PMATH 445/745
Representations of Finite Groups

F. Al-Faisal

Winter 2025

Lectures

To the reader

These notes are meant to supplement (not replace!) my lectures. They will contain proofs of results not proved in class, some further examples and elaborations, and lots of exercises for you to do. I'll be writing things up as I teach the course, so be sure to always download the latest version. If you spot any typos or errors, or if you have any other feedback, please send me an email.

The course. This is an introduction to the representation theory of finite groups. We'll be covering all of the standard topics: representations and subrepresentations, decompositions into irreducible representations, some multilinear algebra and character theory. We will also explore a few prominent applications.

The subject can be broached in a variety of ways. We will begin with a low-tech approach that gets us all the way to the major results of (ordinary) character theory. Afterwards, we will recast everything in terms of modules and algebras. Our representation theoretic results will then arise as consequences of the structure theory of semisimple rings.

All of this material is best illustrated with examples—especially non-trivial ones. Time-permitting, we will look at: Fourier analysis on finite abelian groups; the representation theory of the symmetric group S_n; the representation theory of $GL_2(\mathbb{F}_q)$ (a finite group of Lie type); and the Brauer group of a field. Each example will hopefully deepen your understanding of the abstract theory while simultaneously introducing you to interesting parts of the mathematical landscape.

Prereqs. A solid foundation in linear algebra, group theory and ring theory.

References. There are many excellent sources for the course material. Here are some general recommendations.

For the representation theory of finite groups:

- Your favorite algebra textbook. It probably has a few sections devoted to this.
- James and Liebeck, *Representations and Characters of Groups*, 2nd Ed., Cambridge, 2001.
- Serre, *Linear Representations of Finite Groups*, Springer, 1977.

For module theory and non-commutative algebra:

- Your favorite algebra textbook.
- Beachy, *Introductory Lectures on Rings and Modules*, LMS, 1999.
- Herstein, *Noncommutative Rings*, AMS, 1994.

Lecture 1 Introduction

"Good grief, not another book on representation theory!"

– C.B. Thomas, *Representations of Finite and Lie Groups*

1.1 What is (group) representation theory?

A good way of studying a given group G is by "representing" its elements as more familiar things, such as matrices or linear maps on a vector space. Doing so will allow us to bring tools from linear algebra to tackle problems in group theory. This strategy has been tremendously successful. For example, character theory (a subfield of representation theory) played a vital role in the classification of all finite simple groups.

The use of representations is not limited to applications to group theory. Indeed, since groups are ubiquitous in math, representation theory appears all over the place, including even in physics and chemistry.[1] Here are some examples. (Don't worry if none of this makes any sense; I'm only trying to give you an idea of the broad reach of the subject.)

- If E is an elliptic curve over $\mathbb{Q}$, then there is a representation of the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on something called the Tate module of E. This representation encodes important arithmetic features of E. (See: proof of Fermat's Last Theorem!)
- More generally, representations of Galois groups have become part and parcel of modern day number theory. They form one of the cornerstones of the *Langlands program*, a highly active research program at the interface of number theory and harmonic analysis.
- If $\mathcal{V}$ is a vector bundle over a smooth manifold M with flat connection ∇, then for each $p \in M$ there is a representation of the fundamental group $\pi_1(M, p)$ on the fibre $\mathcal{V}_p$. These representations encode important information about the pair $(\mathcal{V}, \nabla)$.
- Representations of fundamental groups of manifolds also show up in knot theory where they are used to construct knot invariants.
- The representation theory of the symmetric group S_n is intertwined with combinatorial gadgets called Young tableaux. This is a launching point for the field of combinatorial representation theory, where problems in representation theory give rise to interesting combinatorial phenomena (and vice versa).
- In quantum physics, the symmetry group of a quantum system (typically a Lie group) has a representation on the Hilbert space of possible quantum states of particles in the system. Therefore, the representation theory of Lie groups plays an important role in physics.[2] As a concrete example: the representation theory of the Lie group $SU(3)$ led to the discovery of quarks and the omega baryon Ω^-. These particles were postulated to exist by mathematics (representation theory) before they were confirmed to exist by experiment.

[1] The book by Serre mentioned in the preface was initially written for chemists.

[2] Initially, this was much to the dismay of some physicists, who referred to the intrusion of group theory on physics as the *Gruppenpest*.

In addition to all of this, representation theory is a beautiful subject in its own right. This reason alone makes it worthy of study!

Here is the formal definition of a *representation*; I will elaborate on it in the next section.

Definition 1.1. Let G be a group and F be a field. A **representation of G over F** is a pair (V, ρ), where V is an F-vector space and

$$\rho\colon G \to GL(V)$$

is a group homomorphism from G to the group[3] $GL(V)$ of invertible linear maps from V to V. We call V the **representation space** of ρ, and we will often just say "V is a representation of G."

Remark 1.2. Contrary to what you might expect, we do not require ρ to be injective. (The added flexibility will end up being very useful.) If ρ is injective, we say that the representation is **faithful**.

So if V is a representation of G, then each $g \in G$ gives an invertible linear map $\rho(g)\colon V \to V$. If V is finite-dimensional, with say $\dim_F V = n$, then by choosing a basis for V we can equivalently define a representation as being a homomorphism

$$\rho\colon G \to GL_n(F),$$

where $GL_n(F)$ is the group of invertible $n \times n$ matrices with entries in F. In this case, each $g \in G$ gives us an invertible $n \times n$ matrix $\rho(g)$.

Example 1.3. Let $G = C_4$ be the cyclic group of order 4, say with generator a. We can view the elements $1, a, a^2, a^3$ of G as being rotations by 0, 90, 180, 270 degrees (resp.) in the plane. Explicitly, if we define $\rho\colon C_4 \to GL_2(\mathbb{R})$ by

$$\rho(1) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \rho(a) = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \quad \rho(a^2) = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \quad \rho(a^3) = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix},$$

then you can easily check that ρ is a representation of C_4. In fact, since a presentation of G is $\langle a\colon a^4 = 1\rangle$, you just need to check that $\rho(a)$ satisfies $\rho(a)^4 = 1$. It's also clear that ρ is faithful.

Exercise 1.4. Give an example of a faithful representation $\rho\colon C_n \to GL_2(\mathbb{R})$.[4] ▶

We will see many more examples later on.

[3] The group operation being composition. The group $GL(V)$ is called the **general linear group** of V.
[4] Click on ▶ to go to the solution.

1.2 Group actions

To naturally arrive at the definition of "representation" given in Definition 1.1, we should start with the more basic concept of a *group action*. Groups act on things—that's part of what makes them useful and interesting. For example, the symmetric group S_n acts on the set $\{1, 2, \ldots, n\}$ by permuting its elements, i.e. $\pi \in S_n$ sends i to $\pi(i)$. The general linear group $GL_n(\mathbb{R})$ acts on $\mathbb{R}^n$ by having $T \in GL_n(\mathbb{R})$ send $v \in \mathbb{R}^n$ to $T(v) \in \mathbb{R}^n$. The Galois group $\text{Gal}(E/F)$ of a Galois extension E/F acts on E by having σ send e to $\sigma(e)$. Etc.

Exercise 1.5. Think of three other examples. ▶

The formal definition is as follows.

Definition 1.6. Let G be a group. A **group action** of G on a set X is a function

$$G \times X \to X,$$

written as $(g, x) \mapsto g \cdot x$ (or just gx), that satisfies:

(i) $e \cdot x = x$, where $e \in G$ is the identity element.

(ii) $(gh) \cdot x = g \cdot (h \cdot x)$ for all $g, h \in G$.

If we have a group action of G on X, we call X a G**-set**, and we say that G **acts on** X.

Example 1.7. We saw a few concrete examples above; here are some abstract examples:

(a) Any group can be made to act on any nonempty set X by setting $g \cdot x = x$ for all $x \in X$. We call this the **trivial action** and we say that G acts **trivially** on X.

(b) Every group G acts on itself by left multiplication:

$$g \cdot x = gx, \quad g, x \in G.$$

(c) If H is a normal subgroup of G, then G acts on H by conjugation:

$$g \cdot h = ghg^{-1}, \quad g \in G,\ h \in H.$$

(d) If H is a subgroup of G, then G acts on the set G/H of left cosets of H by

$$g \cdot (xH) = (gx)H, \quad g \in G,\ xH \in G/H.$$

If $H = \{e\}$, then this example is essentially the same as the one in part (b).

Exercise 1.8. A group action of G on X is called **faithful** if the only element in G that fixes every $x \in X$ is the identity element (that is, if $g \cdot x = x$ for all $x \in X$ then $g = e$).

Which of the actions in Example 1.7 is faithful? ▶

1.3 The map $G \to \mathrm{Sym}(X)$

If G acts on X, then every $g \in G$ defines a function $a_g\colon X \to X$ by $a_g(x) = g \cdot x$. This function is a bijection with inverse given by $a_{g^{-1}}$. So if we let $\mathrm{Sym}(X)$ denote the set of bijections $X \to X$, then we can define a map

$$G \to \mathrm{Sym}(X)$$

by sending g to a_g. In fact, $\mathrm{Sym}(X)$ is more than just a set: it's a group![5] The **fundamental fact** you need to know about group actions is that the above map is a homomorphism. In fact, we can equivalently define "group action" as "homomorphism $G \to \mathrm{Sym}(X)$." This is the content of the next proposition.

Proposition 1.9. If G acts on X, then the map $\alpha\colon G \to \mathrm{Sym}(X)$ defined by $\alpha(g) = a_g$ is a group homomorphism. Conversely, if $\alpha\colon G \to \mathrm{Sym}(X)$ is a group homomorphism, then we can define a group action of G on X by setting $g \cdot x = \alpha(g)(x)$.

Furthermore, the action of G on X is faithful if and only if the homomorphism α is injective.

Proof: Straightforward book-keeping. If you've never seen this before, you should *definitely* supply all the details and ponder this result until it becomes second nature. ■

Exercise 1.10. Prove Proposition 1.9. ▶

Example 1.11. Applying Proposition 1.9 to the (faithful) action of G on itself by left multiplication, we get an injective homomorphism $G \hookrightarrow \mathrm{Sym}(G)$. If G is finite of order n, so that $\mathrm{Sym}(G) \cong S_n$, this proves Cayley's theorem: Every finite group of order n embeds into S_n.

1.4 Representations are linear actions

We will often encounter a group G that acts on a set X that has additional structure. For example, X could be a vector space, or a ring, or a topological space, etc. In such a case, it might be desirable to restrict attention to actions that preserve this additional structure. So we would ask that each $g \in G$ act on X as a linear map, ring homomorphism, continuous map, etc.

So, for example, if G is acting on an F-vector space V, then we will want each $g \in G$ to satisfy the additional property that

$$g \cdot (cx + y) = c(g \cdot x) + g \cdot y \quad \text{for all } x, y \in V,\ c \in F.$$

[5] The group operation being composition. $\mathrm{Sym}(X)$ is the *symmetric group on* X. If X is a finite set of size n then $\mathrm{Sym}(X) \cong S_n$.

In terms of our map $G \to \text{Sym}(V)$, this means we want the image to land in the subgroup

$$\text{Sym}_{\text{linear}}(V) = \{T \in \text{Sym}(V) \colon T \text{ is linear}\}$$

of *linear* bijections on V. This subgroup is of course none other than the general linear group $GL(V)$! Thus, by Proposition 1.9, an action of G on V by linear maps is the same as a homomorphism

$$G \to GL(V).$$

This is precisely the definition of representation given in Definition 1.1. So now we see what a representation of a group G really is: it is a *linear action* of G on a vector space.

Although the rest of the course will focus primarily on linear actions, it will be a good idea to acquaint yourself with general group actions. They tend to show up all over the place in math. The problem set below contains a few fundamental results that you should know.

Lecture 1 Problems

1.1. Let X be a G-set and let $x \in X$. The **stabilizer** of x in G, denoted by G_x, is the set of all $g \in G$ that fix x, that is, $G_x = \{g \in G \colon gx = x\}$. The G-**orbit** of x is the set $Gx = \{gx \in X \colon g \in G\}$ of images of x under the action of G.

   (a) Prove that G_x is a subgroup of G.

   (b) Prove that distinct G-orbits are disjoint. Deduce that X is a disjoint union of G-orbits.

   (c) Suppose that $x, y \in X$ lie in the same G-orbit. Prove that their stabilizers in G are conjugate.

   (d) Show that the map map $G \to Gx$ sending g to gx induces a bijection $G/G_x \xrightarrow{\sim} Gx$. [**Note:** G_x need not be normal in G. Here we are merely viewing G/G_x as the set of left cosets of G_x in G.]

   (e) Deduce:

      (i) If G is finite, then $|Gx| = [G \colon G_x]$. This is the **Orbit-Stabilizer Formula**.

      (ii) If G is finite, then the size of any G-orbit must divide $|G|$.

      (iii) If X is finite, and if $Gx_1, \ldots, Gx_t$ are the distinct G-orbits in X, then $|X| = \sum_{i=1}^{t} [G \colon G_{x_i}]$.

1.2. Let X be a G-set and assume both X and G are finite. In this problem you will prove **Burnside's Lemma**, which states that the number of G-orbits is equal to the average number of fixed points of the elements of G.

   (a) Let $Y = \{(g, x) \in G \times X \colon gx = x\}$. Show that $|Y| = \sum_x |G_x|$ and $|Y| = \sum_g |X^g|$, where $X^g = \{x \in X \colon gx = x\}$ is the fixed-point set of $g \in G$.

   (b) Using the Orbit-Stabilizer Formula, deduce that $\frac{1}{|G|} \sum_g |X^g| = \sum_x \frac{1}{|Gx|}$.

(c) Prove Burnside's Lemma:

$$\text{number of } G\text{-orbits in } X = \frac{1}{|G|}\sum_{g\in G} |X^g|.$$

1.3. Let X be a G-set. We say that the action of G on X is **transitive** if there is exactly one G-orbit in X—or, equivalently, if for each $x, y \in X$, there is a $g \in G$ such that $y = gx$.

(a) Determine the $GL_2(\mathbb{R})$-orbits in $\mathbb{R}^2$ (under the obvious action) and deduce that $GL_2(\mathbb{R})$ acts transitively on $\mathbb{R}^2 - \{\vec{0}\}$.

(b) Let $SL_2(\mathbb{R}) = \{A \in GL_2(\mathbb{R})\colon \det A = 1\}$. This is the 2×2 **special linear group** with coefficients in $\mathbb{R}$. Does $SL_2(\mathbb{R})$ act transitively on $\mathbb{R}^2 - \{\vec{0}\}$?

(c) What are the $GL_2(\mathbb{Z})$-orbits in $\mathbb{Z}^2$? Here $GL_2(\mathbb{Z})$ is the group of invertible 2×2 integer matrices whose inverse is also an integer matrix; in particular, if $A \in GL_2(\mathbb{Z})$ then $\det A = \pm 1$.

1.4. It's tempting to let S_n "act" on $\mathbb{R}^n$ by permuting the entries of $x = (x_1, \ldots, x_n)$. That is, given $\pi \in S_n$, define $\pi x = (x_{\pi(1)}, \ldots, x_{\pi(n)})$.

(a) Show that this does **not** define a group action of S_n on $\mathbb{R}^n$ if $n > 2$. In fact, show that $(\pi\tau)x = \tau(\pi x)$.

(b) Show that $\pi x = (x_{\pi^{-1}(1)}, \ldots, x_{\pi^{-1}(n)})$ defines a group action of S_n on $\mathbb{R}^n$.

(c) Let S_n act on the standard basis $\{e_1, \ldots, e_n\}$ of $\mathbb{R}^n$ by $\pi e_i = e_{\pi(i)}$. Extend this linearly to an action on all of $\mathbb{R}^n$ by defining

$$\pi(x_1e_1 + \cdots + x_ne_n) = x_1e_{\pi(1)} + \cdots + x_ne_{\pi(n)}.$$

Show that this is exactly the same action defined in part (b).

[**Note:** Amusingly, the first definition of πx given above has appeared in a few sources (including a published textbook) as an example of a group action. The necessity of using π^{-1} on the indices of x will appear in a different guise later (for example, in the next problem!). The heart of the issue is that our definition of "group action" is really a *left* action. The faulty definition is an example of a *right* action, where instead of requiring $(gh)x = g(hx)$, one requires $(gh)x = h(gx)$; this reads better if we write the action on the right, viz. $x(gh) = (xg)h$. It reads better still if we write x^g for the result of g acting on x—now we have $x^{gh} = (x^g)^h$.]

1.5. **Important lesson:** If G acts on X, then G naturally acts on functions on X.

Let X be a G-set, let Y be a set, and let $\mathcal{F}(X, Y)$ be the set of functions $f\colon X \to Y$.

(a) Given $g \in G$ and $f \in \mathcal{F}(X, Y)$, define $g \cdot f$ by $(g \cdot f)(x) = f(gx)$. Show that this does **not** define an action of G on $\mathcal{F}(X, Y)$

(b) Given $g \in G$ and $f \in \mathcal{F}(X, Y)$, define $g \cdot f$ by $(g \cdot f)(x) = f(g^{-1}x)$. Show that this defines an action of G on $\mathcal{F}(X, Y)$.

(c) Explain how the action of S_n on $\mathbb{R}^n$ in the previous problem can be viewed as an instance of this general procedure. [Hint: Find X and Y so that $\mathbb{R}^n = \mathcal{F}(X, Y)$.]

(d) If F is a field then $V = \mathcal{F}(X, F)$ is an F-vector space with respect to the usual definitions of function addition and scalar multiplication. Show that the action of G on V, defined as in part (b), is linear.

(e) If both X and Y are G-sets, show that we can define a G-action on $\mathcal{F}(X, Y)$ by $(g \cdot f)(x) = gf(g^{-1}x)$. Note that this reduces to part (b) if the G-action on Y is trivial.

Lecture 2 Basic Notions and Examples

2.1 Terminology and conventions

In what follows G will be a group, F will be a field, and all vector spaces will be F-vector spaces. For the time being we impose no further restrictions, but soon we'll restrict our attention to finite groups and finite-dimensional vector spaces, and eventually we'll even put conditions on F.

Recall that a representation of G is a pair (V, ρ) where $\rho\colon G \to GL(V)$ is a group homomorphism. The representation space V becomes a G-set with action given by $gv := \rho(g)v$. This action is *linear* in the sense that

$$g(cv + w) = cgv + gw \quad \text{for all } v, w \in V \text{ and } c \in F.$$

A G-set whose action is linear will be called a **G-module** (or **FG-module**, if we want to emphasize F). The terms "G-module" and "representation of G" are synonyms (thanks to Proposition 1.9).

The **degree** of (V, ρ) is defined by $\deg \rho = \dim V$. If V is infinite-dimensional, we will write $\deg \rho = \infty$ and we won't distinguish between infinite cardinals.

If $\dim V = n$ and if we choose a basis $\mathcal{B}$ for V then each $\rho(g)$ gives a matrix

$$[\rho(g)]_{\mathcal{B}} = [r_{ij}(g)] \in GL_n(F).$$

Letting $r(g) = [r_{ij}(g)]$, we obtain a homomorphism

$$r\colon G \to GL_n(F)$$

which we call a **matrix representation** of G. A different basis gives a different matrix representation r' that is conjugate to r, in the sense that there is an invertible matrix $A \in GL_n(F)$ such that

$$r(g) = Ar'(g)A^{-1} \quad \text{for all } g \in G.$$

Since r and r' are essentially the same representation, we make the following definition.

Definition 2.1. The matrix representations $r\colon G \to GL_n(F)$ and $r'\colon G \to GL_n(F)$ of G are said to be **isomorphic** (or **equivalent**) if there is an invertible matrix $A \in GL_n(F)$ such that

$$Ar(g) = r'(g)A \quad \text{for all } g \in G.$$

Translating all of this back to ρ, we arrive at the notion of isomorphism of representations.

Definition 2.2. The representations $\rho\colon G \to GL(V)$ and $\sigma\colon G \to GL(W)$ are said to be **isomorphic** (or **equivalent**), and we write $(V, \rho) \cong (W, \sigma)$ or simply $V \cong W$, if there is an isomorphism of vector spaces $T\colon V \to W$ such that

$$T \circ \rho(g) = \sigma(g) \circ T \quad \text{for all } g \in G. \tag{1}$$

Such a map T is said to be an **isomorphism** of representations.

In terms the G-actions on V and W, the condition in (1) may be concisely expressed as

$$T(gv) = gT(v) \quad \text{for all } g \in G \text{ and } v \in V. \tag{2}$$

Of course, we have to remember that there are possibly two different G-actions in (2).

Definition 2.3. A linear map $T\colon V \to W$ satisfying condition (1) (or, equivalently, (2)) is said to be G-**linear** or G-**equivariant**.

Thus, an isomorphism of representations is a G-linear map that is bijective.

Exercise 2.4. Show that the inverse of a G-linear bijection is also G-linear. ▶

In summary, there are three (equivalent) ways of looking at a representation of G:

1. As a homomorphism $\rho\colon G \to GL(V)$.
2. As a homomorphism $\rho\colon G \to GL_n(F)$ [if $\dim V = n < \infty$].
3. As an FG-module V (i.e. an F-vector space with a linear G-action).

The passage from the first point to the second is just a matter of choosing a basis and representing linear maps as matrices; in the other direction, we take $V = F^n$ (column vectors) and let matrices act as linear maps in the usual way. The connection with the third point comes from Proposition 1.9; the action is given by $g \cdot v = \rho(g)v$.

The FG-module perspective usually allows for cleaner proofs, while the matrix perspective is helpful for concrete calculations (in small dimensions). It's important to get comfortable with all three perspectives. We will use them interchangeably.

2.2 Examples

Example 2.5. Consider $C_2 = \langle a \rangle$. We can define a representation $\rho\colon C_2 \to GL(\mathbb{R}^2)$ by letting $\rho(a)$ be reflection through the x-axis in $\mathbb{R}^2$ (and of course $\rho(e)$ is the identity map). Note that $\rho(a)^2 = \mathrm{id} = \rho(a^2)$ so ρ is a viable homomorphism. In terms of the standard basis for $\mathbb{R}^2$, the associated matrix representation $r\colon G \to GL_2(\mathbb{R})$ has

$$r(a) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

As a C_2-module, $\mathbb{R}^2$ is equipped with the following action:

$$a \cdot \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x \\ -y \end{bmatrix}.$$

If we choose a different basis, yielding a different matrix representation for C_2, then we get a different representation on $\mathbb{R}^2$ and hence a different C_2-module structure. This new C_2-module is isomorphic to the one above via a change of basis matrix.

