The structure of $\mathbb{C}[G]$

In our last lecture we proved that if $d_i$ are the degrees of the irreducible representations of $G$ then

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

Our proof made use of the character of the regular representation and Schur orthogonality.

A different approach to this result is to prove the isomorphism

$$\mathbb{C}[G] \cong \bigoplus_i \operatorname{Mat}_{d_i}(\mathbb{C}).$$

The identity $|G| = \sum d_i^2$ then follows by computing the dimensions of both sides.
The identity

\[ \mathbb{C}[G] \cong \bigoplus_i \text{Mat}_{d_i}(\mathbb{C}) \]

is a consequence of **Wedderburn’s theorem**, a structure theorem for semisimple rings. Dummit and Foote relegate the proof of Wedderburn’s theorem to the exercises. But a much better treatment may be found in Lang’s *Algebra*, in the chapter called **Semisimplicity**. I strongly recommend this account.
I will present a simplified discussion that is suitable for group algebras $F[G]$ where $F$ can be a field of characteristic zero (such as $\mathbb{C}$).

**Definition**

A semisimple algebra over the field $F$ is an algebra $R$ that is finite-dimensional as an $F$-vector space, such that if $M$ is an $R$-module and $N$ a submodule, there exists a complementary submodule $P$ such that $M = N \oplus P$.

For example, a group algebra $F[G]$ is a semisimple algebra if the characteristic of $F$ is not a prime dividing $|G|$, by Maschke’s theorem.
Decomposition into simple modules

Let $R$ be an $F$-algebra. If $M$ is a module over $R$ it is a vector space over $F$. We will say it is finite-dimensional if it is finite-dimensional over $F$.

**Proposition**

Let $R$ be a semisimple algebra and let $M$ be a module that is finite-dimensional. Then $M$ is direct sum of simple modules.

**Note:** the assumption that $M$ is finite-dimensional is unnecessary here. See Lang’s *Algebra* Section XVII.2.
Proof

To prove this, we may assume that $M \neq 0$. Then let $N$ be a nonzero submodule of smallest dimension. Clearly $N$ has no proper, nonzero submodules, so it is simple. By assumption, $M = N \oplus P$ and by induction on dimension, $P$ is a direct sum of simple modules. So, therefore is $M$.

**Wedderburn’s theorem** implies that a semisimple algebra $R$ is a direct sum of matrix rings over division algebras over $F$. If $F$ is algebraically closed, then any division algebra over $F$ is just $F$, so this means that a semisimple algebra over an algebraically closed field $F$ is just a direct sum of matrix rings over $F$ itself.
Direct sum of rings

Let us pause to consider a general ring that is a direct sum of other rings.

(Note: it is actually more correct to this as a direct product but we will use the term direct sum.)

Let

$$ R = R_1 \oplus \cdots \oplus R_h $$

with componentwise addition and multiplication.
The identity element 1 has a decomposition

\[ 1 = (e_1, \cdots, e_h) \]

where \( e_i \) is the identity element of \( R_i \). But we will identify \( R_i \) with its image in \( R \) and write

\[ 1 = e_1 + \cdots + e_h. \]

The ring \( R_i \) becomes a two-sided ideal in \( R \) and

\[ R_i = e_iR = Re_i = e_iRe_i. \]

A decomposition associated with a family of idempotents (more general than this) is sometimes called a Peirce decomposition.

- Peirce decomposition (Wikipedia), web link
Central orthogonal idempotents

Since the injection $R_i \rightarrow R$ does not map the identity element $e_i$ of $R$ to 1, we do not call $R_i$ a subring of $R$. However it is a two-sided ideal. The elements $e_i$ satisfy

$$e_i^2 = e_i, \quad e_i e_j = 0 \text{ if } i \neq j.$$ 

Moreover $e_i$ is in the center of $R$. Thus the $e_i$ are central idempotents, and we express the fact that $e_i e_j = e_j e_i = 0$ by saying that the idempotents are orthogonal. Conversely:

**Proposition**

Let $R$ be a ring, and let $1 = e_1 + \cdots + e_h$ with central orthogonal idempotents $e_i$. Then $R_i = Re_i = e_i R$ is a 2-sided ideal, and

$$R = R_1 \oplus \cdots \oplus R_h.$$
Proof

We check that every element $x$ of $R$ can be uniquely written as $x = \sum x_i$ with $x_i \in R_i$. First, there is such a decomposition since $x = x \cdot 1 = \sum x \cdot e_i$ where $x_i = xe_i \in R_i$. To show the decomposition is unique, if $x = \sum x_i$ with $x_i \in Re_i$ then we may use the property

$$x_i e_j = \begin{cases} x_i & \text{if } i = j, \\ 0 & \text{otherwise} \end{cases}$$

to show that $x_i = xe_i$. 
A useful vanishing property

Let \( R \) be a semisimple algebra.

