.10} that \( \rho(g) \) is a diagonalizable matrix. (Really, you only need that \( \rho(g) \) is conjugate to an upper triangular matrix, and in fact every matrix over \( \mathbb{C} \) is conjugate to an upper triangular matrix.)

2. Conclude using \red{Theorem 12.3} that \( \chi_{\rho}(g) \) is an integral over \( \mathbb{Z} \) for every \( g \in G \).

**Exercise 12.5.** Let \( (\rho, V) \) be an irreducible complex \( G \)-representation. The purpose of this exercise is to show that if \( c \subset G \) is a conjugacy class and \( g \in c \), then \( \#c \chi_{\rho}(g) / \chi_{\rho}(1) \) is integral over \( \mathbb{Z} \).

1. Show that every linear combination of elements \( \rho(g) \) for \( g \in G \) is integral over \( \mathbb{Z} \). Here the map \( R \to S \) of \red{Definition 12.2} is the map from the integers to \( \dim \rho \times \dim \rho \) matrices with integer entries, sending \( n \mapsto n \cdot \text{id}_V \).
(2) Let $c \subset G$ be a conjugacy class. Show that $\sum_{g \in c} \rho(g)$ commutes with $\rho(h)$ for all $h \in G$.

(3) Use Schur’s lemma to show

\[ \sum_{g \in c} \rho(g) = \frac{\# c \cdot \chi_{\rho}(g)}{\chi_{\rho}(1)} \cdot \text{id}_V. \]

(4) Conclude that $\# c \cdot \chi_{\rho}(g) / \chi_{\rho}(1)$ is integral over $\mathbb{Z}$.

**Exercise 12.6.** Show that $\# c \cdot \chi_{\rho}(g) \chi_{\rho}(g) / \chi_{\rho}(1)$ is integral over $\mathbb{Z}$ for any $g \in c$. *Hint:* Use Exercise 12.4, Exercise 12.5, and $\chi_{\rho} = \chi_{\rho^\vee}$.

**Exercise 12.7.** Show that

\[ \frac{1}{\chi_{\rho}(1)} \sum_{c \in \text{Conj}(G)} \frac{\# c \chi_{\rho}(c) \chi_{\rho}(c)}{\chi_{\rho}(1)} \]

is integral over $\mathbb{Z}$.

**Exercise 12.8.** Show that $\frac{1}{\chi_{\rho}(1)} \# G$ is integral over $\mathbb{Z}$. *Hint:* Use Exercise 12.7 and Theorem 9.2 (orthogonality of character tables).

**Exercise 12.9.** Show that any $x \in \mathbb{Q}$ which is integral over $\mathbb{Z}$ in fact lies in $\mathbb{Z}$. *Hint:* If $x = a / b$ in reduced form satisfies some monic polynomial of degree more than 1, expand the polynomial to show there are no primes dividing $b$.

**Exercise 12.10.** Prove Theorem 12.1 by showing $\frac{\# G}{\chi_{\rho}(1)}$ is both integral over $\mathbb{Z}$ and a rational number, hence an integer.
APPENDIX A. DEFINITION AND CONSTRUCTIONS OF FIELDS

To this end, we first define fields. After defining fields, if we have one field $K$, we give a way to construct many fields from $K$ by adjoining elements.

A.1. The definition of a field. A field is a special type of ring. So, we first define a ring:

Definition A.1. A commutative ring with unit is a set $R$ together with two operations $\left(+, \cdot\right)$ satisfying the following properties:

1. Associativity: $a + (b + c) = (a + b) + c, a \cdot (b \cdot c) = (a \cdot b) \cdot c$
2. Commutativity: $a + b = b + a, a \cdot b = b \cdot a$
3. Additive identity: there exists $0 \in R$ so that $a + 0 = a$
4. Multiplicative identity: there exists $1 \neq 0 \in R$ so that $1 \cdot a = a$
5. Additive inverses: For every $a \in R$, there is a additive inverse, denoted $-a$ satisfying $a + (-a) = 0$
6. Distributivity of multiplication over addition: $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.

Remark A.2. Any mention of “ring” in what follows implicitly means “commutative ring with unit.” There will be no non-commutative rings or rings without units.

Definition A.3. A field is a ring $K$ such that every nonzero element has a multiplicative inverse. That is, for each $a \in K$ with $a \neq 0$, there is some $a^{-1} \in K$ so that $a \cdot a^{-1} = 1$.