For instance, the basis $\left\{ \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ -1 \end{bmatrix} \right\}$ gives a matrix representation $r' \colon C_2 \to GL_2(\mathbb{R})$ with

$$r'(a) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

The representations r and r' are conjugates via the change of basis matrix $A = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$:

$$r'(a^i) = A\ r(a^i)\ A^{-1}.$$

Thus, the corresponding C_2-module structures on $\mathbb{R}^2$ are isomorphic via the C_2-linear map $T \colon \mathbb{R}^2 \to \mathbb{R}^2$ defined by $T(x, y) = (x + y, x - y)$ (so that the standard matrix of T is A). Here, the domain has the C_2 action $a(x, y) = (x, -y)$ while the codomain has the action $a(x, y) = (y, x)$. You should confirm that $T(a(x, y)) = aT(x, y)$.

Remark 2.6 (Group presentations)**.** If $G = \langle g_1, \ldots, g_k \colon r_1, \ldots, r_l \rangle$, then to define a representation $\rho \colon G \to GL(V)$ it suffices to define ρ on the generators g_i in such a way that the images $\rho(g_i) \in GL(V)$ satisfy the corresponding relations. For example, if $G = C_n = \langle a \colon a^n = e \rangle$, then we just need to be sure that the relation $\rho(a)^n = \mathrm{id}$ holds. If $G = D_n = \langle r, s \colon r^n = s^2 = e,\ srs = r^{-1} \rangle$, then we just need to ensure that $\rho(r)^n = \rho(s)^2 = \mathrm{id}$ and $\rho(s)\rho(r)\rho(s) = \rho(r)^{-1}$.

The next batch of examples will reappear throughout the course. You should get familiar with them.

Example 2.7 (Trivial representation)**.** For any group G and any vector space V, let $\rho \colon G \to GL(V)$ be the identity homomorphism. This is a representation (albeit not a very exciting one). In the case where $\dim V = 1$, we call this **the trivial representation** of G. Despite all appearances, the trivial representation is actually quite important. For instance, given a non-trivial representation we will often want to determine if it contain a copy of the trivial representation.

Example 2.8 (One-dimensional representations)**.** If $\dim V = 1$ then $GL(V) \cong GL_1(F) = F^\times$. (The first isomorphism requires a choice of basis.) So, up to isomorphism, a one-dimensional representation is a homomorphism $G \to F^\times$. The trivial representation is an example.

For a more interesting example, let $G = S_n$. Then the sign of a permutation defines a representation $\mathrm{sgn} \colon S_n \to F^\times$, where $\mathrm{sgn}(\pi)$ is $+1$ or -1 according to whether π is even or odd, resp. This is called the **alternating representation** of S_n. Together with the trivial representation, these are the only one-dimensional representations of S_n (Problem 2.2).

For another example, let $G = C_n$ and let a be a generator. A homomorphism $\rho\colon G \to F^\times$ is completely determined by what it does to a, and we just need to ensure that $\rho(a)^n = 1$. Thus, let ω be any nth root of unity in F (not necessarily a primitive one, since there might not be one in F!). Then define $\rho(a^i) = \omega^i$. This is a representation of C_n, and every one-dimensional representation of C_n is of this form for some nth root of unity ω. Equivalence of one-dimensional matrix representations is just equality (since conjugation in $F^\times$ is trivial). So different roots of unity give non-isomorphic representations.

Thus, there are n isomorphism classes of one-dimensional representations of C_n over $\mathbb{C}$ since there are n distinct nth roots of unity in $\mathbb{C}$. In $\mathbb{R}$, the only roots of unity are ± 1, and so we only get one real one-dimensional representation (the trivial one) if n is odd and two if n is even.

Example 2.9 (Standard representation of S_3)**.** The symmetric group S_3 can be viewed as the symmetry group of an equilateral triangle. This gives us a linear action of S_3 on the plane $\mathbb{R}^2$ (imagine placing the centre of an equilateral triangle at the origin) hence a two-dimensional representation $\rho\colon S_3 \to GL_2(\mathbb{R})$. We call this the **standard representation of S_3.**

Explicitly, S_3 has the presentation

$$S_3 = \langle a, b\colon a^3 = b^2 = 1, bab = a^2\rangle,$$

where we may take a and b to be any 3- and 2-cycle, resp. (This is also the standard presentation of the dihedral group D_3.) Geometrically, we may view a as performing a $2\pi/3$-rotation while b is a reflection through one of the axes of the triangle. To find a matrix representation, we need to choose a basis. Place the vertices of the triangle at $v = (1, 0)$, $u = (-1/2, \sqrt{3}/2)$ and $w = (-1/2, -\sqrt{3}/2)$. (These are the real coordinates of the third roots of unity in $\mathbb{C}$.) Then $\{v, u\}$ is a basis for $\mathbb{R}^2$, and moreover $w = -v - u$. In terms of this basis, the $2\pi/3$-rotation and the reflection in the x-axis have matrices

$$A = \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 1 & -1 \\ 0 & -1 \end{bmatrix},$$

resp. We can thus define a representation $\rho\colon S_3 \to GL_2(\mathbb{R})$ by setting $\rho(a) = A$ and $\rho(b) = B$. (It's clear from the geometry that $A^3 = B^2 = I$. But you should also confirm that $BAB = A^2$.)

Exercise 2.10. Show that we can define a representation $\varphi\colon S_3 \to GL_2(\mathbb{R})$ by setting

$$\varphi(a) = \begin{bmatrix} \cos(2\pi/3) & -\sin(2\pi/3) \\ \sin(2\pi/3) & \cos(2\pi/3) \end{bmatrix} \quad \text{and} \quad \varphi(b) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

and prove that φ is isomorphic to the representation ρ in the preceding example. ▶

Lecture 2 Problems

2.1. Recall that the **commutator subgroup** of a group G, denoted by $[G, G]$, is the subgroup generated by all commutators $ghg^{-1}h^{-1}$ in G. This is a normal subgroup of G.

(a) Show that if $\rho\colon G \to GL_1(F)$ is a one-dimensional representation of G then $[G, G] \leq \ker(\rho)$. Thus, ρ induces a representation $G/[G, G] \to GL_1(F)$.

(b) Show that there is a bijection of sets $\mathrm{Hom}(G, GL_1(F)) \cong \mathrm{Hom}(G/[G, G], GL_1(F))$.

[**Note:** $\mathrm{Hom}(A, B)$ is the set of group homomorphisms from A to B. The group $G/[G, G]$ is called the **abelianization** of G and is often denoted by G^{ab}. This problem shows that one-dimensional representations of G are essentially the same thing as one-dimensional representations of G^{ab}.]

2.2. Show that, up to isomorphism, the trivial representation and the alternating representation are the only one-dimensional representations of S_n. [Note that if $\operatorname{char} F = 2$ then the alternating representation is equal to the trivial representation.]

2.3. The group $C_2 = \langle a \rangle$ has exactly two distinct one-dimensional representations over $\mathbb{C}$—namely, $\chi_\pm\colon C_2 \to \mathbb{C}^\times$ given by $\chi_\pm(a) = \pm 1$.

(a) Show that every $\mathbb{C}C_2$-module V can be decomposed as a direct sum $V = V_+ \oplus V_-$ of subspaces where, for $v \in V_\pm$, $a \cdot v = \chi_\pm(a)v$ (that is, $av = v$ for $v \in V$ and $av = -v$ for $v \in V_-$).

(b) The group C_2 acts on $V = M_n(\mathbb{C})$ by $a \cdot A = A^T$. (Note that this is a linear action.) The decomposition $V = V_+ \oplus V_-$ in this case is a familiar one. What is it? That is, describe as succinctly as possible the subspaces $V_\pm$ and the decomposition $A = A_+ + A_-$ of a matrix A into the sum of matrices $A_\pm \in V_\pm$.

(c) Consider now the action of C_2 on $V = \mathbb{C}$ by $a \cdot z = \overline{z}$. Note that this action is $\mathbb{R}$-linear (but not $\mathbb{C}$-linear). Thus, V becomes an $\mathbb{R}C_2$-module. Show that we still have a decomposition $V = V_+ \oplus V_-$ of V into subspaces on which a acts by $a \cdot v_\pm = \chi_\pm(a)v_\pm$ as above. Describe this familiar decomposition in simple words.

2.4. Let (V, ρ) and (W, σ) be representations of $C_2 = \langle a \rangle$ over $\mathbb{C}$. Define $\mathbb{C}$-valued functions χ_V and χ_W on C_2 by

$$\chi_V(a^i) = \mathrm{tr}(\rho(a^i)) \quad \text{and} \quad \chi_W(a^i) = \mathrm{tr}(\sigma(a^i)).$$

Prove:

(a) $\dim V = \chi_V(e)$ and $\dim W = \chi_W(e)$.

(b) $V \cong W$ (as representations) if and only if $\chi_V = \chi_W$ (as functions).

[Hint: Diagonalize!]

2.5. Let (V, ρ) be a representation of a finite group G over $\mathbb{C}$. Show that every $\rho(g) \in GL(V)$ is diagonalizable. [Hint: $g^{|G|} = 1$.]

Lecture 3 Permutation Representations and Linear Algebraic Constructions

In this lecture we will learn how to turn a G-set into a G-module and how to build new representations from old ones.

3.1 Permutation representations

Let G be a group and suppose $X = \{x_1, \ldots, x_n\}$ is a finite G-set. We want to create a G-module out of X—in particular, we want to *linearize* X. I will present two (equivalent) constructions.

3.1.1 Construction 1

Let $F\langle X\rangle$ be the free F-vector space on X. That is, $F\langle X\rangle$ consists of all formal linear combinations

$$a_1x_1 + \cdots + a_nx_n$$

where $a_i \in F$. Vector addition and scalar multiplication are defined in the obvious way. The action of G on X extends by linearity to a linear action on $F\langle X\rangle$:

$$g(a_1x_1 + \cdots + a_nx_n) = a_1(gx_1) + \cdots + a_n(gx_n).$$

This turns $F\langle X\rangle$ into a G-module of degree $|X|$. We call it the **permutation representation** induced by the G-set X. The elements of X are called the **standard basis vectors** of $F\langle X\rangle$.

Example 3.1 (Defining representation of S_n)**.** Let S_n act on $X = \{1, \ldots, n\}$ in the usual way. Then

$$F\langle X\rangle = \{a_1\mathbf{1} + \cdots + a_n\mathbf{n} \colon a_i \in F\},$$

where the standard basis vectors have been typeset in bold for clarity. The induced permutation representation in this case is called the **defining representation** of S_n.

Let's specialize to the case $n = 3$. The action of $\pi \in S_3$ is given by

$$\pi(a_1\mathbf{1} + a_2\mathbf{2} + a_3\mathbf{3}) = a_1\pi(\mathbf{1}) + a_2\pi(\mathbf{2}) + a_3\pi(\mathbf{3}).$$

If we use the standard bases to identify $F\langle X\rangle$ with F^3 via

$$a_1\mathbf{1} + a_2\mathbf{2} + a_3\mathbf{3} \leftrightarrow \begin{bmatrix} a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

then the action of $\pi \in S_n$ will be given by

$$\pi \begin{bmatrix} a_1 \\ a_2 \\ a_3 \end{bmatrix} = \begin{bmatrix} a_{\pi^{-1}(1)} \\ a_{\pi^{-1}(2)} \\ a_{\pi^{-1}(3)} \end{bmatrix}.$$

(See Problem 1.4.) For example, the action of $\pi = (1\ 2\ 3)$ on the basis vectors is given by

$$(1\ 2\ 3) \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \quad (1\ 2\ 3) \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \quad \text{and} \quad (1\ 2\ 3) \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}.$$

Thus, if we let $r\colon S_3 \to GL_3(F)$ be the associated matrix representation, we have

$$r((1\ 2\ 3)) = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

As an exercise, I'll let you confirm that

$$r(1) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad r((1\ 2)) = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad r((2\ 3)) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix},$$

$$r((1\ 3)) = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}, \quad r((1\ 3\ 2)) = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}.$$

You should notice that the above matrices are permutation matrices, i.e., matrices whose columns are a permutation of the columns of the identity matrix. This is a general feature of permutation representations.

Remark 3.2. The construction in this section also works if $X = \{x_i\}_{i \in I}$ is infinite. In this case, $F\langle X \rangle$ consists of all *finite* formal linear combinations of the form $\sum_{i \in I} a_i x_i$ where $a_i = 0$ for all but finitely many $i \in I$. We won't deal with this case in this course.

3.1.2 Construction 2

Another way to "linearize" X is to construct the F-vector space $V = \mathcal{F}(X, F)$ of F-valued functions on X. Each $x \in X$ sits in V as the indicator function e_x defined by

$$e_x(x') = \begin{cases} 1 & \text{if } x = x' \\ 0 & \text{otherwise.} \end{cases}$$

The set $\{e_x \colon x \in X\}$ is a basis of V, which we will call the **standard basis**. So X, once identified with this set, "is" the standard basis of V, just like in our construction of $F\langle X \rangle$.

We can turn V into a G-module by defining $(gf)(x) = f(g^{-1}x)$. (See Problem 1.5.) We also call V the **permutation representation** induced by X.

Exercise 3.3. Let X be a finite G-set, and let $V = \mathcal{F}(X, F)$ be the G-module defined above. Show that V is isomorphic (as a G-module) to the permutation representation induced by X constructed in the previous section. ▶

Remark 3.4. The two constructions of the the permutation representation have their respective merits. We will use them interchangeably, depending on which is more convenient for the task at hand.

The function-space construction is nice because functions are familiar objects—in particular, they come with a slew of adjectives (e.g., bounded, continuous, rapidly decaying, etc.). This allows us to construct (important) versions of the permutation representation when X is infinite, where the free vector space definition doesn't generalize quite as nicely.

3.1.3 The regular representation

We are now going to consider a specific instance of the permutation representation construction that is *extremely important* (as you will come to learn).

Let $G = \{g_1, \ldots, g_n\}$ be a finite group. The **regular representation** V_{reg} of G is the permutation representation induced by the action of G on itself by multiplication (Example 1.7(b)). In terms of the first construction above, we have $V_{\text{reg}} = F\langle G\rangle$. The elements of $F\langle G\rangle$ are formal linear combinations

$$a_1 g_1 + \cdots + a_n g_n$$

and the action of $g \in G$ is given by

$$g(a_1 g_1 + \cdots + a_n g_n) = a_1(gg_1) + \cdots + a_n(gg_n),$$

where gg_i is the group product in G. Note that the degree of the regular representation is $|G|$, and that the elements of G form the standard basis of $F\langle G\rangle$.

Example 3.5. For an illustration, take $G = C_3 = \{e, a, a^2\}$. Then

$$V_{\text{reg}} = F\langle G\rangle = \{c_1 e + c_2 a + c_3 a^2 \colon c_i \in F\}.$$

The action of a on $F\langle G\rangle$ is given by

$$a(c_1 e + c_2 a + c_3 a^2) = c_1 a + c_2 a^2 + c_3 e.$$

Thus, if $r\colon C_3 \to GL_3(F)$ is the associated matrix representation (in the standard basis), we have

$$r(a) = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

Exercise 3.6. Find the standard matrices of the regular representation of C_4. ▶

Remark 3.7. What we've defined here is sometimes called the *left* regular representation, since we're letting G act on itself by left multiplication. The *right* regular representation can be defined analogously by letting G act on itself by right multiplication. Note that even though the latter is not an action according to our definition of "action" (it's a *right* action), it still does give a representation. This is best seen via the function-space construction. Both representations are defined on $V = \mathcal{F}(G, F)$. The left regular representation is given by

$$(gf)(x) = f(g^{-1}x)$$

while the right regular representation is given by

$$(gf)(x) = f(xg).$$

It turns out that the left regular representation is isomorphic to the right regular representation (Problem 3.1).

3.2 New representations from old

We can use linear algebra to construct new representations from known ones.

3.2.1 Subrepresentations

We begin by defining what it means for one representation to contain another.

Definition 3.8. Let V be a G-module. A G**-submodule** (or **subrepresentation**) of V is a subspace $U \subseteq V$ that is G-invariant, that is, $gu \in U$ for all $u \in U$ and $g \in G$.

Exercise 3.9. Show that if $U \subseteq V$ is G-invariant, then $gU = U$ for all $g \in G$. ▶

Note that a G-submodule U of V is itself a representation of G. Indeed, if $\rho\colon G \to GL(V)$ is a representation, then so is $\rho|_U\colon G \to GL(U)$, where $\rho|_U(g) = \rho(g)|_U$. The G-invariance of U guarantees that $\rho(g)|_U$ maps U to U so that $\rho(g)|_U \in GL(U)$. By picking a basis for U and extending it to all of V, we see that the corresponding matrix representation $r\colon G \to GL_n(F)$ takes the form

$$r(g) = \begin{bmatrix} r(g)|_U & * \\ 0 & * \end{bmatrix},$$

i.e., it is block upper-triangular. For instance, if U is a 3-dimensional submodule of a 5-

dimensional module V, then the representation on V will be of the form

$$\begin{bmatrix} * & * & * & * & * \\ * & * & * & * & * \\ * & * & * & * & * \\ 0 & 0 & 0 & * & * \\ 0 & 0 & 0 & * & * \end{bmatrix}$$

where the upper-left 3×3 block is the representation on U.

Example 3.10. If V is any G-module, then 0 and V are G-submodules.

Example 3.11. If V and W are G-modules and $T\colon V \to W$ is G-linear, then $\ker(T)$ and $\operatorname{im}(T)$ are G-submodules of V and W, respectively.

Exercise 3.12. Prove this. ▶

Example 3.13 (Fixed points)**.** For any G-module V, the subset

$$V^G = \{v \in V : gv = v \text{ for all } g \in G\}$$

of G-fixed points is a G-invariant *subspace*, hence is a G-submodule.

For instance, if V is the defining representation of S_3 (see Example 3.1), then $V^{S_3} = \operatorname{span}\{\mathbf{1} + \mathbf{2} + \mathbf{3}\}$ is a one-dimensional subrepresentation that is isomorphic to the trivial representation. In general, V^G will be isomorphic to the *direct sum* (see below) of copies of the trivial representation—the number of copies being equal to $\dim V^G$.

3.2.2 Direct sum of representations

Suppose V and W are G-modules. Then their (external) direct sum

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

becomes a G-module under the action

$$g(v, w) = (gv, gw).$$

If $\rho\colon G \to GL(V)$ and $\sigma\colon G \to GL(W)$ are the corresponding representation, we denote the resulting representation on $V \oplus W$ by $\rho \oplus \sigma$.

Suppose now V and W are finite-dimensional. Choose bases $\{v_i\}_{i=1}^n$ and $\{w_j\}_{j=1}^m$ for V and W and let r and r be the matrix representations corresponding to ρ and σ. The matrix representation T of $\rho \oplus \sigma$ with respect to the basis $\{(v_1, 0), \ldots, (v_n, 0), (0, w_1), \ldots, (0, w_m)\}$ will be block diagonal

$$T(g) = \begin{bmatrix} r(g) & 0 \\ 0 & s(g) \end{bmatrix}$$

with the matrix representations r and s as blocks. We denote this by writing $T(g) = r(g) \oplus s(g)$ and $T = r \oplus s$.

This construction can be generalized to the direct sum of any family of representations.

Example 3.14. If $\rho\colon G \to GL_n(F)$ is the identity homomorphism, then ρ is isomorphic to the direct sum of n copies of the trivial representation.

Remark 3.15 (Internal vs. external direct sums)**.** The construction above is sometimes referred to as the **external** direct sum of vector spaces. There is a notion of an **internal** direct sum of subspaces, which goes as follows. If V is a vector space and U_1 and U_2 are subspaces of V, then we can form the subspace sum

$$U_1 + U_2 = \{u_1 + u_2 \colon u_1 \in U_1, u_2 \in U_2\}.$$

(Note that If V is a G-module and U_1 and U_2 are G-invariant, then so is $U_1 + U_2$.) We say that this subspace sum is **direct** if $U_1 \cap U_2 = \{0\}$ and we denote this by writing $U_1 \oplus U_2$ instead of $U_1 + U_2$.

The condition that $U_1 + U_2$ be direct is equivalent to the assertion that every $v \in U_1 + U_2$ can be expressed as $v = u_1 + u_2$ for *unique* $u_1 \in U_1$ and $u_2 \in U_2$. As a result, the internal direct sum of U_1 and U_2 is canonically isomorphic to their external direct sum $\{(u_1, u_2)\colon u_i \in U_i\}$ via the isomorphism $u_1 + u_2 \mapsto (u_1, u_2)$. (If everything is a G-module, then this is an isomorphism of G-modules.) So using the same notation $U_1 \oplus U_2$ for both constructions should not cause any problems.

Remark 3.16 (Direct sum vs. direct product)**.** If $\{V_i\}_{i \in I}$ is a family vector spaces then their **direct product** $V = \prod_i V_i$ is the set of all ordered tuples $(v_i)_i$ where $v_i \in V_i$ for all i. This is vector space under pointwise addition and scaling, and if each V_i is a G-module, then V is also a G-module under the pointwise action:

$$g(v_i)_i = (gv_i)_i.$$

The **direct sum** $U = \bigoplus_{i \in I} V_i$ is the subspace of V consisting of all tuples $(v_i)_i$ where $v_i = 0$ for all but finitely many i. It also carries the same G-action as above. (So U is a G-submodule of V.) The distinction between the direct sum and the direct product is only relevant if the index set I is infinite.