**Proposition**

*Let \( M \) be a simple module and \( L \) a simple left ideal. Then either \( M \cong L \) or \( LM = 0 \).*

Here \( LM \) is the submodule of \( M \) consisting of finite sums

\[
l_1m_1 + \ldots + l_km_k, \quad l_i \in L, m_i \in M.
\]

To prove this assume \( LM \neq 0 \). Pick \( m \in M \) such that \( Lm \neq 0 \) and consider the map \( \phi : L \to M \) defined by \( \phi(x) = xm \). It is easy to see that this is an \( R \)-module homomorphism, and by assumption it is not the zero map. By Schur’s Lemma, it is an isomorphism.
Finite number of isomorphism classes

**Proposition**

*R has only a finite number of isomorphism classes of simple modules.*

To prove this, using the semisimplicity of $R$ we may write

$$R = L_1 \oplus \cdots \oplus L_m$$

where $L_i$ is a simple submodule (left ideal). We may write $1 = \sum l_i$ with $l_i \in L_i$. Then if $M$ is a simple module, $1 \cdot M \neq 0$ so $l_i \cdot M \neq 0$ for some $l_i$. This implies that $M \cong L_i$. Now it is clear that there are at most $m$ classes of simple modules.
The two-sided ideals $R_i$

Now let $M_1, \cdots, M_h$ be representatives of the distinct simple modules. We define $R_i$ to be the sum of all left ideals of $R$ isomorphic to $M_i$.

**Proposition**

$R_i$ is a two-sided ideal.

Indeed $R_i$ is a sum of left ideals, so it is a left ideal. We must show that it is closed under right multiplication. It is enough to show that if $L$ is a left ideal isomorphic to $M_i$, and $r \in R$, then $Lr \subseteq R_i$. There are two cases. If $Lr = 0$, this is obvious. Otherwise, the map $x \mapsto xr$ is a homomorphism $L \rightarrow Lr$ that is not the zero map, so it is an isomorphism by Schur’s Lemma. This means that $Lr$ is a left ideal isomorphic to $M_i$ and so $Lr \subseteq R_i$. This proves that $R_i$ is a right ideal as well as a left ideal.
Orthogonality of the $R_i$

**Proposition**

If $i \neq j$ then $R_iM_j = 0$ and $R_iR_j = 0$.

This is because if $M$ is a simple module and $L$ a simple left ideal then either $M \cong L$ or $LM = 0$. Now $R_i$ is a sum of ideals isomorphic to $M_i$ and $M_j \ncong M_i$, so $R_iM_j = 0$. Also $R_j$ is a sum of ideals to $M_j$, so implies $R_iR_j = 0$. 
Introducing the $e_i$

**Proposition**

We may write $1 = e_i + \cdots + e_j$ with $e_i \in R_i$. If $m \in M_j$ then

$$e_i m = \begin{cases} 
    m & \text{if } i = j, \\
    0 & \text{if } i \neq j.
\end{cases}$$

To prove this, note that $R$ is a direct sum of simple ideals, each of which is contained in some $R_i$. So $R = R_1 + \cdots + R_h$. (We have not yet proved that this sum is direct.) We may therefore write $1 = e_1 + \cdots + e_h$ with $e_i \in R_i$ Now $e_i m = 0$ if $m \in M_j$ with $j \neq i$ since $R_i M_j = 0$. Thus $m = 1 \cdot m = \sum e_i \cdot m = e_j m$ since all but one term is zero. This proves that $e_i m = m$ if $i = j$. 
The $e_i$ are orthogonal idempotents

**Proposition**

If $x \in R_j$ then

$$e_ix = \begin{cases} 
  x & \text{if } i = j, \\
  0 & \text{if } i \neq j.
\end{cases}$$

In particular, $e_i^2 = e_i$ while $e_ie_j = 0$ if $i \neq j$.