Definition A.4. A finite field is simply a field whose underlying set is finite.

Example A.5. Given any prime number $p$, the set $\mathbb{Z}/p\mathbb{Z}$ forms a field under addition and multiplication. This field is denoted $\mathbb{F}_p$. Nearly all the axioms are immediate, except possibly for the existence of multiplicative inverses.

Exercise A.6. Verify that every nonzero element has a multiplicative inverse in two ways:

1. Use the Euclidean algorithm to show that for any $a < p$ there exists some $b$ with $ab \equiv 1 \mod p$ and conclude that $b$ is an inverse for $a$. 
   Hint: Use that $\gcd(a, p) = 1$.
2. Show that $a^{p-1} = 1$, so $a^{p-2}$ is an inverse for $a$. This is also known as “Fermat’s Little theorem,” not to be confused with “Fermat’s Last theorem,” which is much more difficult. 
   Hint: Show that the powers of any element form a subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times := \mathbb{Z}/p\mathbb{Z} - \{0\}$ under multiplication. Use Lagrange’s theorem (i.e., the order of a subgroup divides the order of the ambient group) to deduce that this subgroup generated by $a$ has order dividing $(\mathbb{Z}/p\mathbb{Z})^\times = p - 1$. Conclude that $a^m = 1$ for some $m$ dividing $p - 1$ and hence $a^{p-1} = 1$. 


A.2. Constructing field extensions by adjoining elements. We now explain how to construct extensions of fields by adjoining elements. Here is a prototypical example:

**Example A.7.** Consider the field $\mathbb{Q}(\sqrt{2})$. How should we interpret this? The elements of this field are of the form $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$.

Multiplication works by $(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$.

Here is another perspective on this field: What is $\sqrt{2}$? It is simply a root of the polynomial $x^2 - 2$. Therefore, we could instead consider the field $\mathbb{Q}[x]/(x^2 - 2)$, where this means the ring where we adjoin a root of the polynomial $x^2 - 2$. Concretely, $\mathbb{Q}[x]$ means polynomials with coefficients in $\mathbb{Q}$, and the notation $\mathbb{Q}[x]/(x^2 - 2)$ means that in any polynomial $f(x)$, we can replace $x^2$ by 2. So for example, if we had the polynomial $x^3 + 2x^2 + 3$ this would be considered equivalent to $(x^2) \cdot x + 2 \cdot (x^2) + 3 = 2x + 4 + 3 = 2x + 7$. In this way, we can replace any polynomial with a polynomial of degree 1 of the form $a + bx$. Identifying $x$ with $\sqrt{2}$ gives the isomorphism of this ring with the above field $\mathbb{Q}(\sqrt{2})$.

**Exercise A.8.** Describe the elements of the fields $K$ as in Example A.7 for $K$ one of the following fields

1. $K = \mathbb{Q}(\sqrt{3})$,
2. $K = \mathbb{Q}(7^{1/5})$,
3. $K = \mathbb{Q}(\zeta_3)$, for $\zeta_3$ a primitive cube root of unity.

In each of the above cases, write $K = \mathbb{Q}[x]/f(x)$ for an appropriate polynomial $f$. In each of the above cases, what is the dimension of $K$ over $\mathbb{Q}$, when $K$ is viewed as a $\mathbb{Q}$ vector space?

**Definition A.9.** Let $K$ be a field. Define the polynomial ring

$$K[x] := \left\{ \sum_{i=1}^{n} a_i x^i : a_i \in K \right\}.$$

For $f \in K[x]$, define

$$K[x]/(f) := K[x]/\sim$$
where $\sim$ is the equivalence relation defined by $g \sim h$ if $f \mid g - h$.

**Exercise A.10.** Show that $K[x]/(x) \cong K$, where the map is given by sending a polynomial to its constant coefficient.