3.2.3 Dual representation

Let V be a G-module. The dual space V^* of V can be made into a G-module with G-action given by

$$(gf)(v) = f(g^{-1}v) \text{ for } g \in G, f \in V^* \text{ and } v \in V.$$

(Thus, V^* is a G-submodule of $\mathcal{F}(V, F)$.) With this action, we call V^* the **dual** (or **contragredient**) **representation** associated to V. If ρ is the representation on V, we write ρ^* for the dual representation on V^*. In terms of the duality pairing between V and V^*, we have

$$\langle \rho(g)v, \rho^*(g)f \rangle = \langle v, f \rangle . \tag{3}$$

What does this look like in terms of matrices? If $\mathcal{B}$ is a basis for V and $\mathcal{B}^*$ is the corresponding dual basis for V^*, and if r and r^* are the matrix representations of ρ and ρ^* in these bases, then

$$r^*(g) = r(g^{-1})^t \text{ for all } g \in G.$$

That is, the the dual representation is the *inverse transpose* of the original representation.

> **Exercise 3.17.** Prove the above assertion about r^*. [Hint: This is essentially immediate from (3). Alternatively, if you are unfamiliar with the duality pairing, you can proceed directly as follows. Let $\mathcal{B} = \{e_1, \dots, e_n\}$ and $\mathcal{B}^* = \{e_1^*, \dots, e_n^*\}$. Then the (i,j)th entry of $r^*(g)$ is $(ge_j^*)(e_i) = e_j^*(g^{-1}e_i)$.] ▶

Lecture 3 Problems

3.1. Let G be a finite group and let V (resp. U) denote the left (resp. right) regular representation of G. (Refer to Remark 3.7.) Prove that $U \cong V$ as G-modules.

3.2. Let $V = \mathcal{F}(G, F)$ be the regular representation of G. Show that V^G is the subspace of constant functions.

3.3. Let X be a finite G-set and let $V = F\langle X \rangle$ be the induced permutation representation. Show that $\dim V^G$ is equal to the number of G-orbits in X.

3.4. Let $G = S_3$ and let $\sigma = (1\ 2)$ and $\tau = (1\ 2\ 3)$. Note that σ and τ generate G. Let $H = \langle \sigma \rangle$ be the subgroup of G generated by σ, and let $\rho\colon G \to GL(V)$ be the permutation representation induced by the action of G on G/H.

   (a) Write down a basis for V consisting of coset representatives for G/H. Then write down the corresponding matrices for $\rho(\sigma)$ and $\rho(\tau)$.

   (b) Prove that V is isomorphic to the defining representation of S_3.

3.5. Let V be a G-module and let U be a G-submodule of V.

   (a) Show that the quotient space V/U can be made into a G-module by defining $g(v + U) = gv + U$. [Be sure to check that this is well-defined.]

   (b) Show that the First Isomorphism Theorem carries over to the setting of G-modules: Let $T\colon V \to W$ be a G-linear map to a G-module W. Prove that $V/\ker(T) \cong \operatorname{im}(T)$ as G-modules.

   (c) Formulate and prove versions of the Second and Third Isomorphism Theorems for G-modules.

Lecture 4 Tensor Products of Vector Spaces

We're going to pause our discussion of representation theory for a moment to talk about a very useful linear algebraic construction. In brief: Just like how we we can "add" two G-modules V and W by forming their direct sum $V \oplus W$, we can "multiply" V and W by forming their *tensor product* $V \otimes W$.

The tensor product formally mimics how the multiplication of polynomials $f(x) \in F[x]$ and $g(y) \in F[y]$ results in a polynomial $f(x)g(y) \in F[x, y]$. (In fact, $F[x] \otimes F[y] \cong F[x, y]$, as we'll prove below.) It will be helpful to keep this example in the back of your mind as we make our way through the abstract construction.

4.1 The definition of $V \otimes W$

Let V and W be F-vector spaces. We would like to "multiply" $v \in V$ and $w \in W$. As a first approximation, we will take this to mean the element $v \times w := (v, w)$ in the direct product $V \times W$. The problem with this is that it doesn't obey the familiar rules of multiplication. For instance, we would like to have

$$v \times (w_1 + w_2) = v \times w_1 + v \times w_2,$$

but in general

$$(v, w_1 + w_2) \neq (v, w_1) + (v, w_2).$$

The fix is to just *impose* these rules. Let's work in the free vector space $F\langle V \times W\rangle$ on $V \times W$. This vector space consists of all finite formal linear combinations

$$\sum_{(v,w)\in V\times W} c_{(v,w)}\ (v, w),$$

where $c_{v,w} \in F$ and all but finitely many of these $c_{v,w}$ are 0. In $F\langle V \times W\rangle$, let S be the subspace spanned by all vectors of the form

$$\begin{aligned}
&(v, w_1 + w_2) - ((v, w_1) + (v, w_2))\\
&(v_1 + v_2, w) - ((v_1, w) + (v_2, w))\\
&(cv, w) - c(v, w)\\
&(v, cw) - c(v, w),
\end{aligned}$$

where $v, v_1, v_2 \in V$, $w, w_1, w_2 \in W$ and $c \in F$.

Definition 4.1. The **tensor product** of V and W is the vector space $V \otimes W$ defined by

$$V \otimes W = F\langle V \times W\rangle/S.$$

If we want to emphasize F, we will write $V \otimes_F W$.

The coset $(v, w) + S$ in the quotient space will be denoted by $v \otimes w$. Such an element is called a **pure tensor**. The vectors in $V \otimes W$ are called **tensors**; they are finite linear combinations (in fact, finite sums) of pure tensors.

Warning: Not every tensor is a pure tensor! See Problem 4.2.

By construction, tensors are abstract symbols that obey the following rules:

$$\begin{aligned} v \otimes (w_1 + w_2) &= v \otimes w_1 + v \otimes w_2 \\ (v_1 + v_2) \otimes w &= v_1 \otimes w + v_2 \otimes w \\ cv \otimes w = v \otimes cw &= c(v \otimes w) \end{aligned}$$

for all $v, v_1, v_2 \in V$, $w, w_1, w_2 \in W$ and $c \in F$.

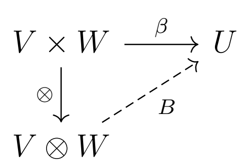
Exercise 4.2. Show that $v \otimes 0 = 0 \otimes w = 0 \otimes 0$ for all $v \in V$ and $w \in W$. ▶

The above rules can be summarized by saying that the function

$$\begin{aligned} \otimes \colon V \times W &\to V \otimes W \\ (v, w) &\mapsto v \otimes w \end{aligned}$$

is *bilinear*. This bilinear map can be used to characterize the tensor product. I won't fully explain what this means (since it's not relevant to our course[6]), but the key point is that we have the following result.

Theorem 4.3 (Universal Property of $\otimes$)**.** Let V, W and U be F-vector spaces. For each bilinear map $\beta \colon V \times W \to U$, there exists a unique linear map $B \colon V \otimes W \to U$ such that $\beta = B \circ \otimes$. In other words, the following diagram commutes:



Proof (Sketch): Define $B(v \otimes w) = \beta(v, w)$ and then extend by linearity to the whole of $V \otimes W$. Things that must be checked: B is well-defined; B is linear; B is the unique linear map satisfying $\beta = B \circ \otimes$. All of this is straightforward symbol-juggling. ■

The universal property tells us that in order to define a linear map B with domain $V \otimes W$, it suffices to define a bilinear β map with domain $V \times W$ and then let $B(v \otimes w) = \beta(v, w)$. Let's see how this is used in practice.

Example 4.4. For any F-vector space V, we have $F \otimes V \cong V$. An isomorphism is given by letting $B \colon F \otimes V \to V$ be the linear map induced by the bilinear map

$$\begin{aligned} \beta \colon F \times V &\to V \\ (a, v) &\mapsto av. \end{aligned}$$

[6] If you're curious, see Problem 4.7.

The inverse map $B^{-1}\colon V \to F \otimes V$ is given by $B^{-1}(v) = 1 \otimes v$, as you can check.

Note that, in particular, $F \otimes F \cong F$, where we identify $a \otimes b$ with ab.

Example 4.5 (Extension of scalars)**.** Let $F \subseteq K$ be fields and suppose V is an F-vector spaces. Viewing K as an F-vector space, we can form the tensor product $V_K := K \otimes_F V$. By construction V_K is an F-vector space. However, it can naturally be be made into a K-vector space by defining

$$b(\sum_i a_i \otimes v_i) = \sum_i (ba_i) \otimes v_i, \text{ for } b, a_i \in K, v_i \in V.$$

We usually omit the $\otimes$ and write av instead of $a \otimes v$. If $a \in F$ then $a \otimes v = 1 \otimes av$ so in this case the short-hand notation av coincides with scalar multiplication in V. Note that V sits inside V_K as the subspace $\{1 \otimes v\colon v \in V\}$.

The process of constructing V_K from V is called **extension of scalars** from F to K.

Exercise 4.6. Let V be an $\mathbb{R}$-vector space. Show that an arbitrary element of $V_{\mathbb{C}} = \mathbb{C} \otimes_{\mathbb{R}} V$ can be written in the form $v + iu = 1 \otimes v + i \otimes u$ for some $v, u \in V$. The $\mathbb{C}$-vector space $V_{\mathbb{C}}$ is called the **complexification** of V. ▶

Example 4.7. Let's show that $F[x] \otimes F[y] \cong F[x, y]$ as F-vector spaces. (In fact, they're isomorphic as F-*algebras*, as we will see later in the course.)

The map $\beta\colon F[x] \times F[y] \to F[x, y]$ defined by $\beta(f(x), g(y)) = f(x)g(y)$ is bilinear hence induces a linear map $B\colon F[x] \otimes F[y] \to F[x, y]$ such that $B(f(x) \otimes g(y)) = f(x)g(y)$. The map B is our desired isomorphism. To prove this, we construct an inverse. Define

$$\begin{aligned} C\colon F[x, y] &\to F[x] \otimes F[y] \\ \sum_{i,j} a_{ij} x^i y^j &\mapsto \sum a_{ij} x^i \otimes y^j. \end{aligned}$$

It's clear that $B \circ C = \mathrm{id}$. For the other direction, first observe that the bilinearity of $\otimes$ allows us to write every tensor in $F[x] \otimes F[y]$ as a linear combination of the pure tensors $x^i \otimes y^j$. So it suffices to show that $(C \circ B)(x^i \otimes y^j) = x^i \otimes y^j$—but this is immediate from the definitions of B and C. Thus, B is an isomorphism and $C = B^{-1}$.

Proposition 4.8 (Tensor Product of Linear Maps)**.** Let $T\colon V \to U$ and $S\colon W \to Z$ be linear maps. There is a unique linear map $T \otimes S\colon V \otimes W \to U \otimes Z$ that satisfies

$$(T \otimes S)(v \otimes w) = T(v) \otimes S(w)$$

for all $v \otimes w \in V \otimes W$.

Proof: The function $\beta\colon V \times W \to U \otimes Z$ defined by $\beta(v, w) = T(v) \otimes S(w)$ is bilinear. Now apply the universal property. ■

Our next result is more subtle to prove. Try to prove it yourself before looking at the proof.

> **Proposition 4.9.** Let V and W be F-vector spaces. Suppose that $v_1, \ldots, v_k \in V$ are linearly independent and that $w_1, \ldots, w_k \in W$ are arbitrary. Then $\sum_{i=1}^k v_i \otimes w_i = 0$ if and only if $w_i = 0$ for all i.

Proof: Note that $v \otimes 0 = v \otimes 0 \cdot 0 = 0(v \otimes 0) = 0$. So if $w_i = 0$ for all i then certainly $\sum_i v_i \otimes w_i = 0$.

Conversely, suppose that $\sum_i v_i \otimes w_i = 0$. Since the v_i are linearly independent, we can find linear functionals $f_1, \ldots, f_k \in V^*$ such that $f_i(v_j) = \delta_{ij}$. [Proof: Extend $\{v_1, \ldots, v_k\}$ to a basis $\mathcal{B}$ for V; then we can define a linear functional on V by defining it on $\mathcal{B}$ in however way we want. Define f_i on the v_j as indicated and define it to be zero on the remaining vectors in $\mathcal{B}$.] Let $g \in W^*$ be an arbitrary linear functional. Using the previous proposition, coupled with the identification $F \otimes F \cong F$, we obtain functionals $f_j \otimes g$ on $V \otimes W$ that satisfy

$$(f_j \otimes g)(v \otimes w) = f_j(v) \otimes g(w) = f_j(v)g(w).$$

Applying $f_j \otimes g$ to $\sum_i v_i \otimes w_i = 0$, we end up with

$$0 = (f_j \otimes g)\left(\sum_i v_i \otimes w_i\right) = \sum_i f_j(v_i)g(w_i) = g(w_j).$$

Since g was an arbitrary linear functional, it follows that w_j must be 0. Since j was arbitrary, the proof is complete. ■

4.2 A more concrete $V \otimes W$

The universal property is good for proving abstract theorems, but it can be of limited use when it comes to actually working with tensors. For instance, our results in the previous section give no indication as to how large $V \otimes W$ is—in particular, what is its dimension? We can get a better handle on things by working with a basis.

> **Theorem 4.10.** Let V and W be F-vector spaces and let $\mathcal{B}$ and $\mathcal{C}$ be bases for V and W, resp. Then the set
> $$\mathcal{B} \otimes \mathcal{C} := \{v \otimes w\colon v \in \mathcal{B} \text{ and } w \in \mathcal{C}\}$$
> is a basis for $V \otimes W$.

Proof: Since every vector in $V \otimes W$ is of the form $\sum_i v_i \otimes w_i$ for some $v_i \in V$ and $w_i \in W$, it's clear (using the bilinearity of $\otimes$) that $\mathcal{B} \otimes \mathcal{C}$ spans $V \otimes W$.

To prove that $\mathcal{B} \otimes \mathcal{C}$ is linearly independent, take a finite number of vectors in $\mathcal{B} \otimes \mathcal{C}$, say

$v_i \otimes w_{i_j}$ where $i \leq n$ and $j \leq m_i$, and consider

$$\sum_{i,j} c_{ij} v_i \otimes w_{i_j} = 0.$$

Using the bilinearity of $\otimes$, we can re-group terms to get

$$\sum_i v_i \otimes \left(\sum_j c_{ij} w_{i_j} \right) = 0.$$

Now since the v_i are linearly independent, Proposition 4.9 implies that

$$\sum_j c_{ij} w_{i_j} = 0.$$

Then, since the w_{i_j} are linearly independent, it follows that all of the c_{ij} are 0. ■

Corollary 4.11. If V and W are finite-dimensional, then $\dim V \otimes W = \dim V \dim W$. ■

Example 4.12. If $V = F[x]$ and $W = F[y]$ and if we take $\mathcal{B} = \{x^i\}_{i=0}^{\infty}$ and $\mathcal{C} = \{y^j\}_{j=0}^{\infty}$, then Theorem 4.10 says that $\mathcal{B} \otimes \mathcal{C} = \{x^i \otimes y^j\}_{i,j}$ is a basis for $F[x] \otimes F[y]$. The isomorphism

$$\begin{gathered} F[x,y] \cong F[x] \otimes F[y] \\ \sum_{i,j} a_{ij} x^i y^j \leftrightarrow \sum_{i,j} a_{ij} x^i \otimes y^j \end{gathered}$$

from Example 4.7 can now be understood simply as the isomorphism that matches up the bases $\{x^i y^j\}$ and $\{x^i \otimes y^j\}$.

Example 4.13. We have $F^n \otimes F^m \cong F^{nm}$. This follows by comparing dimensions, but we can be a bit more explicit. If $e_1, \ldots, e_n$ and $f_1, \ldots, f_m$ are the standard basis vectors for F^n and F^m, then $e_1 \otimes f_1, e_1 \otimes f_2, \ldots, e_1 \otimes f_m, \ldots, e_n \otimes f_1, \ldots e_n \otimes f_m$ are basis vectors for $F^n \otimes F^m$. With this ordering, we have the following identification between vectors in $F^n \otimes F^m$ and vectors in F^{nm}:

$$\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \otimes \begin{bmatrix} y_1 \\ \vdots \\ y_m \end{bmatrix} \leftrightarrow \begin{bmatrix} x_1 y_1 \\ x_1 y_2 \\ \vdots \\ x_1 y_m \\ \vdots \\ x_n y_1 \\ \vdots \\ x_n y_m \end{bmatrix}.$$

Example 4.14 (Kronecker product)**.** The previous example can be extended to define a product between matrices. If $A \in M_{m\times n}(F)$ and $B \in M_{p\times q}(F)$, we define their **Kronecker product** to be the matrix $A \otimes B \in M_{mp\times nq}(F)$ given by

$$A \otimes B = \begin{bmatrix} a_{11}B & \cdots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \cdots & a_{mn}B \end{bmatrix}.$$

For instance,

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} = \left[\begin{array}{cc|cc} 1 & 0 & 2 & 0 \\ 0 & 2 & 0 & 4 \\ \hline 3 & 0 & 4 & 0 \\ 0 & 6 & 0 & 8 \end{array}\right].$$

If you look back at Proposition 4.8, where we defined the tensor product $T \otimes S$ of linear maps, you should be able to convince yourself that (in the appropriate bases) the matrix of $T \otimes S$ is the Kronecker product of the matrices of T and S.

Exercise 4.15. Fill in the details! ▶

4.3 $V \otimes W$ as a G-module

Finally, if V and W are G-modules, we can turn $V \otimes W$ into a G-module by defining

$$g(v \otimes w) = gv \otimes gw$$

and extending this to the whole of $V \otimes W$ by linearity.

In terms of the homomorphisms $\rho\colon G \to GL(V)$ and $\sigma\colon G \to GL(W)$, the G-module $V \otimes W$ carries the representation

$$\begin{aligned} \rho \otimes \sigma\colon G &\to GL(V \otimes W) \\ g &\mapsto \rho(g) \otimes \sigma(g), \end{aligned}$$

where $\rho(g) \otimes \sigma(g)$ is defined as in Proposition 4.8. In matrix form (in the appropriate bases), the matrix of $(\rho \otimes \sigma)(g)$ is the Kronecker product of the matrices of $\rho(g)$ and $\rho(\sigma)$.

Remark 4.16. There is a different way of making a representation out of $V \otimes W$. Namely, we can define a linear $G \times G$-action by

$$(g_1, g_2)(v \otimes w) = g_1 v \otimes g_2 w.$$

This turns $V \otimes W$ into a $G \times G$-module. This construction can be generalized to the case where V and W are representations of different groups: If V is a G-module and W is an H-module then $(g, h)(v \otimes w) = gv \otimes hw$ turns $V \otimes W$ into a $G \times H$-module.

Lecture 4 Problems

4.1. Prove that $0 \otimes w = v \otimes w = 0 \otimes 0$.

4.2. Let $\{e_1, e_2\}$ be a basis for $\mathbb{R}^2$ and let $z = e_1 \otimes e_2 + e_2 \otimes e_1$. Show that z is not equal to a pure tensor in $\mathbb{R}^2 \otimes \mathbb{R}^2$.

4.3. Let V and W be F-vector spaces and let $z \in V \otimes W$. Prove:

(a) There exist linearly independent $v_1, \ldots, v_n \in V$ such that $z = \sum_{i=1}^{n} v_i \otimes w_i$ for some $w_i \in W$.

(b) If $z \neq 0$ then we can arrange for the w_i in part (a) to be linearly independent too. [Hint: Consider the smallest n for which z is the sum of n pure tensors.]

4.4. Let V, W and U be F-vector spaces. Prove that there are canonical isomorphisms:

(a) $(V \otimes W) \otimes U \cong V \otimes (W \otimes U)$.

(b) $(V \oplus W) \otimes U \cong (V \otimes U) \oplus (W \otimes U)$.

4.5. Let X and Y be finite G-sets. The set $X \times Y$ can be made into a G-set with action given by $g(x, y) = (gx, gy)$. Prove that there is an isomorphism $F\langle X \times Y\rangle \cong F\langle X\rangle \otimes F\langle Y\rangle$ of the associated permutation representations.

4.6. Let V and W be finite-dimensional. Prove that $(V \otimes W)^* \cong V^* \otimes W^*$. In fact, prove the following more precise result. Let $\mathcal{B} = \{v_i\}_{i=1}^{n}$ and $\mathcal{C} = \{w_j\}_{j=1}^{m}$ be bases for V and W and let $\mathcal{B}^* = \{v_i^*\}_{i=1}^{n}$ and $\mathcal{C}^* = \{w_j^*\}_{j=1}^{m}$ be the corresponding dual bases for V^* and W^*. Then there exists an isomorphism $T\colon V^* \otimes W^* \to (V \otimes W)^*$ such that $\{T(v_i \otimes w_j)\}_{i,j}$ is the dual basis for $(V \otimes W)^*$ corresponding to the basis $\mathcal{B} \otimes \mathcal{C}$ for $V \otimes W$. [Hint: Start by defining a bilinear map $\beta\colon V^* \times W^* \to (V \otimes W)^*$. There's really only one sensible choice for how to define $\beta(v_i^*, w_j^*)(v \otimes w)$!]

4.7. Suppose that Z is an F-vector space and that $\varphi\colon V \times W \to Z$ is a bilinear map such that the pair (Z, φ) satisfies the universal property of $(V \otimes W, \otimes)$ given in Theorem 4.3. (Meaning: For each bilinear map $\beta\colon V \times W \to U$ there exists a unique linear map $B\colon Z \to U$ such that $\beta = B \circ \varphi$.) Prove that there exists a unique isomorphism $T\colon Z \xrightarrow{\sim} V \otimes W$ such that $T \circ \varphi = \otimes$.

Lecture 5 Hom, Tensor and Trace

More linear algebra!

5.1 Hom spaces

For G-modules V and W, let

$$\mathrm{Hom}(V, W) = \{f : V \to W : f \text{ is a linear map}\}^{7}$$

and

$$\mathrm{Hom}_G(V, W) = \{f : V \to W : f \text{ is a } G\text{-linear map}\}.$$

$\mathrm{Hom}(V, W)$ is naturally a vector space and $\mathrm{Hom}_G(V, W)$ is a subspace of $\mathrm{Hom}(V, W)$. If V and W are finite-dimensional, then by representing linear maps as matrices, we see that $\mathrm{Hom}(V, W)$ is isomorphic to the vector space $M_{m\times n}(F)$ of $m \times n$ matrices, where $m = \dim W$ and $n = \dim V$. In particular,

$$\dim \mathrm{Hom}(V, W) = \dim V \dim W.$$

We can turn $\mathrm{Hom}(V, W)$ into a G-module by defining

$$(gf)(v) = g(f(g^{-1}v)) \text{ for } g \in G, f \in \mathrm{Hom}(V, W) \text{ and } v \in V.$$

Note in particular that $V^* = \mathrm{Hom}(V, F)$ as G-modules (give F the trivial representation). (Compare Problem 1.5, especially parts (d) and (e).)