Indeed, $R_i$ is a sum of left ideals isomorphic to $M_i$. We have proved that left multiplication by $e_i$ acts as the identity on $M_i$, so it acts as the identity on $R_i$. On the other hand, $R_iR_j = 0$ if $i \neq j$, so $e_ix = 0$ if $i \neq j$. 
The $e_i$ are **central** orthogonal idempotents

**Proposition**

The $e_i$ are central orthogonal idempotents and

$$R_i = e_iR = Re_i.$$

We have

$$R = R_1 \oplus \cdots \oplus R_h.$$  

First let us show that the sum $R = R_1 + \cdots + R_h$ is direct. We must show that if $x_i \in R_i$ and $x_1 + \ldots + x_h = 0$ then each $x_i = 0$. We have

$$0 = \sum_j e_i x_j = x_i$$

by our last Proposition. This proves that $R = \bigoplus R_i$. 
Proof (continued)

We have already proved that the \( e_i \) are orthogonal idempotents, but we need to prove they are central. It is enough to show that \( e_i x = x e_i \) if \( x \in R_j \). Both are zero if \( i \neq j \), so we have only to show that \( x e_i = x \) when \( i = j \). We have

\[
x = x \cdot 1 = \sum x \cdot e_i = x e_j
\]

since \( x e_i = 0 \) when \( i \neq j \). This proves that \( e_i \) are central orthogonal idempotents.

The idempotent \( e_i \) serves as identity element in the ideal \( R_i \), which then becomes a ring.
The $R_i$ are rings but not subrings

We have made a lot of progress towards proving Wedderburn’s theorem. Let us say that a ring is **simple** if it is semisimple and has a unique isomorphism class of simple left modules. We have proved that a semisimple algebra $R$ decomposes

$$R = R_1 \oplus \cdots \oplus R_h$$

where $R_i$ is a two-sided ideal that is itself a ring with unit $e_i$.

We have noted that the ideals $R_i$ are rings (with unit $e_i$). We do not consider the injection $R_i \hookrightarrow R$ to be a ring homomorphism because it does not take the multiplicative identity element $e_i$ to 1. However the projection $R \twoheadrightarrow R_i$ is a ring homomorphism.
Proposition

$R_i$ is a simple ring.

We must show that $R_i$ has a unique simple isomorphism class of simple modules. If $M$ is a simple $R_i$-module, then by means of the surjection $R \twoheadrightarrow R_i$ we may consider $M$ to be a module for $R$. If $M$ is simple as an $R_i$-module, it is simple as an $R$-module, so $M \cong M_j$ for some $j$. Moreover $e_i \rightarrow e_i$ in the projection $R \twoheadrightarrow R_i$, so $e_i$ acts as the identity on $M$, which tells us that $M \cong M_j$. We have proved that $R_i$ has a unique class of simple modules, and it is easy to see that it is semisimple since $R$ is, and so $R$ is a simple ring.
Wedderburn’s theorem

Theorem (Wedderburn)

A simple ring is a matrix ring over a division ring.

Of course if $R$ is a simple ring that is a finite-dimensional algebra over a field $F$, the division ring is itself a division algebra. So if we prove this theorem of Wedderburn, we have proved that every semisimple algebra is a direct sum of matrix rings over division algebras.

We will prove Wedderburn’s theorem next week.
Division algebras over algebraically closed fields

**Proposition**

*Moreover if $D$ is a finite-dimensional division algebra over an algebraically closed field $F$, then $D = F$.***

Indeed, if $x \in D$ then the powers of $x$ are linearly dependent, proving that $x$ satisfies an algebraic relation over $D$; hence the $F$ algebra $F[x]$ is a finite-dimensional field extension of $F$, but $x$ is algebraically closed so $x \in F$. Therefore $D = F$.

So a simple algebra over an algebraically closed field is just a matrix ring. Note that the unique simple module of $\text{Mat}_d(\mathbb{C})$ is just $\mathbb{C}^d$. 
Application to representations

Thus Wedderburn’s theorem implies that

\[ \mathbb{C}[G] = \bigoplus_{i=1}^{h} \text{Mat}_{d_i}(\mathbb{C}) \]

for some \( d_i \). The simple modules of \( \mathbb{C}[G] \) are the same as the irreducible representations of \( \mathbb{C} \), and the \( d_i \) are their dimensions. Thus comparing the dimensions, we get another proof that

\[ |G| = \sum_{i=1}^{h} d_i^2. \]