**Lemma A.11.** Let $K$ be a field and let $f \in K[x]$ be a monic irreducible polynomial. Then $K[x]/(f)$ is a field.

**Proof.** Note that $K[x]/(f)$ is a ring as it inherits multiplication and addition and all the resulting properties of a ring from $K[x]$. (Check this!) Therefore, it suffices to check that if $f$ is monic and irreducible, then every element has an inverse. In other words, given any $g \in K[x]/(f)$, we need to show there is some $h$ with $gh = 1$. We can consider $g \in K[x]$ as a polynomial of degree less than $f$. Since $f$ is irreducible, and $\deg g < \deg f$, it follows that the two polynomials share no common factors. Then, by the Euclidean algorithm for polynomials (if you have only seen the Euclidean algorithm over the integers, check that the natural analog to the Euclidean algorithm for the integers works equally well in polynomial rings over arbitrary fields, where the remainder is then a polynomial of degree less than the polynomial you are dividing by) we obtain some $h, k \in K[x]$ with $gh + fk = 1$ as elements of $K[x]$. It follows that $gh \sim 1$ in $K[x]/(f)$ because $gh - 1 = fk \in K[x]$. □

**Exercise A.12.** Let $K$ be a field and $f \in K[x]$ a monic irreducible polynomial. Suppose $L = K[x]/(f)$. Show that $\dim_K L = \deg f$, where $\deg f$ denotes the degree of the polynomial $f$ and $\dim_K L$ denotes the dimension of $L$ as a $K$ vector space.

**Example A.13.** Consider the field $\mathbb{F}_2[x]/(x^2 + x + 1)$. We claim this is a finite field of order 4. Indeed, this holds because the polynomial $x^2 + x + 1$ is irreducible. To check this, we only need to check it has no linear factors. It has a linear factor if and only if $x^2 + x + 1$ has a root in $\mathbb{F}_2$. But, when we evaluate it at 0 we get 1 mod 2 and when we evaluate it at 1, we get 1 mod 2. So it has no roots, and the claim follows from Lemma A.11.

**Exercise A.14.** For any $p > 2$, show that there are exactly $\frac{p+1}{2}$ elements $x \in \mathbb{F}_p$ with $x = y^2$ for some $y \in \mathbb{F}_p$. We call such $x$ squares. Conclude that there is some $x \in \mathbb{F}_p$ which is not a square whenever $p > 2$. **Hint:** Show that if $x = y^2$ then we also have $x = (-y)^2$ and further that there $y$ and $-y$ are the only two elements of $\mathbb{F}_p$ squaring to $x$.

**Example A.15.** Let $p > 2$ be a prime and let $\varepsilon \in \mathbb{F}_p$ be an element which is not a square (which exists by Exercise A.14). Then, $\mathbb{F}_p[x]/(x^2 - \varepsilon)$
is a finite field of order $p^2$. It is order $p^2$ because it is a two dimensional vector space over $\mathbb{F}_p$ spanned by the basis 1 and $x$. It is a field because $x^2 - \epsilon$ is irreducible in $\mathbb{F}_p[x]$. Indeed, to see this, note that if it were not irreducible, it would factor as a product of two linear factors, which means it would have a root. But, if it had a root, there would be some $y \in \mathbb{F}_p$ so that $y^2 = \epsilon$. However, we chose $\epsilon$ not to be a square, and so no root exists.
APPENDIX B. A QUICK INTRO TO FIELD THEORY

In this section, we discuss maps of fields and the characteristic of a field.


**Definition B.1.** Given two fields $K$ and $L$, a map $\phi : K \to L$ is a map of sets sending $1 \mapsto 1, 0 \mapsto 0$ such that $\phi(a +_K b) = \phi(a) +_L \phi(b)$ and $\phi(a \cdot_K b) = \phi(a) \cdot_L \phi(b)$.

**Remark B.2.** Sometimes, a map of fields is referred to as a homomorphism or extension. Whenever we have a map of fields, it is required to be compatible with the addition and multiplication operations, as defined above. If we do not wish to require such compatibility, we will call the map “a map of sets”

**Remark B.3.** We shall typically drop the subscript $+_K, \cdot_K$ on addition and multiplication when it is clear from context.

**Exercise B.4.** Verify from the definition of map that $\phi(a^{-1}) = \phi(a)^{-1}$

and

$\phi(-a) = -\phi(a)$.

We next prove that maps of fields are injective. If you have not worked much with the notion of injectivity before, you may want to try the following exercise first.

**Exercise B.5.** Show that a map of rings is injective (using the definition that $f : R \to S$ is injective if $f(a) = f(b)$ implies $a = b$) if and only if the only element mapping to 0 is 0. *Hint:* Consider $f(a - b)$.