Exercise 5.1. Show that $\mathrm{Hom}_G(V, W) = \mathrm{Hom}(V, W)^G$. [Recall that U^G is the set of G-fixed points in U.] ▶

The principal result of this lecture is that there is a *canonical* isomorphism

$$V^* \otimes W \cong \mathrm{Hom}(V, W).$$

(Here "canonical" means: does not depend on a choice of basis.) The underlying idea is simple. How can we view $f \otimes w \in V^* \otimes W$ as a linear map $V \to W$? There's really only one natural choice: given $v \in V$, define $(f \otimes w)(v) = f(v)w$. The rest is just book-keeping.

Theorem 5.2. Let V and W be finite-dimensional F-vector spaces. There is an isomorphism

$$T : V^* \otimes W \xrightarrow{\sim} \mathrm{Hom}(V, W)$$

that sends $f \otimes w$ to the linear map $v \mapsto f(v)w$.

If V and W are G-modules, the isomorphism T is G-linear.

[7] A linear map is also called a *homomorphism* of vector spaces, hence the name "Hom" for this set.

Proof: Define $\beta\colon V^* \times W \to \mathrm{Hom}(V, W)$ by

$$\beta(f, w)(v) = f(v)w.$$

Clearly β is bilinear, hence it induces a linear map $T\colon V^* \otimes W \to \mathrm{Hom}(V, W)$ given by

$$T(\sum_i f_i \otimes w_i)(v) = \sum_i f_i(v)w_i.$$

In particular, T sends $f \otimes w$ to the map $v \mapsto f(v)w$. I claim that T is an isomorphism. Since

$$\dim V^* \otimes W = \dim V \dim W = \dim \mathrm{Hom}(V, W),$$

it suffices to prove that T is surjective.

Let's use coordinates for this. Let $\{e_1, \ldots, e_n\}$ be a basis for V, $\{e_1^*, \ldots, e_n^*\}$ be the dual basis for V^*, and $\{f_1, \ldots, f_m\}$ be a basis for W. Then $\{e_i^* \otimes f_j\}$ is a basis for $V^* \otimes W$. On the other hand, a basis for $\mathrm{Hom}(V, W)$ consists of the linear maps η_{ij} defined on the basis $\{e_k\}$ of V by $\eta_{ij}(e_k) = \delta_{kj} f_i$. (Under the isomorphism $\mathrm{Hom}(V, W) \cong M_{m\times n}(F)$, these η_{ij} are the standard unit matrices E_{ij} with a 1 in the (i, j)th position and zeroes elsewhere.) Now simply note that $T(e_j^* \otimes f_i) = \eta_{ij}$, so T takes a basis for $V^* \otimes W$ to a basis for $\mathrm{Hom}(V, W)$. Thus, T is surjective.

It remains to prove that T is G-linear if V and W are G-modules. For this, it suffices to show that

$$T(g(f \otimes w))(v) = (gT(f \otimes w))(v)$$

for all $g \in G$, $f \in V^*$, $w \in W$ and $v \in V$. To this end, we first recall that the G-action on V^* is given by $(gf)(v) = f(g^{-1}v)$. Consequently, we have

$$\begin{aligned} T(g(f \otimes w))(v) &= T(gf \otimes gw)(v) \\ &= [(gf)(v)](gw) \\ &= f(g^{-1}v)\,(gw). \end{aligned}$$

On the other hand,

$$\begin{aligned} (gT(f \otimes w))(v) &= g[T(f \otimes w)(g^{-1}v)] \\ &= g[f(g^{-1}v)w] \\ &= f(g^{-1}v)\,(gw). \end{aligned}$$

So $T(g(f \otimes w))(v) = (gT(f \otimes w))(v)$, as desired. ∎

Exercise 5.3. Prove directly that the map T in the above theorem is injective. ▶

5.2 Trace

The **trace** of a square matrix $A \in M_n(F)$, denoted by $\operatorname{tr}(A)$, is by definition the sum of the diagonal entries of A. Trace is cyclic, in the sense that

$$\operatorname{tr}(ABC) = \operatorname{tr}(BCA) = \operatorname{tr}(CAB) \text{ for all } A, B, C \in M_n(F).$$

Because of this, trace is a similarity invariant:

$$\operatorname{tr}(SAS^{-1}) = \operatorname{tr}(A) \text{ for all } A \in M_n(F) \text{ and } S \in GL_n(F).$$

Consequently, we can define the trace of an operator $T \in \operatorname{Hom}(V, V)$ on a finite-dimensional vector space V to be the trace of the matrix of T in any basis $\mathcal{B}$ of V: $\operatorname{tr}(T) = \operatorname{tr}([T]_{\mathcal{B}})$. Since different bases give similar matrices, $\operatorname{tr}(T)$ is well-defined.

All of this is well and good, but it does feel a bit ad hoc. Why consider the sum of diagonal entries of a matrix to begin with?

Since the trace of a representation will end up playing a crucial role later, it will be worthwhile to have a more organic approach to the concept. The basic idea is that trace defines a linear map

$$\operatorname{tr}\colon \operatorname{Hom}(V, V) \to F.$$

Therefore, in view of the isomorphism $\operatorname{Hom}(V, V) \cong V^* \otimes V$, trace gives a linear map

$$V^* \otimes V \to F.$$

We will now attempt to reverse this line of reasoning. The big question is: *Is there a "natural" linear map that we can define from $V^* \otimes V$ to F?*

A moment's thought should convince you that there is one particularly obvious map here. Namely, evaluation:

$$f \otimes v \mapsto f(v).$$

Surely this is as natural as natural can be. The remarkable thing here is that *evaluation is trace.*

Theorem 5.4. Let V be finite-dimensional, and let $\tau\colon V^* \otimes V \to F$ be the linear map defined by $\tau(f \otimes v) = f(v)$. Then, under the isomorphism $T\colon V^* \otimes V \xrightarrow{\sim} \operatorname{Hom}(V, V)$ of Theorem 5.2, the corresponding linear map $\operatorname{Hom}(V, V) \to F$ is trace. In other words, the following diagram commutes:

$$\begin{array}{ccc} V^* \otimes V & \xrightarrow{\tau} & F \\ {\scriptstyle T}\downarrow & & \downarrow{\scriptstyle \mathrm{id}} \\ \operatorname{Hom}(V, V) & \xrightarrow{\operatorname{tr}} & F \end{array}$$

Proof: Let $\mathcal{B} = \{e_i\}_{i=1}^n$ be a basis for V and let $\mathcal{B}^* = \{e_i^*\}_{i=1}^n$ be the dual basis for V^*. Then, by Theorem 4.10, $\mathcal{B}^* \otimes \mathcal{B} = \{e_i^* \otimes e_j\}_{i,j}$ is a basis for $V^* \otimes V$. So it suffices to prove that

$$\operatorname{tr}(T(e_i^* \otimes e_j)) = \tau(e_i^* \otimes e_j). \tag{4}$$

The right-side is $\tau(e_i^* \otimes e_j) = e_i^*(e_j) = \delta_{ij}$ by definition. For the left-side, first recall from the proof of Theorem 5.2 that the $\mathcal{B}$-matrix of $T(e_i^* \otimes e_j)$ is the matrix E_{ji} with a 1 in the (j,i)th entry and zeroes elsewhere. Thus, $\operatorname{tr}(T(e_i^* \otimes e_j)) = \operatorname{tr}(E_{ji}) = \delta_{ij}$ and so (4) holds. ■

Exercise 5.5. To practice this new perspective, prove the following fundamental property of trace

$$\operatorname{tr}(AB) = \operatorname{tr}(BA) \quad \text{for all } A, B \in M_n(F)$$

by working in $V^* \otimes V$. [**Note:** This can be used to show that trace is cyclic.] ▶

Lecture 5 Problems

5.1. Let G be a finite group and let (V, ρ) be a finite-dimensional $\mathbb{C}G$-module. For each $g \in G$, let $\chi(g) = \operatorname{tr}(\rho(g))$. Prove:

(a) If g and h are in the same conjugacy class of G, then $\chi(g) = \chi(h)$.

(b) $|\chi(g)| \leq \dim V$. [Hint: If $g^k = e$, what can you say about the eigenvalues of $\rho(g)$?]

5.2. Let X and Y be finite G-sets.

(a) Prove that the permutation representation $F\langle X\rangle$ is *self-dual:* $F\langle X\rangle^* \cong F\langle X\rangle$.

(b) Deduce that there is an isomorphism $\operatorname{Hom}(F\langle X\rangle, F\langle Y\rangle) \cong F\langle X \times Y\rangle$ of G-modules, where $X \times Y$ is equipped with the G-action $g(x, y) = (gx, gy)$.

(c) Conclude that $\dim \operatorname{Hom}_G(F\langle X\rangle, F\langle Y\rangle) =$ number of G-orbits in $X \times Y$.

(d) Determine $\dim \operatorname{Hom}_{S_n}(V, V)$, where V is the defining representation of S^n.

5.3. Assume G is finite. Let V be an FG-module and let $\chi\colon G \to F^\times$ be a one-dimensional representation of G. Put $V_\chi = \{v \in V : gv = \chi(g)v\}$ and note that this is a G-submodule of V. Let F_χ denote the G-module determined by χ; that is, $F_\chi = F$ and the action of $g \in G$ on $a \in F$ is given by $g \cdot a = \chi(g)a$.

(a) Show that $\operatorname{Hom}_G(F_\chi, V) \cong V_\chi$ as vector spaces.

(b) Determine $\dim \operatorname{Hom}_G(F_\chi, V_{\text{reg}})$ if χ is the trivial representation of G.

[**Note:** In a sense, $\operatorname{Hom}_G(F_\chi, V)$ is picking out the piece of the representation V that looks like the representation χ. We will elaborate on this very soon.]

5.4. Let V, U and W be F-vector spaces.

(a) (Tensor-Hom adjunction.) Prove that there is a canonical isomorphism

$$\operatorname{Hom}(V \otimes U, W) \cong \operatorname{Hom}(V, \operatorname{Hom}(U, W)).$$

[In fancy lingo, we say that $\otimes$ and Hom are *adjoint functors*.]

(b) Deduce that there is a canonical isomorphism $(V \otimes U)^* \cong V^* \otimes U^*$ if V and U are finite-dimensional. (Compare Problem 4.6.)

Lecture 6 Irreducible Representations

Back to representation theory.

Given a group G, we would like to classify its representations up to isomorphism. If we've identified two representations V and W, and if we come across a third representation U such that $U \cong V \oplus W$ then in some sense we've gained nothing new. So we will want to focus on representations that are "atomic" and cannot be broken up into smaller pieces. There are two candidate definitions for what we might mean by an "atomic" representation.

Definition 6.1. A G-module V is said to be

- **indecomposable** if whenever V is isomorphic to the direct sum of G-modules $V \cong U \oplus W$, then either $U = 0$ or $W = 0$;
- **irreducible** (or **simple**) if $V \neq 0$ and if the only G-submodules of V are 0 and V itself.

We say that V is **decomposable** (resp. **reducible**) if it is not indecomposable (resp. irreducible).

An irreducible module is indecomposable. In general, the converse is false (see Example 6.3 and Problem 6.3 below)—and we will have more to say about this next lecture.

Example 6.2. A 1-dimensional representation is irreducible (hence indecomposable). A 2-dimensional representation will be irreducible if and only if it doesn't contain a 1-dimensional G-invariant subspace. Thus, $\rho\colon G \to GL_2(F)$ is reducible if and only if all of the $\rho(g)$ have a common eigenvector. For dimensions 3 and up, things are not so simple. For example, a 4-dimensional representation may be reducible because it contains a 2-dimensional G-invariant subspace, and such a subspace need not contain any common eigenvectors.

Example 6.3. Let (V, ρ) be the regular representation of $C_2 = \langle a \rangle$ on $V = F\langle C_2 \rangle$. I claim that V is reducible.

In terms of the standard basis $\mathcal{B} = \{1, a\}$ of V, we have

$$[\rho(1)]_{\mathcal{B}} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad [\rho(a)]_{\mathcal{B}} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Since $\dim(V) = 2$ and C_2 is generated by a, a proper submodule is simply just an eigenspace for $\rho(a)$. The eigenspaces of $[\rho(a)]_{\mathcal{B}}$ are easily found to be

$$E_1 = \operatorname{span}\left\{ \begin{bmatrix} 1 \\ 1 \end{bmatrix} \right\} \quad \text{and} \quad E_{-1} = \operatorname{span}\left\{ \begin{bmatrix} 1 \\ -1 \end{bmatrix} \right\}.$$

(Note that $E_1 = E_{-1}$ if $\operatorname{char} F = 2$.) Switching back from coordinate vectors, we obtain the C_2-submodules

$$U_+ = \operatorname{span}\{1 + a\} \quad \text{and} \quad U_- = \operatorname{span}\{1 - a\}$$

of V. So V is reducible since it contains proper, non-zero submodules.

Pushing further though, note that these submodules are irreducible (since $\dim U_\pm = 1$). Moreover, if $\operatorname{char} F \neq 2$ we have

$$V = U_+ \oplus U_-.$$

Explicitly, we can write each $v \in V$ as $v = v_+ + v_-$ where $v_\pm = \frac{1}{2}(v \pm av) \in U_\pm$. Thus, although V itself is not irreducible, it is the direct sum of irreducible representations.

On the other hand, if $\operatorname{char} F = 2$, then $U_+ = U_-$ and this is the *only* G-invariant subspace in V. In particular, we cannot write V as a direct sum of two G-invariant subspaces. So in this case V is indecomposable but reducible.

Example 6.4. Let $\rho\colon C_4 \to GL_2(\mathbb{R})$ be the representation of $C_4 = \langle a \rangle$ defined by letting a act as a 90-degree rotation (see Example 1.3). This representation is irreducible. Indeed, since $\deg \rho = 2$, any proper invariant subspace will have to be one-dimensional and hence will contain an eigenvector for the rotation $\rho(a)$. But $\rho(a)$ has no eigenvectors in $\mathbb{R}^2$.

On the other hand, if we use the same matrices to define $\rho_{\mathbb{C}}\colon C_4 \to GL_2(\mathbb{C})$, then the resulting representation on $\mathbb{C}^2$ is no longer irreducible. In fact, each of the matrices $\rho(a^i)$ is diagonalizable (why?), and because they commute with each other, they are *simultaneously* diagonalizable. In this case it's easy to find the simultaneous eigenbasis by hand (do it!). Thus we can decompose $\mathbb{C}^2$ into a direct sum $\mathbb{C}^2 = U_1 \oplus U_2$ of simultaneous eigenspaces for the matrices $\rho(a^i)$. This is a decomposition into C_4-invariant subspaces.

Example 6.5. The standard representation of S_3 on $\mathbb{R}^2$ (see Example 2.9) is irreducible. Indeed, in this representation a 3-cycle acts a $2\pi/3$-rotation, hence has no real eigenvectors. The representation remains irreducible over $\mathbb{C}$, since although a $2\pi/3$-rotation will now have eigenvectors, these will not be eigenvectors for all of the 2-cycles (reflections). That is, there are no simultaneous eigenvectors, hence no invariant one-dimensional subspaces.

Exercise 6.6. Confirm the above by showing that $A = \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & -1 \\ 0 & -1 \end{bmatrix}$ do not share an eigenvector. ▶

Example 6.7. Let $X = \{1, 2, 3\}$ and let $V = F\langle X \rangle$ be the defining representation of S_3 given in Example 3.1. The subspace $U = \operatorname{span}\{\mathbf{1} + \mathbf{2} + \mathbf{3}\}$ is S_3-invariant hence is a submodule. Assume that $\operatorname{char} F \neq 3$. Then, with a little thought, we discover that

$W = \{a\mathbf{1} + b\mathbf{2} + c\mathbf{3} : a+b+c=0\}$ is an S_3-invariant complement to U in V. Indeed, it's easy to check that $U \cap W = \{0\}$ (this is where we need $\operatorname{char} F \neq 3$) and then it follows that $V = U \oplus W$ for dimension reasons.

The S_3-module U, being one-dimensional, is irreducible. What about W? I'll leave it as an exercise for you to show that W is irreducible. Thus, we've decomposed the defining representation V of S_3 into a direct sum $V = U \oplus W$ of irreducible subrepresentations—at least if $\operatorname{char} F \neq 3$.

Exercise 6.8. Assuming $\operatorname{char} F \neq 3$, prove that W is irreducible by showing that W does not contain a one-dimensional S_3-invariant subspace. If $F = \mathbb{R}$ prove that W is in fact isomorphic to the standard representation from Example 2.9. ▶

In the above examples, we saw that if the given representation V was not irreducible, then we were at at least able to decompose it into a direct sum of irreducible subrepresentations (provided we made some assumption about $\operatorname{char} F$). Are we always able to do this? The answer will be revealed next time! Let's close this lecture by determining all of the irreducible representations of S_3 (over $\mathbb{C}$). First, some notation: Let's write $\operatorname{Irr}_F(G)$ for the set of isomorphism classes of irreducible representation of G over F.

Example 6.9 ($\operatorname{Irr}_{\mathbb{C}}(S_3)$)**.** We have seen three irreducible complex representations so far:

- The trivial representation V_{triv}.
- The alternating (or sign) representation V_{sgn}.
- The standard representation V_{std} (see Example 2.9).

The first two are one-dimensional, while V_{std} is two-dimensional. I claim:

$$\operatorname{Irr}_{\mathbb{C}}(S_3) = \{V_{\text{triv}}, V_{\text{sgn}}, V_{\text{std}}\}.$$

Proof: Suppose that (V, ρ) is an irreducible representation of S_3. Le $a = (1\ 2\ 3)$ and $b = (1\ 2)$. Note that a and b generate S_3. Since $a^3 = 1$, a acts on V as a *diagonalizable* operator $\rho(a)$ with eigenvalues $1, \omega$ and ω^2, where $\omega = \exp(2\pi i/3)$ is a third root of unity. Thus, we have a decomposition

$$V = V_1 \oplus V_\omega \oplus V_{\omega^2}$$

of V into eigenspaces for $\rho(a)$, where $V_\lambda := \{v \in V : \rho(a)v = \lambda v\}$. Of course, these eigenspaces are $\rho(a)$-invariant but need not be G-invariant. Let's consider the action of b. Since $ab = ba^2$, we see that if $v \in V_{\omega^i}$ then $\rho(b)v \in V_{\omega^{2i}}$: Indeed,

$$\rho(a)(\rho(b)v) = \rho(b)(\rho(a)^2 v) = \rho(b)(\omega^{2i} v) = \omega^{2i}(\rho(b)v).$$

Thus, $\rho(b)$ sends V_1 to itself and sends V_ω to V_{ω^2}. In particular, V_1 is S_3-invariant since it is sent to itself by both b and a (and these two elements generate S_3). Since V is irreducible, it follows that either $V_1 = 0$ or $V_1 = V$.

Suppose $V_1 = V$. Since $b^2 = e$, V decomposes into a direct sum $V = U_+ \oplus U_-$ of ± 1-eigenspaces for $\rho(b)$. Since a acts trivially on V_1, it follows that these eigenspaces are G-invariant. Further, any given eigenvector spans a G-invariant subspace. So, since V is irreducible, then either $V = U_+$ or $V = U_-$ and in both cases these eigenspaces are one-dimensional. In the first case, V is the trivial representation and in the second case V is the alternating representation.

On the other hand, if $V_1 = 0$, then we see that $V = V_\omega \oplus V_{\omega^2}$. We have noted that $\rho(b)$ sends V_ω to V_{ω^2} and conversely; thus, we have an isomorphism $\rho(b)\colon V_\omega \to V_{\omega^2}$ of vector spaces. So if $\{v_i\}$ is a basis for V_ω then $\{\rho(b)v_i\}$ is a basis for V_{ω^2}. Set $W_i := \operatorname{span}\{v_i, \rho(b)v_i\}$. This is clearly a G-invariant subspace. Since V is irreducible, it follows that $i = 1$ and $V = W_1$. In particular, $\dim V = 2$. I'll leave it as an exercise for you to check that V is in fact isomorphic to the standard representation. This completes the proof. ■

In particular, if $V \in \operatorname{Irr}_{\mathbb{C}}(S_3)$, then $\dim V \leq 2$.

Exercise 6.10. Show that W_i is isomorphic to the standard representation of S_3. ▶

Remark 6.11. The above ad hoc approach doesn't generalize to arbitrary finite groups. We were fortunate that S_3 contained a subgroup $H = \langle a \rangle \cong C_3$ whose action was both particularly easy to analyze (we decomposed V into a direct sum of H-invariant subspaces) and interacted well with the rest of G (b permuted the H-invariant subspaces). For a general finite group G, there won't be such a magical subgroup H. Curiously, this approach does generalize to certain families of Lie groups and algebraic groups, where one is always able to find a suitable H ("Cartan subgroup").

The other thing worth noting is that if you study the preceding argument carefully and drop the irreducibility assumption on V, then you'll see that we've essentially proved that every complex representation of S_3 is isomorphic to a direct sum of copies of V_{triv}, V_{sgn} and V_{std}. In other words, every complex representation of S_3 decomposes into a direct sum of irreducible representations. Intriguing...

Lecture 6 Problems

6.1. Suppose that V and W are isomorphic G-modules. Prove that if V is indecomposable (resp. irreducible) then W is indecomposable (resp. irreducible).

6.2. Show that every irreducible representation of a finite group is finite-dimensional. [Hint: If $G = \{g_1, \ldots, g_n\}$ and $V \neq 0$ is given, can you construct a G-invariant subspace "by hand"?]