**Lemma B.6.** Any map of fields is injective.

**Proof.** By Exercise B.5 it suffices to show that any $c \neq 0$ does not satisfy $\phi(c) = 0$. Suppose there is some such $c$. But note that $1 = \phi(1) = \phi(cc^{-1}) = \phi(c)\phi(c^{-1}) = 0\phi(c^{-1}) = 0$, a contradiction. Therefore, every nonzero element does not map to 0 and the map is injective. \[\square\]

**Remark B.7.** Because of Lemma B.6, a map of fields is also typically called an **extension of fields** or a field extension.

**Remark B.8.** The property that maps of fields are injective is very special to fields. Indeed, it is not true for groups. For example, the map $\mathbb{Z} \to \{1\}$ is not injective!
Remark B.9. Using Lemma B.6, whenever we have a map of fields $\phi : K \to L$, we can consider $L$ as a vector space over $K$. The map $K \times L \to L$ corresponding to scalar multiplication is given by

$$K \times L \to L$$

$$(a, b) \mapsto \phi(a) \cdot b$$

B.2. Characteristic of a field.

Definition B.10. Let $K$ be a field. If there is some $n$ so that

$$(B.1) \quad n := 1 + 1 + \cdots + 1$$

is equal to 0 in $K$, the the minimal such $n$ is defined to be the characteristic of $K$, denoted $\text{char}(K)$. If no such $n \in \mathbb{Z}_{\geq 0}$ exists, then we say $K$ has characteristic 0.

Example B.11. The rational numbers $\mathbb{Q}$ has characteristic 0, but the field $\mathbb{F}_p$ has characteristic $p$.

Exercise B.12 (Important exercise). Let $p$ be a prime number and suppose $K$ is a field of characteristic $p$. Show that for any $x, y \in K$, we have

$$(x + y)^p = x^p + y^p.$$

Hint: Expand the left hand side using binomial coefficients, and show that $p$ divides nearly all of the binomial coefficients.

B.3. Basic properties of characteristic.

Lemma B.13. The characteristic of any field is either 0 or prime.

Proof. Note that the characteristic cannot be 1 because $1 \neq 0$. So, we have to show that the characteristic is never composite.

Let $n$ be a composite number with $n = fg$ for $f, g > 1$ two factors of $n$.

Exercise B.14. Suppose $a, b \in K$ with $ab = 0$. Then show either $a = 0$ or $b = 0$.

By the above exercise, if $n = fg = 0$, then either $f = 0$ or $g = 0$. Say $f = 0$. But then, we obtain that $f < n$, and so $K$ does not have characteristic $n$. □

Definition B.15. For $K$ a field, we say a subset $K' \subset K$ is a subfield if it is a field and the inclusion $K' \subset K$ is a map of fields (meaning $1 \mapsto 1, 0 \mapsto 0$ and the multiplication and addition are compatible).
Exercise B.16. Verify similarly that any field of characteristic 0 contains $\mathbb{Q}$ as a subfield. Hint: Define a map of fields

$$\phi: \mathbb{Q} \rightarrow K$$

$$\frac{a}{b} \mapsto ab^{-1}.$$ 

Use that $b \in K$ is nonzero by the assumption that $K$ has characteristic 0 to show this is well defined.

Lemma B.17. Any field $K$ of characteristic $p > 0$ (for $p$ a prime) contains $\mathbb{F}_p$ as a subfield.

Proof. Inside $K$, consider the subset $\{0, 1, 2, \ldots, p-1\}$. These form $p$ distinct elements because $\text{char}(K) = p$. By definition, of $n = \underbrace{1 + 1 + \cdots + 1}_n$, the elements $0, 1, \ldots, p - 1$ satisfy the same addition and multiplication rules as $\mathbb{F}_p \simeq (\mathbb{Z}/p\mathbb{Z})$. Therefore, when we restrict the multiplication and addition from $K$ to $\{0, 1, 2, \ldots, p - 1\}$, we realize $\mathbb{F}_p$ as this subfield. $\square$
APPENDIX C. ALGEBRAIC CLOSURES

In this section, we discuss “algebraic closures.”

**Definition C.1.** An extension of fields $\phi : K \to L$ is **finite** if $\phi$ makes $L$ into a finite dimensional vector space over $K$. An extension of fields $\phi : K \to L$ is **algebraic** if for every $a \in L$, there is a finite extension $K \to L_a$ with $L_a \subset L$ a subfield containing $a$.

It is not too difficult to show algebraic closures exists, but to jump to the interesting stuff, we will defer it for later:

**Definition C.2.** A field $K$ is **algebraically closed** if any finite field extension $K \to L$ is an isomorphism.

**Exercise C.3.** Show that the real numbers are not algebraically closed. Show that the rational numbers are not algebraically closed.

**Lemma C.4.** Let $K$ be a field. The following are equivalent.

1. $K$ is algebraically closed.
2. Every monic irreducible polynomial over $K$ has a root.
3. Every monic irreducible polynomial over $K$ factors as a product of linear polynomials.

**Proof.** For (1) $\implies$ (2), we suppose $K$ is algebraically closed and show every monic irreducible polynomial over $K$ has a root. Let $f$ be any monic irreducible polynomial over $K$. Then, $K[x]/(f)$ is a field extension of $K$. Because $K$ is algebraically closed, the natural map $K \to K[x]/(f)$ is an isomorphism. Therefore, $\dim_K K[x]/(f) = 1$ and so $f$ has degree 1 by Exercise A.12 (which says $\deg f = \dim_K K[x]/(f)$), and hence has a root.

Next, if (2) holds, one can prove (3) by induction on the degree of the polynomial.

Finally, for (3) $\implies$ (1), suppose $K$ is not algebraically closed. We want to show there is some irreducible polynomial over $K$ which does not factor completely. Let $L$ be a finite extension of $K$ with the inclusion $K \to L$ not an isomorphism. Since $K \to L$ is an injection it is not a surjection, so we may take some $y \in L \setminus K$. We claim there is some monic irreducible polynomial $f \in K[x]$ with $f(y) = 0$. Indeed, this is the content of the following exercise.

**Exercise C.5.** Let $K \to L$ be an algebraic extension. Show that any element $x \in L$ satisfies some monic irreducible polynomial $f(x) = x^n + k_{n-1}x^{n-1} + \cdots + k_0$, for $k_i \in K$. **Hint:** By definition of an algebraic extension, show that the powers of $x$ satisfy some linear dependence relation, and obtain the monic irreducible polynomial from this relation.
Note that since \( y \not\in K \), the polynomial \( f \) with \( f(y) = 0 \) has degree more than 1. Since \( f \) is irreducible and has degree more than 1, \( f \) does not have a root in \( K \), as we wanted to show. \( \square \)

**Exercise C.6.** Show that the complex numbers are algebraically closed (you may assume that every polynomial over the complex numbers has a root).

**Definition C.7.** A field extension \( K \to \overline{K} \) is an algebraic closure if

1. \( K \to \overline{K} \) is algebraic and
2. \( \overline{K} \) is algebraically closed.

**Exercise C.8.** Let \( K \to L \) be an algebraic extension and let \( \overline{L} \) denote an algebraic closure of \( L \). Show that \( \overline{L} \) is also an algebraic closure of \( K \).

**Theorem C.9** (Existence of algebraic closures). Let \( K \) be a field.

1. \( K \) has an algebraic closure.
2. Any two algebraic closures of \( K \) are isomorphic as field extensions (meaning that for two algebraic closures \( \overline{K}, \overline{K}' \), with \( K \) as a subfield via the maps \( \phi : K \to \overline{K}, \phi' : K \to \overline{K}' \), there is an isomorphism \( f : \overline{K} \to \overline{K}' \) so that \( f \circ \phi = \phi' \)).

**Appendix D. Existence of Algebraic Closures**

We guide the reader through a proof of the existence of algebraic closures in series of exercises.

We first prove the existence of an algebraic closure [Theorem C.9](#), and then show it is unique up to (non-unique) isomorphism. The key to proving the existence of an algebraic closure will be Zorn’s lemma, which we now recall:

**Lemma D.1.** Suppose \( I \) is a partially ordered set. Suppose any totally ordered subset \( I' \subset I \) has a maximum element, i.e., there is some \( i \in I \) with \( i \geq j \) for all \( j \in I' \). Then \( I \) contains a maximal element, i.e., there is some \( i \in I \) so that for any \( j \in I, j \not> i \).

**Remark D.2.** Zorn’s lemma is not a lemma in the conventional sense because it is equivalent to the axiom of choice. Therefore, we will not prove it, but rather take it as an axiom.

We next aim to prove existence of algebraic closures. Logically, if you’d like, you can skip directly to [Exercise D.5](#). However, it may help your understanding of that exercise if you do the prior exercises first.

**Exercise D.3.** We now prove some basic properties about cardinalities of field extensions.
(1) Show that if \( L \) is an algebraic extension of a finite field \( K \), then \(|L| \leq |Z|\). Here \(|S|\) denotes the set-theoretic cardinality of a set \( S \).