6.3. Let $\mathbb{F}_p$ be the finite field of size p and let $\rho\colon C_p \to GL_2(\mathbb{F}_p)$ be the representation defined by

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

where a is a generator of C_p. Show that ρ is indecomposable but not irreducible. [Hint: If you remember your linear algebra, there is an obvious invariant subspace. Show that this is in fact the *only* invariant subspace.]

6.4. Refer to Example 6.7. Show that the defining representation V of S_3 is indecomposable if char $F = 3$. [Hint: Begin by showing that the only one-dimensional submodule of V is $U = \text{span}\{\mathbf{1} + \mathbf{2} + \mathbf{3}\}$.]

6.5. Let W be the standard representation of S_3 and let U be the alternating representation. Prove that $W \otimes U \cong W$ (as representations of S_3).

6.6. Let V and W be a finite-dimensional G-modules. Prove or disprove:

(a) V^* is irreducible if and only if V is irreducible.

(b) $V \otimes W$ is irreducible if and only if V and W are irreducible.

Lecture 7 Maschke's Theorem

7.1 Complete Reducibility

We raised the following question last lecture.

> Given a representation V, is it possible to decompose V into a direct sum
>
> $$V = U_1 \oplus U_2 \oplus \cdots \oplus U_k$$
>
> of irreducible subrepresentations?

We saw that the answer is sometimes "no." The goal of this lecture is to give a general answer this question. We begin with a definition.

Definition 7.1. A representation is said to be **completely reducible** (or **semisimple**) if it is isomorphic to a direct sum of irreducible representations.

Exercise 7.2. Show that a representation is completely reducible if and only if it is equal to the direct sum of irreducible subrepresentations. ▶

Note that, in this definition, we allow for the possibility of infinite direct sums. However, going forwards, we're going to restrict our attention to finite-dimensional representations. In this case, a representation will be completely reducible if and only if it is isomorphic to a finite direct sum of irreducible representations.

Here is our main result:

Theorem 7.3 (Maschke)**.** Let G be a finite group and assume that $\operatorname{char} F \nmid |G|$. Every finite-dimensional FG-module V is completely reducible.

[The hypothesis $\operatorname{char} F \nmid |G|$ always holds if $\operatorname{char} F = 0$.]

Proof: We will prove Maschke's theorem under the following temporary assumption.

Assumption. If U is a G-submodule of V then U has a G-invariant complement, i.e., there exists a G-submodule W such that $V = U \oplus W$.

We will give two proofs of this assumption in the next two sections (see Proposition 7.11 and 7.17). With this in hand, we can proceed as follows. If V is irreducible, we are done. Otherwise, V has a proper non-zero invariant subspace U. By *assumption*, U has a G-invariant complement W and so $V = U \oplus W$ is a decomposition into G-invariant subspaces. Now apply this argument to U and W. Since $\dim V < \infty$, this procedure must eventually terminate, leaving us with V as a direct sum of irreducible invariant subspaces. ■

Corollary 7.4. If $\operatorname{char} F \nmid |G|$, then a finite-dimensional FG-module is irreducible if and only if it is indecomposable. ■

Remark 7.5. If G is infinite or if $\operatorname{char} F$ divides $|G|$ then the above two results are no longer true. (See Problems 6.3 and 7.1.) In fact, we have the following converse of Maschke's theorem: If G is a finite group and if $\operatorname{char} F$ divides $|G|$, then there exists a finite-dimensional G-module that is not completely reducible (Problem 7.2).

Thus, the theory when $\operatorname{char} F$ divides $|G|$ is decidedly more subtle; the subject matter here is called *modular* representation theory. The case where $\operatorname{char} F \nmid |G|$, in particular when $\operatorname{char} F = 0$, is called *ordinary* representation theory. In this course, we will focus mostly on the ordinary case. So for us, "irreducible" and "indecomposable" are synonyms, thanks to Corollary 7.4.

7.2 Unitarizability

In this section, we restrict F to be either $\mathbb{R}$ or $\mathbb{C}$ (so, in particular, $\operatorname{char} F = 0$). Fix a finite-dimensional G-module V. Our goal is to show that every G-submodule of V has a G-invariant complement W.

How are we to construct such a W? The idea is to put an inner product (this is where we use $F = \mathbb{R}$ or $\mathbb{C}$) on V and then take W to be the orthogonal complement $U^\perp$ of U. However, $U^\perp$ need not be G-invariant in general.

Example 7.6. Consider the representation $\rho\colon C_2 \to GL_2(\mathbb{R})$ defined by

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

Then $U = \operatorname{span}\left\{\begin{bmatrix} 1 \\ 0 \end{bmatrix}\right\}$ is a C_2-submodule. The orthogonal complement of U with respect to the dot product is $U^\perp = \operatorname{span}\left\{\begin{bmatrix} 0 \\ 1 \end{bmatrix}\right\}$—and this is not $\rho(a)$-invariant.

The problem is that the inner product, if chosen at random, has no reason to play nice with the G-action. Let's call an inner product **G-invariant** if it satisfies

$$\langle gv, gw \rangle = \langle v, w \rangle \text{ for all } g \in G \text{ and } v, w \in V.$$

Lemma 7.7. Let V be a G-module equipped with a G-invariant inner product $\langle\ ,\ \rangle$. If U is a G-submodule of V, then its orthogonal complement $U^\perp$ with respect to $\langle\ ,\ \rangle$ is also a G-submodule.

Exercise 7.8. Prove Lemma 7.7. ▶

In terms of the representation $\rho\colon G \to GL(V)$, if V admits a G-invariant inner product $\langle\ ,\ \rangle$, then the linear maps $\rho(g)$ are unitary with respect to $\langle\ ,\ \rangle$. So giving V an invariant inner product **unitarizes** the representation. Remarkably, every finite-dimensional representation can be unitarized.

Proposition 7.9 (Weyl's Unitary Trick)**.** Let G be a finite group and let V be a finite-dimensional G-module (over $\mathbb{R}$ or $\mathbb{C}$). Then V admits a G-invariant inner product.

Proof: Let $\langle\ ,\ \rangle_0$ be any inner product on V. We can obtain a G-invariant inner product by averaging over G.[8] Explicitly, define

$$\langle v, u \rangle := \frac{1}{|G|} \sum_{g \in G} \langle gv, gu \rangle .^{9}$$

It's easy to check that $\langle\ ,\ \rangle$ is an inner product, so let me just confirm that it is indeed G-invariant. Given $h \in G$, we have

$$\langle hv, hu \rangle := \frac{1}{|G|} \sum_{g \in G} \langle g(hv), g(hu) \rangle = \frac{1}{|G|} \sum_{g \in G} \langle (gh)v, (gh)u \rangle .$$

Since $g \mapsto gh$ is a bijection on G, as g runs over the elements of G, so does gh. So we can re-index the sum above to obtain

$$\langle hv, hu \rangle := \frac{1}{|G|} \sum_{k \in G} \langle kv, ku \rangle = \langle v, u \rangle ,$$

completing the proof. ■

Remark 7.10. Weyl's unitary trick also applies to infinite groups provided we can replace the discrete sum $\sum_{g \in G}$ by some kind of G-invariant integral $\int_{g \in G}$. This is possible, e.g., if G is a compact group. This fact is important in the representation theory of Lie groups.

With this in hand, we can now prove our key result.

Proposition 7.11. Let G be a finite group and assume that F is $\mathbb{R}$ or $\mathbb{C}$. If V is a finite-dimensional G-module and if U is a submodule of V, then there exists a G-module W such that $V = U \oplus W$.

Proof: By Weyl's unitary trick, there exists a G-invariant inner product $\langle\ ,\ \rangle$ on V. If we let $W = U^\perp$ be the orthogonal complement of U with respect to $\langle\ ,\ \rangle$, then W is G-invariant (by Lemma 7.7) and $V = U \oplus U^\perp$ (note: we need $\dim V < \infty$ here). ■

Exercise 7.12. Use Weyl's unitary trick to fix Example 7.6. That is, construct an invariant inner product on $\mathbb{R}^2$ and use it to find an invariant complement to U. ▶

[8] This is a common trick in the subject. Get used to it!

[9] Strictly speaking, the factor of $1/|G|$ isn't necessary here. However, it is necessary in other applications of the averaging trick, so it was included here to get you accustomed to seeing it.

7.3 Projections

Our second proof of the *assumption* in the proof of Maschke's theorem works for any field F whose characteristic doesn't divide $|G|$. The idea is fairly simple: If V is a G-module and if $U \subseteq V$ is a G-submodule, then as a subspace of V, U has many complements. We want to locate a G-invariant one. We start by asking: How do we find subspace complements?

Proposition 7.13. Let U be a subspace of a vector space V. Then there is a subspace W such that $V = U \oplus W$ if and only if there is a linear map $p\colon V \to V$ such that $\operatorname{im}(p) = U$, $\ker(p) = W$ and $p \circ p = p$.

Proof: If $V = U \oplus W$ then $v \in V$ can be written as $v = u + w$ where $u \in U$ and $w \in W$ are uniquely determined by v. We can define the desired $p\colon V \to V$ by $p(u + w) = u$.

Conversely, suppose we are given p as in the statement. Given $v \in V$, write $v = (v - p(v)) + p(v)$. Then $p(v - p(v)) = p(v) - p^2(v) = 0$, so $v - p(v) \in \ker(p)$. This shows that $V = \ker(p) + \operatorname{im}(p)$. To show that the sum is direct, suppose $v \in \ker(p) \cap \operatorname{im}(p)$. Then $v = p(v)$ since $v \in \operatorname{im}(p)$ but $p(v) = 0$ since $v \in \ker(p)$, so $v = p(v) = 0$. ■

Remark 7.14. A linear map $p\colon V \to V$ satisfying $p^2 = p$ is called a **projection** (onto $\operatorname{im}(p)$). Proposition 7.15 shows that there is a one-to-one correspondence between complements of U in V and projections onto U. Namely, the complements of U are the kernels of such projections.

This suggests that to find a G-invariant complement, we ought to find a G-linear projection p, i.e., one that satisfies

$$p(gv) = gp(v) \quad \text{for all } g \in G \text{ and } v \in V.$$

Indeed, the kernel of any G-linear map is G-invariant. How do we find a G-invariant projection? As you hopefully will have guessed: start with a projection and average it over G. Note that the condition for p to be G-linear may be re-written as

$$gp(g^{-1}v) = p(v) \quad \text{for all } g \in G \text{ and } v \in V.$$

In terms of the G-action on $\operatorname{Hom}(V, V)$, this is saying that $g \cdot p = p$ for all g. (Compare Exercise 5.15.) So we should be considering $\frac{1}{|G|}\sum_g g \cdot p$.

Proposition 7.15. Let U be a G-submodule of V, and let $p_0\colon V \to V$ be a projection onto U. Assuming that $\operatorname{char} F \nmid |G|$, define $p\colon V \to V$ by

$$p(v) = \frac{1}{|G|}\sum_{g \in G} gp_0(g^{-1}v).$$

(This is well-defined since $|G| \neq 0$ in F.) Then p is a G-linear projection onto U.

Proof: The fact that p is linear is immediate. The proof that p is G-linear is similar to how we proved Weyl's unitary trick, and is left for you as an instructive exercise.

To see that $p^2 = p$, we first observe that each $p_0(g^{-1}v)$ in U, since $\mathrm{im}(p_0) = U$, and therefore since U is G-invariant, $p(v) \in U$ too. Thus, $\mathrm{im}(p) \subseteq U$. Now,

$$\begin{aligned}
p^2(v) &= p\left(\frac{1}{|G|}\sum_{g\in G} gp_0(g^{-1}v)\right) \\
&= \frac{1}{|G|}\sum_{g\in G} gp(p_0(g^{-1}v)) && \text{(by } G\text{-linearity)} \\
&= \frac{1}{|G|}\sum_{g\in G} g\left(\frac{1}{|G|}\sum_{h\in h} hp_0(h^{-1}p_0(g^{-1}v))\right) \\
&= \frac{1}{|G|^2}\sum_{g,h\in G} ghp_0(h^{-1}p_0(g^{-1}v)).
\end{aligned}$$

Observe that $h^{-1}p_0(g^{-1}v)$ is in U, since U is G-invariant and $\mathrm{im}(p_0) = U$. Thus,

$$p_0(h^{-1}p_0(g^{-1}v)) = h^{-1}p_0(g^{-1}v)$$

and so we end up with

$$\begin{aligned}
p^2(v) &= \frac{1}{|G|^2}\sum_{g,h\in G} ghh^{-1}p_0(g^{-1}v) \\
&= \frac{1}{|G|^2}\sum_{g,h\in G} gp_0(g^{-1}v) \\
&= \frac{|G|}{|G|^2}\sum_{g\in G} gp_0(g^{-1}v) \\
&= p(v).
\end{aligned}$$

Thus, $p^2 = p$. Finally, it remains to show that $U \subseteq \mathrm{im}(p)$. So let $u \in U$. Then $g^{-1}u \in u$ and so $p_0(g^{-1}u) = g^{-1}u$. The definition of p now gives $p(u) = u$, completing the proof. ■

> **Remark 7.16.** Unlike in the proof of Weyl's unitary trick (Proposition 7.9), where the factor of $1/|G|$ in the averaged inner product was optional, the factor of $1/|G|$ in the averaged projection is necessary. It's needed to show that $p^2 = p$; without it, we would have $p^2 = |G|p$.

We can now prove the temporary *assumption* in the proof of Maschke's theorem. Note that this proof works even if $\dim V = \infty$ (though our proof of Maschke's theorem does not).

> **Proposition 7.17.** Let G be a finite group and assume that $\operatorname{char} F \nmid |G|$. If V is a G-module and U is a submodule of V, then there exists a G-module W such that $V = U \oplus W$.

Proof: Let W_0 be any subspace complement to U in V (obtained e.g. by extending a basis of U to V), and then let p_0 be the associated projection as per Proposition 7.13. Let p be the G-invariant projection provided by Proposition 7.15. Then $\ker(p)$ is a G-invariant complement to U by Proposition 7.13. ■

Lecture 7 Problems

7.1. Consider the representation $\rho\colon \mathbb{Z} \to GL_2(\mathbb{R})$ defined by

$$\rho(n) = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}.$$

Show that ρ is not completely reducible.

7.2. Let G be a finite group and assume that $\operatorname{char} F \mid |G|$. In this problem you will show that the regular representation $V = F\langle G\rangle$ is not completely reducible.

(a) Let $v_0 = \sum_{g\in G} g$ and set $U = \operatorname{span}_F\{v_0\}$. Show that U is a G-invariant subspace of V.

(b) Assume that V is completely reducible. Show that $V = U \oplus W$ for some G-submodule W of V.

(c) Derive a contradiction by considering the decomposition $e = cv_0 + w$ of the group identity $e \in V = U \oplus W$.

7.3. Let G be a finite subgroup of $GL_n(\mathbb{C})$. Show that G is conjugate to a subgroup of the unitary group $U_n(\mathbb{C})$.

7.4. Let V be an G-module and let U be a G-submodule of V. Show that a complement W of U in V is G-invariant if and only if the associated projection $p\colon V \to V$ is G-linear.

7.5. Let $\rho\colon G \to GL_3(\mathbb{C})$ be a representation of a finite group G. Prove that ρ is reducible if and only if there is a common eigenvector for all $\rho(g)$.

7.6. The regular representation V_{reg} of C_3 over $\mathbb{C}$ is completely reducible. Find irreducible representations $V_1, \dots, V_k$ such that $V_{\text{reg}} \cong \bigoplus_{i=1}^k V_i$. [Hint: As a first step, determine $\dim V_{\text{reg}}$.]

Lecture 8 Isotypic Decompositions and Schur's Lemma

In this lecture, G is a finite group and all representations are finite-dimensional.

To what extent do we have uniqueness in the decomposition of a representation into a direct sum of irreducible representations? Some care is needed here. For example, as a representation of the trivial group, $\mathbb{R}^2$ has infinitely many decompositions into a direct sum of irreducible subrepresentations (one-dimensional subspaces). However, each of these decompositions is the direct sum of two copies of the trivial representation. We will show that, in general, the isomorphism types of the irreducible representations that appear, and the number of times that they each appear, will be the same across all decompositions.

If $V = \bigoplus_{i=1}^n U_i$ is a decomposition of the finite-dimensional G-module V into a direct sum of irreducible representations, then by grouping together isomorphic U_i's, we can re-write this decomposition as

$$V \cong \bigoplus_{i=1}^{k} V_i^{\oplus m_i},$$

where the V_i are mutually non-isomorphic irreducible representations, and $V_i^{\oplus m_i}$ denotes the direct sum of m_i copies of V_i. The piece $V_i^{\oplus m_i}$ is referred to as the V_i-**isotypic component** (or the V_i-**isotype**) of V, and m_i is the **multiplicity** of V_i in V.

In order for this to be well-defined, we must prove that if we have another decomposition

$$V \cong \bigoplus_{j=1}^{l} W_j^{\oplus n_j},$$

where the W_j mutually non-isomorphic and irreducible, then we must have $k = l$ and (after re-indexing if necessary) $V_i \cong W_i$ and $m_i = n_i$ for all i. This will require some preparation. In a way, this situation reminiscent of the Fundamental Theorem of Arithmetic: Proving the existence of a factorization into primes ("Maschke's theorem"!) is easy, but proving uniqueness requires a bit of work, including something like Euclid's Lemma. Our stand-in for Euclid's Lemma is...

8.1 Schur's Lemma

The following is one of the most important results in representation theory (despite its almost trivial proof!). It will be the key to establishing uniqueness of isotypic decompositions.

> **Theorem 8.1** (Schur's Lemma)**.** Let V and W be irreducible FG-modules.
>
> (a) If $f \in \mathrm{Hom}_G(V, W)$ then f is either zero or else is an isomorphism.
>
> (b) If F is algebraically closed, then every $f \in \mathrm{Hom}_G(V, V)$ is of the form $f = \lambda\,\mathrm{id}$ for some $\lambda \in F$.

Proof: Let $f \in \mathrm{Hom}_G(V, W)$. Then since $\ker(f)$ is a submodule of V, it's either 0 or V. If it's V, we're done. If it's 0, then f is injective. Next, $\mathrm{im}(f)$ is a submodule of W, so it's either 0 or W. The former is impossible since f is injective and V is irreducible (hence non-zero). Thus, f is surjective hence is an isomorphism. This proves part (a).

For part (b), since F is algebraically closed, f has an eigenvalue $\lambda \in F$. So $f - \lambda\,\mathrm{id}$ has a non-zero kernel and hence cannot be an isomorphism. Thus, $f - \lambda\,\mathrm{id} = 0$ by part (a). ■

Remark 8.2 (The endomorphism ring)**.** Homomorphisms from an object to itself are called **endomorphisms**. The set $\mathrm{End}_G(V) := \mathrm{Hom}_G(V, V)$ of (G-linear) endomorphisms of the G-module V is a ring under composition. Schur's Lemma says that if V is irreducible, then every non-zero $f \in \mathrm{End}_G(V)$ is an isomorphism hence is invertible. Thus, $\mathrm{End}_G(V)$ is a (possibly noncommutative) *division ring*. If F is algebraically closed, then part (b) of Schur's Lemma tells us that $\mathrm{End}_G(V) \cong F$ is a field.

In what follows, we will assume that F is algebraically closed so that $\mathrm{End}_G(V) \cong F$ for all irreducible V. Technically speaking, this isn't *necessary* and everything can formulated more generally in terms of the division ring $\mathrm{End}_G(V)$. However, since this can be a bit distracting at this stage, I've decided to focus for now on the simpler case where F is algebraically closed. We will return to the general case later in the course.

Corollary 8.3. If F is algebraically closed and if V and W are irreducible FG-modules, then

$$\dim \mathrm{Hom}_G(V, W) = \begin{cases} 1 & \text{if } V \cong W, \\ 0 & \text{otherwise.} \end{cases}$$

Proof: Assume $V \cong W$. Given non-zero $f, h \in \mathrm{Hom}_G(V, W)$, part (a) of Schur's Lemma tells us that that f and h are isomorphisms and then part (b) tells us that $h^{-1} \circ f \in \mathrm{Hom}_G(V, V)$ is a scalar. That is, $f = \lambda h$ for some $\lambda \in F$. This shows that $\dim \mathrm{Hom}_G(V, W) = 1$. If $V \ncong W$ then part (a) of Schur's Lemma immediately implies that $\mathrm{Hom}_G(V, W) = 0$. ■

Here is a neat application of Schur's Lemma.

Proposition 8.4. Let G be a finite abelian group. If F is algebraically closed, then an FG-module V is irreducible if and only if $\dim V = 1$.

Proof: Let (V, ρ) be a representation of G. Since G is abelian, $\rho(g)$ is G-linear for all $g \in G$:

$$\rho(g)(hv) = \rho(g)(\rho(h)v) = \rho(gh)(v) = \rho(hg)(v) = \rho(h)(\rho(g)(v)) = h\rho(g)(v).$$

Thus, if V is irreducible, then each $\rho(g)$ must be a scalar by Schur's Lemma. Consequently, every subspace of V will be G-invariant. This is a contradiction unless $\dim V = 1$. The converse is obvious. ■

Exercise 8.5. Give another proof of Proposition 8.4 by using the fact that a commuting family of diagonalizable matrices is simultaneously diagonalizable. ▶

Remark 8.6. Proposition 8.4 is false if F is not algebraically closed. For instance, in Example 6.4 we saw a two-dimensional irreducible representation of C_4 over $\mathbb{R}$. (Actually, algebraic closure is excessive; all we need is for F to contain enough roots of unity to diagonalize each $\rho(g)$.)

Proposition 8.4 admits a partial converse: If $\operatorname{char} F \nmid |G|$, and if all irreducible FG-modules are one-dimensional, then G is abelian. We will prove this later, but try to see if you can prove it now. [Hint: The regular representation is faithful.] The hypothesis on $\operatorname{char} F$ is necessary since, for example, one can show that the only irreducible representations of S_3 over $\mathbb{F}_3$ are the trivial and alternating representations—both one-dimensional.

Example 8.7 ($\operatorname{Irr}_{\mathbb{C}}(C_n)$)**.** We have already determined all of the 1-dimensional representations of $C_n = \langle a \rangle$ over $\mathbb{C}$ (see Example 2.8). Proposition 8.4 tells us that these are *all* of the irreducible complex representations. Explicitly, if we fix an nth root of unity $\zeta \in \mathbb{C}$ (say $\zeta = \exp(2\pi i/n)$), then we have

$$\operatorname{Irr}_{\mathbb{C}}(C_n) = \{\chi_0, \chi_1, \ldots, \chi_{n-1}\},$$

where $\chi_i \colon C_n \to \mathbb{C}^\times$ is defined on the generator a by

$$\chi_i(a) = \zeta^i.$$

In particular, χ_0 is the trivial representation of C_n.

Lecture 8 Problems

8.1. Prove that if a finite group G has an irreducible faithful representation $\rho \colon G \to GL_n(\mathbb{C})$ then the center $Z(G)$ of G must be cyclic. [Hint: A finite subgroup of $\mathbb{C}^\times$ is cyclic.]

8.2. Refer to Example 8.7.

(a) Show that if $\chi_i, \chi_j \in \operatorname{Irr}_{\mathbb{C}}(C_n)$, then $\chi_i \otimes \chi_j \cong \chi_{i+j}$. [Here $i+j$ is to be understood as its least residue mod n. So, for example, if $\chi_2, \chi_3 \in \operatorname{Irr}_{\mathbb{C}}(C_5)$, then $\chi_2 \otimes \chi_3 \cong \chi_1$.]

(b) Deduce that $\otimes$ defines a group operation on $\operatorname{Irr}_{\mathbb{C}}(C_n)$.

(c) Show that $(\operatorname{Irr}_{\mathbb{C}}(C_n), \otimes)$ is isomorphic to C_n.

8.3. Describe $\operatorname{Irr}_{\mathbb{C}}(C_p \times C_q)$ where p and q are primes (and possibly $p = q$). Does $\otimes$ define a group operation on this set?

8.4. Let V be an FG-module. A bilinear form $B \colon V \times V \to F$ is said to be ***G*-invariant** if

$$B(gv, gw) = B(v, w) \text{ for all } g \in G \text{ and } v, w \in V.$$

Assume that V is irreducible and F is algebraically closed.

(a) Prove that if $B \colon V \times V \to F$ is a G-invariant bilinear form then there exists a scalar $c \in F$ such that $B(v, w) = cB(w, v)$ for all $v, w \in V$. [Hint: Use B to construct two maps $V \to V^*$.]

(b) Assume that there exists a non-zero G-invariant bilinear form $B\colon V \times V \to F$ and choose a scalar c as in part (a). Prove that if B' is another G-invariant bilinear form then $B'(v, w) = cB'(w, v)$ for all $v, w \in V$ and with the same scalar c. Thus, we may write c_V for the scalar c since it is independent of the choice of $B \neq 0$. Note that $c_V \neq 0$.

In the case where the only G-invariant bilinear form is the zero form, we set $c_V = 0$.

(c) Prove that $c_V \in \{0, \pm 1\}$ and $c_V = 0$ if and only if $V \not\cong V^*$ (as representations).

8.5. (a) Prove the following converse to Schur's Lemma (over $\mathbb{C}$): Let V be a $\mathbb{C}G$-module. If every $f \in \mathrm{Hom}_G(V, V)$ is of the form $f = \lambda\,\mathrm{id}$ for some $\lambda \in \mathbb{C}$ then V must be irreducible.

(b) What hypotheses must be placed on F for the result in part (a) to hold for FG-modules?

Lecture 9 Uniqueness of Isotypic Decompositions

In this lecture, G is a finite group and all representations are finite-dimensional.

Our goal now is to prove the uniqueness of the isotypic decomposition of a given FG-module V, as discussed at the beginning of last lecture. See Theorem 9.5 below for the precise statement. As a first step, we will explain how to calculate the number of copies of an arbitrary $U \in \mathrm{Irr}_F(G)$ that occur in the decomposition of a given V into irreducible representations. This number will be called the **multiplicity** of U in V.

We begin with a lemma.

Lemma 9.1. Let V, U_1 and U_2 be FG-modules. There are canonical isomorphisms:

(a) $\mathrm{Hom}_G(V, U_1 \oplus U_2) \cong \mathrm{Hom}_G(V, U_1) \oplus \mathrm{Hom}_G(V, U_2)$.

(b) $\mathrm{Hom}_G(U_1 \oplus U_2, V) \cong \mathrm{Hom}_G(U_1, V) \oplus \mathrm{Hom}_G(U_2, V)$.

Proof: This is just a matter of writing down the obvious maps and checking that they are G-linear isomorphisms. To this end, let $\pi_i \colon U_1 \oplus U_2 \to U_i$ be projection map onto the ith component. Note that π_i is G-linear. Next, define

$$\begin{aligned} \Phi\colon \mathrm{Hom}_G(V, U_1 \oplus U_2) &\to \mathrm{Hom}_G(V, U_1) \oplus \mathrm{Hom}_G(V, U_2) \\ f &\mapsto (\pi_1 \circ f, \pi_2 \circ f). \end{aligned}$$

Clearly, Φ is G-linear, and has a G-linear inverse given by $(f_1, f_2) \mapsto f_1 \oplus f_2$, where $f_1 \oplus f_2$ is defined by $(f_1 \oplus f_2)(v) = (f_1(v), f_2(v))$. This proves part (a).

For part (b), let $\iota_i \colon U_i \to U_1 \oplus U_2$ be the natural inclusions into the ith component. Define

$$\begin{aligned} \Psi\colon \mathrm{Hom}_G(U_1 \oplus U_2, V) &\to \mathrm{Hom}_G(U_1, V) \oplus \mathrm{Hom}_G(U_2, V) \\ f &\mapsto (f \circ \iota_1, f \circ \iota_2). \end{aligned}$$

This is a G-linear map with inverse given by $(f_1, f_2) \mapsto f_1\pi_1 + f_2\pi_2$. ■

By repeatedly applying the previous lemma, we deduce:

Corollary 9.2. Let $\{V_i\}_{i=1}^n$ and $\{W_j\}_{j=1}^m$ be families of FG-modules. There is a canonical isomorphism

$$\mathrm{Hom}_G\left(\bigoplus_{i=1}^n V_i, \bigoplus_{j=1}^m W_j\right) \cong \bigoplus_{i=1}^n \bigoplus_{j=1}^m \mathrm{Hom}_G(V_i, W_j).$$ ■

With this in hand, we can now easily show that the multiplicity of a given irreducible representation is the same across all decompositions into irreducibles.

Proposition 9.3. Assume F is algebraically closed. Suppose V is an FG-module that has a decomposition

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

into irreducible FG-modules U_i. Then, for any irreducible FG-module U,

$$\dim_F \operatorname{Hom}_G(U, V) = |\{i \colon U_i \cong U\}| \,.$$

Proof: By Corollary 9.2,

$$\operatorname{Hom}_G(U, V) \cong \bigoplus_{i=1}^{n} \operatorname{Hom}_G(U, U_i).$$

Now, by Corollary 8.3, each $\operatorname{Hom}_G(U, U_i)$ is either zero (if $U \ncong U_i$) or else is one-dimensional (if $U \cong U_i$). The result follows. ■

Remark 9.4. A similar proof also shows that $\dim \operatorname{Hom}_G(V, U) = |\{i \colon U_i \cong U\}|$.

Thus, the multiplicity of a given irreducible representation U in any isotypic decomposition of V is completely determined by U and V alone and is independent of the isotypic decomposition.

Theorem 9.5 (Uniqueness of Isotypic Decompositions)**.** Assume F is algebraically closed. Let V be an FG-module and suppose that $V = \oplus_{i=1}^{k} V_i^{\oplus m_i}$ and $V = \oplus_{j=1}^{l} W_j^{\oplus n_j}$ are decompositions of V into irreducible representations V_i and W_j, resp., such that the V_i are pairwise non-isomorphic and the W_j are pairwise non-isomorphic. Then:

(a) $k = l$.

(b) After re-indexing if necessary, $V_i \cong W_i$ and $m_i = n_i$ for all i.

Proof: By Proposition 9.3, the number of V_i that are isomorphic to a given irreducible representation U is equal to the number of W_j that are isomorphic to U. Applying this observation to $U = V_{i_0}$, we deduce that there must be exactly one W_j, say W_{i_0} (after re-indexing if necessary), that is isomorphic to V_{i_0} and furthermore $m_{i_0} = n_{i_0}$. So all of the V_i's appear among the W_j's with the same multiplicities. A similar argument applied to $U = W_{j_0}$ completes the proof. ■

Remark 9.6. Both the statement and proof of Theorem 9.5 go through without change if F is not algebraically closed. What needs to be modified is Proposition 9.3, which gives the multiplicity of an irreducible representation U in V as $\dim_F \operatorname{Hom}_G(U, V)$. When F is not algebraically closed, the formula for the multiplicity will involve the division ring $\operatorname{End}_G(U)$. It will still be independent of the particular decomposition of V into irreducibles.

9.1 Examples

For simplicity, let's work over $F = \mathbb{C}$. For this next result, it will be helpful to recall our determination of $\mathrm{Irr}_{\mathbb{C}}(C_n)$ in Example 8.7.

Proposition 9.7. Let a be a generator of C_n and let (V, ρ) be a $\mathbb{C}C_n$-module. The isotypic decomposition of V is given by

$$V = \bigoplus_{\lambda} V_\lambda,$$

where the sum is over the eigenvalues λ of $\rho(a)$ and V_λ is λ-eigenspace of $\rho(a)$.

Proof: By Proposition 8.4, all irreducible $\mathbb{C}C_n$-modules are 1-dimensional. Thus, each irreducible submodule U of V must be of the form $U = \mathrm{span}\{v\}$, where $v \in V$ is such that $\rho(a)v = \chi(a)v$ for some $\chi \in \mathrm{Irr}_{\mathbb{C}}(C_n)$. In particular, v is an eigenvector for $\rho(a)$ with eigenvalue $\lambda := \chi(a)$. If u is an eigenvector with eigenvalue $\mu \neq \lambda$, then the $\mathbb{C}C_n$-submodules $\mathrm{span}\{v\}$ and $\mathrm{span}\{u\}$ are not isomorphic since $\rho(a)$ acts on u via some other $\chi' \in \mathrm{Irr}_{\mathbb{C}}(C_n)$. Finally, if $\{v_1, \dots, v_k\}$ is a basis for V_λ, then we have $V_\lambda = \bigoplus_{i=1}^k \mathrm{span}\{v_i\} \cong \chi^{\oplus k}$, and it follows that V_λ is the χ-isotypic component of V. ■

Remark 9.8. Proposition 9.7 says that the problem of determining the isotypic decomposition of a $\mathbb{C}C_n$-module is equivalent to the problem of diagonalizing $\rho(a)$. In this context, we get both Maschke's theorem and the uniqueness of isotypic decompositions (Theorem 9.5) for free since we can prove directly that $\rho(a)$ is diagonalizable (it's annihilated by the polynomial $x^n - 1$ which has no repeated roots in $\mathbb{C}$).

Let's look at some concrete examples.

Example 9.9. Let (V, ρ) be an arbitrary $\mathbb{C}C_2$-module. Since $\rho(a)^2 = \mathrm{id}$, the possible eigenvalues of $\rho(a)$ are ± 1, and so we have

$$V = V_+ \oplus V_-$$

where $V_+ = \{v \in V : \rho(a)v = v\}$ and $V_- = \{v \in V : \rho(a)v = -v\}$ are the ± 1-eigenspaces of $\rho(a)$. Note that we may have $V_+ = 0$ or $V_- = 0$. (Consider, e.g., the trivial representation.)

In terms of $\mathrm{Irr}_{\mathbb{C}}(C_2) = \{\chi_0, \chi_1\}$, we see that V_+ and V_- are the χ_0- and χ_1-isotypes of V, respectively. Indeed, if we let $\mathbb{C}_+$ and $\mathbb{C}_-$ denote the representation spaces for χ_0 and χ_1, and if we choose bases $\{v_1, \dots, v_n\}$ and $\{u_1, \dots, u_m\}$ for V_+ and V_-, then we have

$$V_+ = \bigoplus_{i=1}^n \mathrm{span}(v_i) \cong \bigoplus_{i=1}^n \mathbb{C}_+ = (\mathbb{C}_+)^{\oplus n}.$$

Similarly, $V_- \cong (\mathbb{C}_-)^{\oplus m}$. Therefore,

$$V \cong (\mathbb{C}_+)^{\oplus n} \oplus (\mathbb{C}_-)^{\oplus m},$$

that is, V is isomorphic to $n = \dim V_+$ copies of the trivial representation χ_0 and $m = \dim V_-$ copies of the representation χ_1. Consequently, we see that the $\mathbb{C}C_2$-module V is determined up to isomorphism by the pair $(n, m) \in \mathbb{Z}^2_{\geq 0}$, which perhaps we should refer to as the *signature* of V (this is nonstandard terminology). In concrete terms, n and m are, respectively, the multiplicities of $+1$ and -1 as eigenvalues of a acting on V.

Exercise 9.10. Determine the signature (n, m) of each of: (i) the regular representation V_{reg} of C_2, and (ii) the representation $U = \mathbb{C}^3$ of C_2 given by $a(x, y, z) = (y, x, z)$. ▶

Example 9.11. Let's determine the isotypic decomposition of the regular representation $V_{\text{reg}} = \mathbb{C}\langle C_n \rangle$ of $C_n = \langle a \rangle$. In the standard basis for V_{reg}, the matrix of a is given by

$$A = \begin{bmatrix} 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \end{bmatrix}.$$

Now, either by direct calculation or by recognizing A as a companion matrix, we find that the characteristic polynomial of A is equal to $x^n - 1$. In particular, the eigenvalues of A are the n distinct nth roots of unity in $\mathbb{C}$. Since $\dim V_{\text{reg}} = |C_n| = n$, it follows that each eigenspace is one-dimensional. Since A acts on each of the n eigenspaces by multiplication by a different nth root of unity, we conclude that

$$V_{\text{reg}} \cong \chi_0 \oplus \chi_1 \oplus \cdots \oplus \chi_{n-1}.$$

Thus, each $\chi \in \operatorname{Irr}_{\mathbb{C}}(C_n)$ occurs in V_{reg} with multiplicity equal to 1.

Next lecture, we will generalize the previous example to all finite abelian groups. Let's close this lecture by considering a nonabelian example.

Example 9.12. In Example 6.9, we showed that $\operatorname{Irr}_{\mathbb{C}}(S_3) = \{V_{\text{triv}}, V_{\text{sgn}}, V_{\text{std}}\}$. So if V is a $\mathbb{C}S_3$-module, we have

$$V \cong V_{\text{triv}}^{\oplus n} \oplus V_{\text{sgn}}^{\oplus m} \oplus V_{\text{std}}^{\oplus p},$$

for some $(n, m, p) \in \mathbb{Z}^3_{\geq 0}$, and the question is: How do we determine (n, m, p)?

What we did in Example 6.9 actually answers this question. Namely, if

$$V = V_1 \oplus V_\omega \oplus V_{\omega^2}$$

is the decomposition of V into eigenspaces for the action of $a = (1\ 2\ 3)$, then $V_\omega \oplus V_{\omega^2}$ further decomposes into a direct sum of $\dim V_\omega$ copies of V_{std}. So this gives us $p = \dim V_\omega$, i.e., p is the multiplicity of ω as an eigenvalue of a.

Furthermore, we saw that V_1 decomposes under the action of $b = (1\ 2)$ into a direct sum $V_1 = U_+ \oplus U_-$ of eigenspaces for the eigenvalues ± 1. (This is an instance of Example 9.9!) Thus, $n = \dim U_+$ (resp. $m = \dim U_-$) is the multiplicity of $+1$ (resp. -1) as an eigenvalue for b viewed as an operator on V_1 (not on V).

Let's illustrate. Take $V = \mathbb{C}^3$ to be the defining representation of S_3, where the action of $\pi \in S_3$ on $(a_1, a_2, a_3) \in \mathbb{C}^3$ is given by $\pi(a_1, a_2, a_3) = (a_{\pi^{-1}(1)}, a_{\pi^{-1}(2)}, a_{\pi^{-1}(3)})$. In the standard basis, the matrix of $a = (1\ 2\ 3)$ is given by

$$A = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

A calculation shows that ω occurs as an eigenvalue of A with multiplicity 1. (Alternatively, A is the companion matrix of $x^3 - 1$, so its eigenvalues are $1, \omega, \omega^2$.) Further, the eigenspace V_1 is equal to $\mathrm{span}\{(1, 1, 1)\}$, on which b acts trivially. Thus, $n = 1$ and $m = 0$, and consequently

$$V \cong V_{\text{triv}} \oplus V_{\text{std}}.$$

Of course, we already knew this! See Example 6.7.

While this kind of "eigen-analysis" is fun (at least I think so), it doesn't generalize to arbitrary groups. The trouble is that, in general, different group elements need not interact well with each other's eigenspaces in a representation. In S_3, the relationship $ba = a^2 b$ gave order to the action of b on the a-eigenspaces. We won't always be as lucky. So we will need to find better techniques.

Lecture 9 Problems

9.1. Determine the isotypic decompositions of the $\mathbb{C}S_3$-modules V_{reg}, $(V_{\text{std}})^*$ and $V_{\text{std}} \otimes V_{\text{std}}$.

9.2. Let $V = \mathbb{C}^2$ be the representation of $C_4 = \langle a \rangle$ in which a acts as a 90-degree counter-clockwise rotation. Determine the isotypic decomposition of $W = \mathrm{Hom}(V, V)$.

9.3. Assume $n \geq 3$. In this problem you will determine the isotypic decomposition of the defining representation $V = \mathbb{C}^n$ of S_n. (Compare Example 9.12.) Let

$$U = \mathrm{span}\{(1, 1, \ldots, 1)\} \quad \text{and} \quad W = \{(x_1, \ldots, x_n) \in \mathbb{C}^n \colon x_1 + \cdots + x_n = 0\}.$$

(a) Show that U and W are S_n-invariant and that $V = U \oplus W$.

(b) Let $e_1, \ldots, e_n$ denote the standard basis vectors of $\mathbb{C}^n$. Let w be a nonzero vector in W. Show that $e_1 - e_i \in \mathrm{span}\{\pi w \colon \pi \in S_n\}$ for all $i = 2, \ldots, n$. Deduce that W has no proper nonzero S_n-invariant subspaces.

[Thus, $V = U \oplus W$ is a direct sum of V into irreducible representations. We have $U \cong$ triv and we call W the **standard representation** of S_n.]

Lecture 10 Fourier Analysis on Abelian Groups

10.1 Taking stock

Let F be an algebraically closed field of characteristic zero and let G be a finite group. Then, by Maschke's theorem, every finite-dimensional FG-module V is completely reducible. Furthermore, by Theorem 9.5, each such V admits a *unique* (up to isomorphism) decomposition of the form

$$V \cong \bigoplus_{i=1}^{n} U_i^{\oplus m_i}$$

where the U_i are pairwise non-isomorphic irreducible FG-modules. The multiplicities m_i are given by the formula

$$m_i = \dim_F \operatorname{Hom}_G(U_i, V).$$

This prompts several natural questions. For instance:

1. How do we find all of the irreducible FG-modules for a given group G?
2. How many irreducible FG-modules are there? Finitely many? Infinitely many?
3. Is there an easy way to determine if two given irreducible FG-modules are isomorphic?

We will now try to answer these questions. We begin with the case where G is a finite abelian group, since in this case we at least have some useful information: according to Proposition 8.4, all the irreducible modules are one-dimensional. In what follows, we work over $\mathbb{C}$ (for historical reasons), but all of the key results hold over an arbitrary algebraically closed field of characteristic zero.

10.2 Classical Fourier analysis

One of the earliest occurrences of a "representation" goes back to Dirichlet's proof of his famous theorem on primes in arithmetic progressions. A key ingredient of this proof, as we understand it now, was the use of Fourier analysis on the finite ableian group $(\mathbb{Z}/n\mathbb{Z})^\times$ of units modulo n. In general, we have the following slogan:

For a finite abelian group, representation theory $\equiv$ Fourier analysis.

We're going to learn about one aspect of this relationship in this lecture.

Let's begin with classical Fourier analysis on $\mathbb{R}$ (or, more accurately, on $\mathbb{R}/2\pi\mathbb{Z}$). The primary objects of interest are **Fourier series**, which are series of the form

$$f(x) = \sum_{n\geq 0} a_n \cos(nx) + \sum_{n\geq 1} b_n \sin(nx).$$

Such a series is 2π-periodic, and so defines a function on $\mathbb{R}/2\pi\mathbb{Z}$.[10] Using the fact that

[10] In this lecture, I will be ignoring issues of convergence, integrability, etc.

$e^{inx} = \cos(nx) + i\sin(nx)$, we can re-write $f(x)$ in the form

$$f(x) = \sum_{n\in\mathbb{Z}} c_n e^{inx}.$$

This form is more convenient for us because the function $e_n(x) := e^{inx}$ defines a one-dimensional representation $e_n\colon \mathbb{R} \to GL_1(\mathbb{C}) = \mathbb{C}^\times$ of the additive group $\mathbb{R}$.

Definition 10.1. A **unitary character** of an abelian group G is a one-dimensional complex representation $\chi\colon G \to \mathbb{C}^\times$ such that $|\chi(g)| = 1$ for all $g \in G$. (Thus, the image of χ lies in the 1×1 unitary group $U_1(\mathbb{C}) = \{z \in \mathbb{C}\colon |z| = 1\}$.) The set of all unitary characters of G will be denoted by $\widehat{G}$.

Example 10.2. The functions e_n defined above are unitary characters of $\mathbb{R}$. In fact, since they are 2π-periodic, they are unitary characters of $\mathbb{R}/2\pi\mathbb{Z}$.