(2) Show that if \( L \) is an algebraic extension of an infinite field \( K \), then \(|L| = |K|\). \( \text{Hint:} \) Show that \( K \) has the same cardinality as \( K[x] \) and defined a map of sets \( L \to K[x] \) by sending an element to its minimal polynomial. Show that there are only finitely many elements with a given minimal polynomial and deduce \(|K| = |L|\).

(3) Conclude that for any infinite field \( K \), if \( T \) is a set with \(|T| > |K|\) then for any algebraic extension \( L \) of \( K \), we have \(|T| > |L|\).

(4) Conclude that for any field \( K \) if \( T \) is an infinite set with \(|T| > |K|\), then \(|T| \geq |L|\) for any algebraic extension \( L \) of \( K \). (By the above, the only interesting case is the case that \( K \) is finite.)

**Exercise D.4.** Assume \( K \) is an infinite field. Using **Exercise D.3**, solve a slightly simplified version of **Exercise D.5** with the modification that \( S \) is any set so that \(|S| > |K|\) (so that there is no intermediate set \( T \) in the picture). Therefore, the addition of \( T \) is only needed to deal with finite fields.

**Exercise D.5** (Difficult exercise). Use Zorn’s lemma to show an algebraic closure of a field \( K \) exists as follows: Let \( T \) be an infinite set with \(|T| > |K|\) and let \( S \) be a set with \(|S| > |T|\).

(1) Consider the partially ordered set

\[ R := \{(L, \phi) : L \text{ is an algebraic extension of } K \text{ and } \phi : L \to S \text{ is a subset}\} \]

Check that one can define a partial ordering on \( R \) by declaring \((L_1, \phi_1) \leq (L_2, \phi_2)\) if \( i : L_1 \to L_2 \) is an algebraic extension, and \( \phi_2 \circ i = \phi_1 \).

(2) Use Zorn’s lemma, **Lemma D.1** to show that \( R \) has a maximal element, call it \((M, \phi)\).

(3) Show that \( M \) is algebraically closed by showing that if \( i : M \to N \) is any algebraic extension then there is a map \( \psi : N \to S \) with \( \psi \circ i(x) = \phi(x) \). \( \text{Hint:} \) Use that \(|N| \leq |M| \leq |T| < S \) and \(|S - M| = |S| > |N - M|\).

**Exercise D.6.** Suppose we have an algebraic extension \( K \subset L \) and \( K \subset \bar{K} \) with \( \bar{K} \) algebraically closed. Show that there is a map of extensions \( L \to \bar{K} \) in the following steps:

(1) Consider the partially ordered set \( I \) of pairs \((M, \phi)\) with \( K \subset M \subset L \) and \( \phi : M \to \bar{K} \) a map of fields. Check that the relation

\[ (M_1, \phi_1) \leq (M_2, \phi_2) \]

if \( M_1 \subset M_2 \) and \( \phi_2|_{M_1} = \phi_1 \) defines a partial ordering on such pairs \((M, \phi)\).
(2) Show that any totally ordered subset \( I' \subset I \) corresponding to a collection \( \{(M_i, \phi_i)\}_{i \in I'} \) has a maximum element given by taking \( (\cup_i M_i, \cup_i \phi_i) \), with \( \cup_i \phi_i \) interpreted suitably.

(3) Using Zorn’s lemma obtain a maximal element \((M, \phi)\) of \( I \).

(4) Verify that the maximum element \((M, \phi)\) has \( M = L \) and conclude there is a map \( L \to \bar{K} \). *Hint:* Suppose \( L \neq M \). Then there is some \( x \in L - M \). Show that \( x \) satisfies some minimal polynomial over \( L \). Deduce there is a map \( M(x) \to \bar{K} \) restricting to the given map \( \phi : M \to \bar{K} \), and hence \((M, \phi)\) was not maximal.

**Exercise D.7.** Prove Theorem C.9(2) using Exercise D.6 as follows:

1. Show that for any two algebraic closures \( \bar{K}_1, \bar{K}_2 \) of the same field \( K \) there is an injective map between \( \phi : \bar{K}_1 \to \bar{K}_2 \).
2. Show that the injective map \( \phi \) is an algebraic extension.
3. Conclude that the map produced \( \bar{K}_1 \to \bar{K}_2 \) is an isomorphism from the definition of algebraic closure.