Example 10.3. If G is a *finite* abelian group, then

$$\widehat{G} = \mathrm{Irr}_{\mathbb{C}}(G).$$

Proof: The containment $\subseteq$ is clear. Conversely, since every irreducible complex representation of G is one-dimensional (Proposition 8.4), it suffices to show that each $\chi \in \mathrm{Irr}_{\mathbb{C}}(G)$ is unitary, i.e. has image in $U_1(\mathbb{C})$. This follows from Weyl's unitary trick (how?) but we can give a direct argument: $g^{|G|} = 1 \implies \chi(g)^{|G|} = 1$, so $\chi(g)$ is a root of unity in $\mathbb{C}$ hence $|\chi(g)| = 1$. ∎

Now, given a Fourier series

$$f(x) = \sum_{n\in\mathbb{Z}} c_n e^{inx}, \tag{5}$$

its **Fourier coefficients** c_n are given by

$$c_n = \frac{1}{2\pi}\int_0^{2\pi} f(x)e^{-inx}\,dx.$$

What is going on here is that the functions $e_n(x) = e^{inx}$ are orthonormal with respect to the inner product

$$\langle f, g\rangle = \frac{1}{2\pi}\int_0^{2\pi} f(x)\overline{g(x)}\,dx. \tag{6}$$

In fact, the set $\{e_n\}_{n\in\mathbb{Z}}$ an orthonormal basis for the Hilbert space $L^2(\mathbb{R}/2\pi\mathbb{Z})$. So, for f in $L^2(\mathbb{R}/2\pi\mathbb{Z})$, equation (5) can be viewed as the expansion

$$f = \sum_{n\in\mathbb{Z}} c_n e_n \tag{7}$$

of f in this basis. Therefore, the coefficients in this expansion are given by $c_n = \langle f, e_n \rangle$. What is also true, but won't be proved here, is that the e_n constitute the set of *all* (continuous) unitary characters of $\mathbb{R}/2\pi\mathbb{Z}$. So we can re-write (7) more suggestively as:

$$f = \sum_{\chi \in \widehat{G}} \langle f, \chi \rangle \, \chi. \tag{8}$$

In other words, the Fourier expansion of a function is really a representation theoretic construction.

10.3 Characters of finite abelian groups

We are now going to establish a version of (8) for G a finite abelian group in place of the group $\mathbb{R}/2\pi\mathbb{Z}$. This is not a drastic shift: the latter is a *compact* abelian group, and among the infinite groups the compact ones are the ones most similar to finite groups.

To start, let $\ell^2(G) = \{f \colon G \to \mathbb{C}\}$ be the vector space of complex functions on G, and equip it with the inner product

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

Aside: This inner product can be seen to be formally identical to (6) if G is equipped with the discrete measure. The factor $|G|$ is the total measure of G—just like 2π is the total measure of $\mathbb{R}/2\pi\mathbb{Z}$ with respect to Lebesgue measure ($\mathbb{R}/2\pi\mathbb{Z} \cong$ the interval $[0, 2\pi]$ with the end points identified).

The vector space $\ell^2(G)$ has a basis given by the functions δ_g ($g \in G$) defined by

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

Thus, $\dim \ell^2(G) = |G|$.

Exercise 10.4. Show that $\{\delta_g\}_{g \in G}$ is an orthogonal basis for $\ell^2(G)$. ▶

There is another orthogonal (in fact, orthonormal) basis that is more suited to our investigations.

Theorem 10.5. Let G be a finite abelian group.

(a) (Orthogonality of Characters) The set $\widehat{G}$ of unitary characters is orthonormal.

(b) (Completeness of Characters) The set $\widehat{G}$ of unitary characters is a basis for $\ell^2(G)$.

This result plays an important role in the proof of Dirichlet's theorem on primes in arithmetic progressions. It is the finite group version of the fact that the characters $\{e_n\}_{n \in \mathbb{Z}}$ form a Hilbert space basis for $L^2(\mathbb{R}/2\pi\mathbb{Z})$.

Granting Theorem 10.5 for now, we can expand each $f \in \ell^2(G)$ as a "Fourier series"

$$f(x) = \sum_{\chi \in \widehat{G}} c_\chi \, \chi(x),$$

where the "Fourier coefficients" c_χ are given by

$$c_\chi = \langle f, \chi \rangle = \frac{1}{|G|} \sum_{x \in G} f(x)\overline{\chi(x)}.$$

This is completely analogous to the Fourier series expansion (8) of $f \in L^2(\mathbb{R}/2\pi\mathbb{Z})$.

We now turn our attention to the proof of Theorem 10.5. It will be helpful to know that $|\widehat{G}| = \dim \ell^2(G) = |G|$, so we prove this now.

Proposition 10.6. Let G be a finite abelian group. Then G has $|G|$ distinct irreducible complex representations. That is, $|\widehat{G}| = |G|$.

Proof: First note that $\widehat{G} = \mathrm{Irr}_{\mathbb{C}}(G)$. If $G = C_n$ is cyclic, we saw in Example 2.8 that $|\widehat{G}| = n = |G|$, as desired. In general, we appeal to the fact that every finite abelian group is a product of cyclic groups. Write

$$G = \langle a_1 \rangle \times \langle a_2 \rangle \times \cdots \langle a_k \rangle,$$

where $a_i \in G$ has order n_i, say. Any unitary character χ of G is completely determined by the values $\chi(a_i)$. These values must be n_ith roots of unity, and we can prescribe them as we wish. Thus, every unitary character χ of G is of the form

$$\chi(a_1^{r_1} \cdots a_k^{r_k}) = \omega_1^{r_1} \cdots \omega_k^{r_k}$$

where ω_i is an n_ith root of unity in $\mathbb{C}$. So χ is determined by the k-tuple $(\omega_1, \ldots, \omega_k)$. Distinct k-tuples give rise to distinct characters (why?). The result follows. ■

Remark 10.7. The proof of Proposition 10.6 needs the underlying field to be algebraically closed *and* to contain n distinct nth roots of unity for every n that is the order of a cyclic factor of G. (The latter condition holds, e.g., if $\mathrm{char}\, F \nmid |G|$.) Without these hypotheses, the corollary is false. For example, a finite p-group only has one irreducible representation (the trivial one) over any field of characteristic p (Problem 10.1).

Example 10.8. The proof of Proposition 10.6 shows that the unitary characters of the Klein four-group $C_2 \times C_2 = \langle a, b \colon a^2 = b^2 = 1, ab = ba \rangle$ are in bijection with ordered pairs (ω_1, ω_2) where $\omega_i \in \{\pm 1\}$. Explicitly, the unitary characters of $C_2 \times C_2$ are given by:

$$\begin{aligned}
\chi_{1,1} &: a \mapsto 1,\ b \mapsto 1 \\
\chi_{1,-1} &: a \mapsto 1,\ b \mapsto -1 \\
\chi_{-1,1} &: a \mapsto -1,\ b \mapsto 1 \\
\chi_{-1,-1} &: a \mapsto -1,\ b \mapsto -1.
\end{aligned}$$

> *Aside:* If you stare at these, you'll see that the set of unitary characters looks a lot like the group $C_2 \times C_2$ itself. In fact, we can set up an isomorphism by declaring $a \leftrightarrow \chi_{1,-1}$ and $b \leftrightarrow \chi_{-1,1}$ (say). It is a general fact that $\widehat{G}$ is in a natural way a group (use pointwise multiplication) and that with this group structure we have a (non-canonical) isomorphism $G \cong \widehat{G}$. (Compare Problem 8.2.) We won't pursue this thread of ideas further in this course. However, if you're curious, look at Problem 10.3.

We are now ready for the proof of our main result.

Proof of Theorem 10.5: We must prove two things:

(i) If $\chi \in \widehat{G}$, then $\langle \chi, \chi \rangle = 1$.

(ii) If $\chi, \psi \in \widehat{G}$ are distinct, then $\langle \chi, \psi \rangle = 0$.

This will show that $\widehat{G}$ is an orthonormal set. Then Proposition 10.6 implies that it is an orthonormal basis for the $|G|$-dimensional space $\ell^2(G)$.

Part (i) is an easy computation:

$$\langle \chi, \chi \rangle = \frac{1}{|G|} \sum_g \chi(g)\overline{\chi(g)} = \frac{1}{|G|} \sum_g |\chi(g)|^2 = \frac{1}{|G|} \sum_g 1 = \frac{1}{|G|}|G| = 1.$$

For part (ii), suppose first that $\psi = \chi_0$ is the trivial character defined by $\chi_0(g) = 1$ for all $g \in G$. Then

$$\langle \chi, \chi_0 \rangle = \frac{1}{|G|} \sum_g \chi(g)\overline{\chi_0(g)} = \frac{1}{|G|} \sum_g \chi(g).$$

If $\chi \neq \chi_0$, there exists an $h \in G$ such that $\chi(h) \neq 1$. Since $g \leftrightarrow gh$ is a bijection on G, summing over $g \in G$ is the same as summing over $gh \in G$. Thus,

$$\begin{aligned}
\langle \chi, \chi_0 \rangle &= \frac{1}{|G|} \sum_g \chi(gh) \\
&= \frac{1}{|G|} \sum_g \chi(g)\chi(h) \\
&= \chi(h)\frac{1}{|G|} \sum_g \chi(g) \\
&= \chi(h) \langle \chi, \chi_0 \rangle .
\end{aligned}$$

Since $\chi(h) \neq 1$, it follows that $\langle \chi, \chi_0 \rangle = 0$. The general case follows from this together with the fact that

$$\langle \chi, \psi \rangle = \langle \chi\overline{\psi}, \chi_0 \rangle = 0.$$

For the last equality to hold, we need to be sure that $\chi\overline{\psi}$ is a character and that it is non-trivial if $\chi \neq \psi$; I will leave this for you to check. ■

Exercise 10.9. Let G be a finite group, and let $\chi, \psi \in \widehat{G}$. Prove:

(a) $\overline{\chi(g)} = \chi(g)^{-1}$.

(b) $\chi\psi \in \widehat{G}$, where $\chi\psi$ is defined by $\chi\psi(g) = \chi(g)\psi(g)$.

(c) $\overline{\psi} \in \widehat{G}$, where $\overline{\psi}$ is defined by $\overline{\psi}(g) = \overline{\psi(g)}$.

Also show that if $\chi \neq \psi$ then $\chi\overline{\psi}$ is not the trivial character. ►

10.4 Summary

Let G be a finite abelian group. Then:

- The irreducible complex representations of G are one-dimensional, hence are unitary characters.
- The set $\widehat{G}$ of unitary characters is an orthonormal basis for $\ell^2(G) = \{f : G \to \mathbb{C}\}$.
- Thus, every $f \in \ell^2(G)$ can be expanded as $f = \sum_{\chi \in \widehat{G}} \langle f, \chi \rangle \chi$.
- Equivalently, if $\widehat{G} = \{\chi_1, \ldots, \chi_n\}$, then there is an orthogonal direct sum decomposition

$$\ell^2(G) = \operatorname{span}\{\chi_1\} \oplus \cdots \oplus \operatorname{span}\{\chi_n\}. \tag{9}$$

The space $\ell^2(G) = \mathcal{F}(G, \mathbb{C})$ is of course none other than the representation space of the regular representation of G. Viewed as such, the decomposition in (9) gives the isotypic decomposition of the regular representation. We will explore this in more detail next time.

Lecture 10 Problems

10.1. Let G be a finite p-group, i.e. a group all of whose elements have order a power of p. Let F be a field of characteristic p. Prove that $\operatorname{Irr}_F(G)$ consists of only the trivial representation, as follows. (This argument is from Serre's book.)

   (a) Let V be an irreducible representation and choose $v \neq 0$ in V. We have a copy of $\mathbb{F}_p$, the finite field of size p, in F. Let U be the $\mathbb{F}_p$-span of $\{gv : g \in G\}$. Show that $|U| = p^n$ for some $n \in \mathbb{Z}_{>0}$.

   (b) Show that G acts on U with orbits of size 1 or some positive power of p.

   (c) Deduce that $|U^G| \equiv |U| \pmod p$ and conclude that U^G is a nonzero G-invariant subspace of V.

10.2. Show that the result that $\widehat{G} = \operatorname{Irr}_{\mathbb{C}}(G)$ can fail spectacularly if G is nonabelian: Find an example of a nonabelian group G such that $\widehat{G}$ consists only of the trivial representation but $|\operatorname{Irr}_{\mathbb{C}}(G)| > 1$. [Hint: Problem 2.1.]

10.3. In the problems below, you will prove some of the basic results of harmonic analysis in the finite abelian setting. There are more general (infinite and nonabelian) versions, but the proofs are much more involved.

Let G be a finite abelian group.

(a) Show that the pointwise product of functions turns $\widehat{G}$ into an abelian group. [We call $\widehat{G}$ the **dual group** of G.]

(b) Prove that $\widehat{G} \cong G$. [Hint: Show first that $\widehat{C_n} \cong C_n$. Then show that $\widehat{G \times H} \cong \widehat{G} \times \widehat{H}$.]

(c) The isomorphism in part (b) is non-canonical (it requires choices of generators). Prove, however, that there is a canonical isomorphism $G \cong \widehat{\widehat{G}}$. [This is referred to as **Pontryagin duality**.]

(d) For a subgroup $H \leq G$, define

$$H^{\perp} = \{\chi \in \widehat{G} \colon \chi(h) = 0 \text{ for all } h \in H\}.$$

(i) Show that $H^{\perp}$ is a subgroup of $\widehat{G}$.

(ii) Determine $G^{\perp}$ and $\{1\}^{\perp}$.

(iii) Prove that $H^{\perp} \cong \widehat{G/H}$ and $\widehat{G}/H^{\perp} \cong \widehat{H}$.

(e) Prove the **Poisson summation formula**: For $f \in \ell^2(G)$ and $H \leq G$, we have

$$\frac{1}{|H|} \sum_{h \in H} f(h) = \frac{1}{|G|} \sum_{\chi \in H^{\perp}} \widehat{f}(\chi),$$

where $\widehat{f}(\chi) = |G| \langle f, \chi \rangle$. [Hint: Prove this for $f = \delta_g$ and then use linearity.]

The function $\widehat{f} \in \ell^2(\widehat{G})$ defined in this manner is called the **Fourier transform** of f. Explicitly, $\widehat{f}$ is given by

$$\widehat{f}(\chi) = \sum_{g \in G} f(\chi)\overline{\chi(g)}, \quad \text{for } \chi \in \widehat{G}.$$

This is an analogue of the Fourier transform of a function f on $G = \mathbb{R}$, which is given by

$$\widehat{f}(y) = \int_{\mathbb{R}} f(x) e^{-2\pi i x y}\, dx.$$

Our Fourier series expansion can be written as $f = \frac{1}{|G|} \sum_{\chi} \widehat{f}(\chi)\chi$; in this form, it's referred to as the **Fourier inversion formula** because it reconstructs f from its Fourier transform $\widehat{f}$.

Lecture 11 The Regular Representation

In this lecture, G is a finite group.

11.1 The Fourier decomposition of $\ell^2(G)$

If G is abelian, we saw last time that the vector space $\ell^2(G) = \{f : G \to \mathbb{C}\}$ of complex functions on G decomposes into a direct sum of one-dimensional subspaces, each spanned by a unitary character of G:

$$\ell^2(G) = \bigoplus_{\chi \in \widehat{G}} \operatorname{span}\{\chi\}. \tag{10}$$

If we view $\ell^2(G)$ as the representation space for the regular representation, with G-action

$$(gf)(x) = f(g^{-1}x), \quad \text{where } f \in \ell^2(G) \text{ and } g, x \in G,$$

then the decomposition (10) turns out to be the isotypic decomposition of $\ell^2(G)$.

> **Lemma 11.1.** Let G be a finite abelian group, and let $\chi \in \widehat{G}$ be a unitary character. The subspace $\operatorname{span}\{\chi\}$ of $\ell^2(G)$ is G-invariant. Moreover, as a $\mathbb{C}G$-module, $\operatorname{span}\{\chi\}$ is isomorphic to $\mathbb{C}_{\overline{\chi}}$, the representation space of the unitary character $\overline{\chi}$.

Proof: Simply observe that $(g\chi)(x) = \chi(g^{-1}x) = \chi(g^{-1})\chi(x)$. Since $\chi(g^{-1})$ is a scalar, we see that $g\chi$ is a scalar multiple of χ for each $g \in G$. This proves the first claim. Next, since $|\chi(g)| = 1$, we have $\chi(g^{-1}) = \chi(g)^{-1} = \overline{\chi(g)}$. This shows that each $g \in G$ acts on the one-dimensional space $\operatorname{span}\{\chi\}$ via multiplication by $\overline{\chi(g)}$, proving the second claim. ■

> **Remark 11.2.** In the *right* regular representation, we would have $\operatorname{span}\{\chi\} \cong \mathbb{C}_\chi$ instead of $\mathbb{C}_{\overline{\chi}}$.

As χ runs over $\widehat{G}$, so does $\overline{\chi}$. Thus, recalling that $\widehat{G} = \operatorname{Irr}_{\mathbb{C}}(G)$ (Example 10.3), we arrive at:

> **Theorem 11.3.** Let G be a finite abelian group. The isotypic decomposition of the regular representation $\mathbb{C}\langle G\rangle$ of G is given by
>
> $$\mathbb{C}\langle G\rangle \cong \bigoplus_{V \in \operatorname{Irr}_{\mathbb{C}}(G)} V.$$
>
> In particular, every irreducible representation of G occurs exactly once in $\mathbb{C}\langle G\rangle$. ■

Among other things, this theorem tells us where to find the irreducible complex representations of an abelian group: they all occur in the regular representation. Taking our cue from this, we now turn to an investigation of the regular representation $F\langle G\rangle$ of an arbitrary finite group G over an arbitrary field F such that $\operatorname{char} F \nmid |G|$. (This condition on $\operatorname{char} F$ is necessary since otherwise the regular representation is not completely reducible.) Amazingly, Theorem 11.3 generalizes beautifully to this setting. Below we will see how this plays out if F is algebraically closed. We will be able to drop this assumption on F later in the course.

11.2 The isotypic decomposition of $F\langle G\rangle$

As a first step towards decomposing the regular representation $F\langle G\rangle$, we prove:

Lemma 11.4. Let U be an irreducible FG-module. The map

$$T\colon \operatorname{Hom}_G(F\langle G\rangle, U) \to U$$
$$f \mapsto f(1)$$

is an isomorphism of F-vector spaces.

Proof: A linear map $f\colon F\langle G\rangle \to U$ is completely determined by what it does to the basis G of $F\langle G\rangle$, and the values $f(g)$, for $g \in G$, may be assigned arbitrarily. If f is G-linear, then $f(g) = f(g \cdot e) = gf(e)$ shows that f is completely determined by what it does to the identity element $e \in G$. The value $f(e) \in U$ can be assigned completely arbitrarily. This shows that the map T is a bijection. I'll leave it to you to check that T is linear. ■

Theorem 11.5. Assume F is algebraically closed and $\operatorname{char} F \nmid |G|$. Then every irreducible FG-module U occurs as a submodule of the regular representation $F\langle G\rangle$. Furthermore, the multiplicity of U in $F\langle G\rangle$ is equal to $\dim U$.

Proof: Let U be an irreducible FG-module. Then, since FG is completely reducible, the multiplicity of U in $F\langle G\rangle$ is given by $\dim_F \operatorname{Hom}(F\langle G\rangle, U)$. (See Proposition 9.3 and Remark 9.4.) By the previous lemma, $\dim_F \operatorname{Hom}_G(FG, U) = \dim_F U$. This proves the proposition. ■

Remark 11.6. The first half of Theorem 11.5 is true even if F is not algebraically closed (Problem 11.1). However, in this case the multiplicity of U need not be equal to $\dim U$. We will revisit this later.

Let's deduce some important consequences of Theorem 11.5.

Corollary 11.7. Assume F is algebraically closed and $\operatorname{char} F \nmid |G|$. Then there are only finitely many irreducible FG-modules (up to isomorphism).

If $\operatorname{Irr}_F(G) = \{V_1, \ldots, V_r\}$ is a full set of representatives of the distinct isomorphism classes of irreducible FG-modules, then:

(a) $F\langle G\rangle \cong \bigoplus_{i=1}^r V_i^{\oplus \dim V_i}$. (Isotypic Decomposition of $F\langle G\rangle$)

(b) $|G| = (\dim V_1)^2 + \cdots + (\dim V_r)^2$. (Dimension Formula)

(c) $r \leq |G|$.

Proof: Since $\dim F\langle G\rangle = |G|$ is finite, and since each irreducible representation appears as a submodule (hence direct summand) of $F\langle G\rangle$, there can only be finitely many such. Part (a) is just a restatement of Theorem 11.5 together with Maschke's theorem. Part (b) follows from (a) by calculating the dimension of both sides. Finally, part (c) follows from (b) plus the fact that $\dim V_i \geq 1$. ■

Note that if $F = \mathbb{C}$ and G is abelian, Theorem 11.5 reduces to Theorem 11.3 and the decomposition of $\mathbb{C}\langle G\rangle$ in Corollary 11.7(a) is the same as the one in Theorem 11.3. So we've obtained our desired generalization!

There remains one lingering question:

What is the number r of irreducible FG-modules?

The bound $r \leq |G|$ in Corollary 7.4(c) is attained if G is abelian (Proposition 10.6 proves this for $F = \mathbb{C}$ and the proof given there works for any algebraically closed field F such that $\operatorname{char} F \nmid |G|$). In general, we will see later that (under the same assumptions on F)

$$r = \text{ the number of conjugacy classes in } G.$$

When G is abelian, every conjugacy class is a singleton, so we see again that $r = |G|$. In fact, $r = |G|$ if and only if G is abelian; this follows from:

Proposition 11.8. Let G be a finite group. Let $[G, G]$ be the commutator subgroup of G and let $\pi\colon G \to G/[G, G]$ be the quotient map. Then the map

$$\begin{aligned} \operatorname{Hom}(G/[G, G], F^\times) &\to \operatorname{Hom}(G, F^\times) \\ \rho &\mapsto \rho \circ \pi \end{aligned}$$

is a bijection of sets.

In particular, the number of isomorphism classes of one-dimensional representations of G is equal to the number of isomorphism classes of one-dimensional representations of $G/[G, G]$.

Proof: (This is Problem 2.2.) We construct the inverse map. Given $\varphi \in \operatorname{Hom}(G, F^\times)$, observe that since the codomain $F^\times$ is abelian, $[G, G] \subseteq \ker \varphi$. Thus, we can define a homomorphism $\widetilde{\varphi}\colon G/[G, G] \to F^\times$ by $\widetilde{\varphi}(g[G, G]) = \varphi(g)$. The well-definedness of $\widetilde{\varphi}$ follows from the fact that $[G, G] \subseteq \ker \varphi$. By construction, $\varphi \circ \pi = \widetilde{\varphi}$, and so $\varphi \mapsto \widetilde{\varphi}$ is our desired inverse map. ■

Exercise 11.9. Assume F is algebraically closed[11] and $\operatorname{char} F \nmid |G|$. Prove that G is abelian if and only if all of the irreducible FG-modules are one-dimensional.

[Hint: Use Corollary 11.7 and Proposition 11.8 to count the number of distinct one-dimensional representations. (Ethan Shai Oyberman)] ►

[11] As previously noted in Remark 8.6, the forward direction fails if F is not algebraically closed. The backwards direction, however, is true without this assumption. See Problem 11.2.

Let's look at a couple of examples of these results action.

Example 11.10 ($\mathrm{Irr}_{\mathbb{C}}(S_3)$)**.** Consider $G = S_3$ and let $d_1, \ldots, d_r$ be the degrees of the irreducible representations of S_3 over $\mathbb{C}$ (say). Then Corollary 7.4(b) gives

$$6 = d_1^2 + \cdots + d_r^2.$$

The only solutions to this equation are $6 = 1^2 + \cdots + 1^2$ and $6 = 1^2 + 1^2 + 2^2$. The first of these can be discarded since S_3 is nonabelian. More precisely, since $S_3/[S_3, S_3] = S_3/A_3 \cong C_2$, Proposition 11.8 implies that S_3 only has two one-dimensional representations. We conclude that there are three irreducible representations of degrees 1, 1 and 2. This is inline with (but completely independent of) our earlier determination of $\mathrm{Irr}_{\mathbb{C}}(S_3)$ in Example 6.9. The problem here, of course, is that this gives us the number and degrees of the irreducible representations but not how to construct them. (That said, Proposition 11.8 tells us how to define the one-dimensional representations: lift them from $S_3/[S_3, S_3] \cong C_2$.)

Observe further that S_3 has three conjugacy classes (corresponding to the cycle types (1)(2)(3), (1)(2 3), and (1 2 3); or, equivalently, to the three partitions $3 = 1 + 1 + 1 = 1 + 2 = 3$ of 3). This is in accordance with our claim above that the number of irreducible representations is equal to the number of conjugacy classes.

Example 11.11 ($\mathrm{Irr}_{\mathbb{C}}(D_8)$)**.** Consider the dihedral group

$$D_8 = \langle a, b \colon a^4 = b^2 = e, bab = a^{-1} \rangle$$

consisting of the symmetries of the square. I will let you check that:

- D_8 has order 8 and contains five conjugacy classes.
- The derived subgroup of D_8 is $[D_8, D_8] = \langle a^2 \rangle$.
- The quotient $D_8/[D_8, D_8]$ is isomorphic to the Klein four-group $C_2 \times C_2$.

Thus, D_8 has $r = 5$ irreducible representations; let their degrees be $d_1, \ldots, d_5$. Since $D_8/[D_8, D_8]$ has order 4, it follows that D_8 has four one-dimensional representations. The dimension formula then gives

$$8 = 1^2 + 1^2 + 1^2 + 1^2 + d_5^2 \quad \Longrightarrow \quad d_5 = 2.$$

Now let's construct these representations. The one-dimensional ones are given by

$$\begin{aligned} \chi_{1,1} &: a \mapsto 1,\ b \mapsto 1 \\ \chi_{1,-1} &: a \mapsto 1,\ b \mapsto -1 \\ \chi_{-1,1} &: a \mapsto -1,\ b \mapsto 1 \\ \chi_{-1,-1} &: a \mapsto -1,\ b \mapsto -1. \end{aligned}$$

(Compare Example 10.8.) As for the two-dimensional one, there is one natural candidate: the action of D_8 on the square with a acting as a 90-degree rotation and b as a reflection. Explicitly, define $\rho\colon D_8 \to GL_2(\mathbb{C})$ by

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

A quick calculation confirms that these two matrices do not share a common eigenvector (in fact, $\rho(b)$ interchanges the $\pm i$-eigenspaces of $\rho(a)$). So ρ is irreducible.

Exercise 11.12. Confirm the assertions about D_8 made in the previous example. ▶

Lecture 11 Problems

11.1. Assume that $\operatorname{char} F \nmid |G|$. Let U be an irreducible FG-module. Prove that U occurs as a direct summand in the regular representation $F\langle G\rangle$ by considering the kernel and image of a non-zero map $f \in \operatorname{Hom}_G(F\langle G\rangle, U)$.

11.2. (a) Assume that $\operatorname{char} F \nmid |G|$. Show that if all of the irreducible FG-modules are one-dimensional, then G must be abelian. [Hint: Decompose the regular representation $F\langle G\rangle$ into a direct sum of irreducibles. The action of G on $F\langle G\rangle$ is faithful.]

(b) Show that the hypothesis $\operatorname{char} F \nmid |G|$ is necessary by proving that if $F = \mathbb{F}_3$ is the finite field of order 3, then $\operatorname{Irr}_F(S_3) = \{V_{\text{triv}}, V_{\text{sgn}}\}$.

11.3. In this problem you will determine $\operatorname{Irr}_{\mathbb{C}}(S_4)$.

(a) Prove that the trivial representation and the alternating representation are the only one-dimensional representations of S_4.

(b) Prove that the tensor product of an irreducible representation and a one-dimensional representation is irreducible. (Compare A2 Q4.)

(c) Determine the number and dimensions of the irreducible representations of S_4.

(d) Figure out (or look up) how to realize S_3 as a quotient of S_4. Use this to produce an irreducible two-dimensional representation of S_4.

(e) Describe $\operatorname{Irr}_{\mathbb{C}}(S_4)$.

11.4. Determine $\operatorname{Irr}_{\mathbb{C}}(A_4)$, where A_4 is the alternating group on four elements. [Hint: For the 3-dimensional representation, look at the previous problem.]

11.5. Consider the quaternion group of order 8 given by

$$Q_8 = \langle i, j, k\colon i^2 = j^2 = k^2 = ijk\rangle.$$

(a) Write 1 for $e \in Q_8$ and -1 for $i^2 \in Q_8$. Show that $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$.

(b) Determine the conjugacy classes and derived subgroup of Q_8. [Hint: There are 5 conjugacy classes.]

(c) Determine the one-dimensional representations of Q_8. [Hint: There are four (up to isomorphism).]

(d) Show that the map $\rho\colon Q_8 \to GL_2(\mathbb{C})$ defined by

$$\rho(i) = \begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix}, \quad \rho(j) = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \quad \text{and} \quad \rho(k) = \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix}$$

is a representation of Q_8. Show also that ρ irreducible and faithful.

(e) Describe $\mathrm{Irr}_{\mathbb{C}}(Q_8)$.

Lecture 12 Characters

In this lecture, and until further notice, all groups are finite, all representations are finite-dimensional, and our base field F will be $\mathbb{C}$.

The results of character theory take their strongest form over algebraically closed fields of characteristic zero. Just about everything we will do in the next several lectures will hold in that generality. I am choosing to work over $\mathbb{C}$ just to keep things simple. In particular, complex conjugation will allow us to streamline some of the arguments.

12.1 Definition and basic properties

One of the miracles of representation theory is that there is a very simple *complete invariant* of a representation. This is the *character* of the representation. Two representations are isomorphic if and only if their characters are equal.[12] Thus, the character *characterizes* the representation.

How would we go about finding a complete invariant of a representation? Any such invariant must also be a similarity invariant of matrices. This is because we can always pick a basis to get a matrix representation, and different bases produce isomorphic (similar) matrix representations. Looking for simple similarity invariants, one is quickly led to the coefficients of the characteristic polynomial, the most notable of which are the determinant and the trace. The determinant is too coarse of an invariant: There are non-isomorphic representations $\rho \not\cong \rho'$ such that $\det(\rho(g)) = \det(\rho'(g))$ for all $g \in G$. On the other hand, this somehow never happens for the trace! (This is far from obvious.)

Exercise 12.1. Give an example of representations $\rho \not\cong \rho'$ such that $\det(\rho(g)) = \det(\rho'(g))$ for all $g \in G$. ▶

Definition 12.2. The **character** of a $\mathbb{C}G$-module (V, ρ) is the function

$$\begin{aligned} \chi_\rho \colon G &\to \mathbb{C} \\ g &\mapsto \operatorname{tr}(\rho(g)). \end{aligned}$$

We sometimes write χ_V instead of χ_ρ. We also carry over terminology from (V, ρ) to χ_ρ. For example, if (V, ρ) is irreducible (resp., of degree n, faithful, ...) then we say χ_ρ is irreducible (resp., of degree n, faithful, ...).

The passage from ρ to χ_ρ seems like a huge compression of information. So it should be completely surprising that χ_ρ characterizes ρ up to isomorphism. This will still feel miraculous even after we develop the theory. However, let me at least give some hints as to why χ_ρ knows a lot about the representation ρ.

[12]This is only true in characteristic 0; hence the standing assumption in this lecture.

For $k \in \mathbb{Z}_{>0}$, the character value $\chi_\rho(g^k)$ is the sum of the eigenvalues of $\rho(g^k) = \rho(g)^k$. If the eigenvalues of $\rho(g)$ are $\lambda_1, \ldots, \lambda_n$, then the eigenvalues of $\rho(g)^k$ are $\lambda_1^k, \ldots, \lambda_n^k$, so χ_ρ knows the sums $\sum_i \lambda_i^k$ for all k. By Newton's identities, these sums can be used to determine the coefficients of the polynomial $\prod_i (x - \lambda_i)$ whose roots are the λ_i. Thus, χ_ρ knows the characteristic polynomials (hence the eigenvalues) of all $\rho(g)$. Furthermore, since each $\rho(g)$ is diagonalizable, this means that χ_ρ knows the diagonal matrix representing $\rho(g)$ in an eigenbasis. But there's a catch—two of them, in fact:

- χ_ρ doesn't know the eigenbasis. There is generally tension between the actual construction of the representation ρ on V and the character χ_ρ.
- Even if somehow we knew the eigenbasis for one $\rho(g)$, this in general will not be an eigenbasis for another $\rho(g')$. That is, we generally cannot *simultaneously* diagonalize all $\rho(g)$—not unless the group G is abelian.

Exercise 12.3. Find expressions for the coefficients of $p(x) = \prod_{i=1}^n (x - \lambda_i)$ in terms of the power sums $\sum_{i=1}^n \lambda_i^k$ $(0 \leq k \leq n)$ in the cases where $n = 2$ and $n = 3$. ▶

Let's look at some examples of characters.

Example 12.4 (Linear characters)**.** If $\deg \rho = 1$ then the character of ρ is ρ itself:

$$\chi_\rho(g) = \operatorname{tr} \rho(g) = \rho(g).$$

We call such characters **linear characters**. In particular, if G is abelian, then what we had previously called unitary characters are exactly the linear characters of G.

Example 12.5 (Trivial character)**.** The character of the trivial representation is called the **trivial character** and is denoted by χ_{triv}. We have $\chi_{\mathrm{triv}}(g) = 1$ for all $g \in G$.

Example 12.6. If $(\mathbb{C}^3, \rho)$ is the defining representation of S_3 (Example 3.1), then

$$\begin{aligned} \chi_\rho(1) &= 3, \\ \chi_\rho((1\ 2)) = \chi_\rho((1\ 3)) = \chi_\rho((2\ 3)) &= 1, \\ \chi_\rho((1\ 2\ 3)) = \chi_\rho((1\ 3\ 2)) &= 0. \end{aligned}$$

Example 12.7 (Permutation characters)**.** More generally, let (V, ρ) be the permutation representation induced by the action of an arbitrary G on the finite set X. Then, by considering the matrix of ρ in the standard basis, we see that

$$\chi_\rho(g) = |\mathrm{Fix}(g)| = |\{x \in X : gx = x\}|.$$

Exercise 12.8. Supply the details. ▶

Example 12.9 (Regular character)**.** Let χ_{reg} be the character of the regular representation of G. As a special case of the preceding example, we find that

$$\chi_{\text{reg}}(g) = \begin{cases} |G| & \text{if } g = e \\ 0 & \text{otherwise.} \end{cases}$$

The fact that the values of χ_ρ in Example 12.6 are constant on 2-cycles and on 3-cycles can be explained by recalling that elements with the same cycle type are conjugate in S_3, and trace is constant on conjugacy classes. In general, characters are constant on conjugacy classes. We record this fact, together with a few other basic properties of characters, in the next proposition.

Proposition 12.10 (Properties of Characters)**.** Let (V, ρ) and (W, σ) be representations of G. Then:

(a) $\chi_\rho(hgh^{-1}) = \chi_\rho(g)$ for all $g, h \in G$.

(b) If $V \cong W$ then $\chi_\rho = \chi_\sigma$. [The converse is true and will be proved later.]

(c) $\chi_\rho(e) = \dim V$.

(d) $\chi_{\rho\oplus\sigma}(g) = \chi_\rho(g) + \chi_\sigma(g)$.

(e) $\chi_{\rho\otimes\sigma}(g) = \chi_\rho(g)\chi_\sigma(g)$.

(f) $\chi_{\rho^*}(g) = \chi_\rho(g^{-1}) = \overline{\chi_\rho(g)}$.

(g) $|\chi_\rho(g)| \le \chi_\rho(e)$ for all $g \in G$.

Proof: Parts (a) and (b) follow from the fact that trace is a similarity invariant. Part (c) follows because, in a matrix representation, $\rho(e)$ is the $n \times n$ identity matrix, where $n = \dim V$.

Next, choose bases $\mathcal{B}$ for V and $\mathcal{C}$ for W and let $r(g)$ and $s(g)$ be the matrices of $\rho(g)$ and $\sigma(g)$ in these bases. Then, in the basis $\mathcal{B} \oplus \mathcal{C}$ basis for $V \oplus W$, the matrix of $(\rho \oplus \sigma)(g)$ is

$$\begin{bmatrix} r(g) & 0 \\ 0 & s(g) \end{bmatrix}.$$

Part (d) now follows. For part (e), in the $\mathcal{B} \otimes \mathcal{C}$ basis the matrix for $(\rho \otimes \sigma)(g)$ is the Kronecker product of $r(g)$ and $s(g)$:

$$\begin{bmatrix} r_{11}(g)s(g) & r_{12}(g)s(g) & \cdots \\ r_{21}(g)s(g) & r_{22}(g)s(g) & \cdots \\ \vdots & \vdots & \ddots \end{bmatrix}.$$

Thus,

$$\chi_{\rho\otimes\sigma}(g) = \sum_i r_{ii}(g)\operatorname{tr}(s(g)) = \operatorname{tr}(r(g))\operatorname{tr}(s(g)) = \chi_\sigma(g)\chi_\rho(g).$$

Next, if $\mathcal{B}^*$ is the dual bases for V^*, then $\rho^*(g) = \rho(g^{-1})^T$, whence $\chi_{\rho^*}(g) = \chi_\rho(g)^{-1}$ since $\operatorname{tr}(A^T) = \operatorname{tr}(A)$. This proves the first equality in part (f). For the second equality, observe that since the eigenvalues λ_i of $\rho(g)$ are roots of unity (because $g^{|G|} = 1 \implies \rho(g)^{|G|} = 1 \implies \lambda_i^{|G|} = 1$), the eigenvalues of $\rho(g^{-1})$ are thus $\lambda_i^{-1} = \overline{\lambda_i}$. Consequently, since trace is the sum of the eigenvalues, $\chi_\rho(g^{-1}) = \sum \overline{\lambda_i} = \overline{\sum \lambda_i} = \overline{\chi_\rho(g)}$. This proves part (f).

Finally, part (g) follows since $|\chi_\rho(g)| \leq \sum |\lambda_i| = \sum 1 = \dim V = \chi_\rho(e)$. ■

Remark 12.11. Parts (d) and (e) above show that the sum and product of two characters is again a character. This is not a priori obvious.

Example 12.12. In Example 12.7 we see that $\chi_\rho(e) = |X| = \dim V$, which is in line with Proposition 12.10(c).

Example 12.13 (Standard representation of S_3)**.** In Example 6.7 we decomposed the defining representation $V = \mathbb{C}^3$ of S_3 into the direct sum $V = U \oplus W$, where

$$U = \operatorname{span}\{(1,1,1)\} \quad \text{and} \quad W = \{(a,b,c) \colon a+b+c = 0\}.$$

Thus, $\chi_V = \chi_U + \chi_W$ by Proposition 12.10(d) and consequently $\chi_W = \chi_V - \chi_U$. The subspace U carries the trivial representation, so $\chi_U(\pi) = 1$ for all $\pi \in S_3$. The representation W is the standard representation of S_3 and its character is denoted by χ_{std}. We have $\chi_{\text{std}} = \chi_V - 1$. Using our calculation of χ_V from Example 12.6, we find:

$$\begin{aligned} \chi_{\text{std}}(1) &= 3 - 1 = 2 \\ \chi_{\text{std}}(\text{2-cycle}) &= 1 - 1 = 0 \\ \chi_{\text{std}}(\text{3-cycle}) &= 0 - 1 = -1. \end{aligned}$$

Lecture 12 Problems

12.1. Let (V, ρ) be a permutation representation of G with character χ_ρ. Show that the function $\psi \colon G \to \mathbb{C}$ defined by $\psi(g) = \chi_\rho(g) - 1$ is the character of some representation of G. Is this true if (V, ρ) is an arbitrary representation?

12.2. Prove that

$$|G| = \sum_{V \in \operatorname{Irr}_{\mathbb{C}}(G)} \chi_V(e)^2.$$

12.3. Let (V, ρ) be a $\mathbb{C}G$-module with character $\chi = \chi_\rho$. Prove:

(a) $|\chi(g)| = \chi(e)$ if and only if $\rho(g) = \lambda\,\mathrm{id}$ for some $\lambda \in \mathbb{C}$. [Hint: Examine the proof of Proposition 12.10(g).]

(b) $\chi(g) = \chi(e)$ if and only if $g \in \ker \rho$.

[We define the **kernel** of a character χ to be $\ker\chi = \{g \in G\colon \chi(g) = \chi(e)\}$. Part (b) shows that $\ker\chi_\rho = \ker\rho$.]

12.4. Show that if χ is a non-trivial irreducible character of G, then

$$\sum_{g\in G} \chi(g) = 0.$$

[Note: We proved a version of this in an earlier lecture. Do you remember where?]

12.5. Let χ be a character of G. Prove:

(a) If $g = g^{-1}$, then $\chi(g) \in \mathbb{Z}$.

(b) If g is conjugate to g^{-1}, then $\chi(g) \in \mathbb{R}$. Deduce that all characters of S_n are real-valued.

(c) If g is conjugate to g^i for all integers i that are coprime to $\operatorname{ord}(g)$, then $\chi(g) \in \mathbb{Z}$. Deduce that all characters of S_n are integer-valued. [Hint: If ζ is an nth root of unity, then $\sum_{\substack{1\le i\le n\\ \gcd(i,n)=1}} \zeta^i$ is an integer.]

Lecture 13 Orthogonality of Irreducible Characters

13.1 Class Functions

When G is abelian, we proved that the irreducible characters of G form an orthonormal basis for the space $\ell^2(G)$ of complex-valued functions on G (Theorem 10.5). We now search for an analogue of this for nonabelian groups. The identical assertion is definitely false since characters lie in a proper subspace of $\ell^2(G)$.

Definition 13.1. The space of **class functions** on G is the vector space

$$\mathcal{C}(G) = \{f \colon G \to \mathbb{C} \colon f(gxg^{-1}) = f(x) \text{ for all } g, x \in G\}$$

of complex-valued functions that are constant on the conjugacy classes of G. The **class number** of G, denoted by $h(G)$ or h, is the number of distinct conjugacy classes in G.

Every character of G belongs to $\mathcal{C}(G)$ by Proposition 12.10(a). If G is abelian, $\mathcal{C}(G) = \ell^2(G)$; for nonabelian G, $\mathcal{C}(G)$ is a proper subspace of $\ell^2(G)$. In general, a basis for $\mathcal{C}(G)$ is given by the indicator functions of the conjugacy classes of G. More precisely, if $C_1, \ldots, C_h$ are the distinct conjugacy classes of G, define $e_{C_i} \in \mathcal{C}(G)$ by

$$e_{C_i}(g) = \begin{cases} 1 & \text{if } g \in C_i \\ 0 & \text{otherwise.} \end{cases}$$

Then $\{e_{C_i}\}_{i=1}^h$ is a basis for $\mathcal{C}(G)$ and therefore

$$\dim \mathcal{C}(G) = h(G).$$

13.2 Character Orthogonality

We equip $\mathcal{C}(G)$ with the (Hermitian) inner product

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

Our goal now is to prove that the irreducible characters of G are orthogonal with respect to this inner product. The next result, which reformulates the inner product in more representation-theoretic terms, will be fundamental in achieving this goal.

Proposition 13.2. Let V and W be $\mathbb{C}G$-modules. Then:

$$\langle \chi_V, \chi_W \rangle = \dim \operatorname{Hom}_G(W, V) = \dim \operatorname{Hom}_G(V, W).$$

To prove this, we require the following lemma which is interesting in its own right. (It implies, for instance, that the multiplicity of the trivial representation in V is equal to $\langle \chi_V, \chi_{\text{triv}} \rangle$. We will generalize this below; see Corollary 13.7(a).)

Lemma 13.3. Let (V, ρ) be a $\mathbb{C}G$-module. Then:

$$\dim V^G = \frac{1}{|G|} \sum_{g \in G} \chi_V(g).$$

Proof: Each $g \in G$ defines a linear map $\rho(g)\colon V \to V$. Consider now

$$\widetilde{\rho} = \frac{1}{|G|} \sum_{g \in G} \rho(g).$$[13]

Then $\widetilde{\rho}$ is a G-linear map from V to V (as you can check) and

$$\operatorname{tr}(\widetilde{\rho}) = \frac{1}{|G|} \sum_{g \in G} \chi_V(g).$$

We can calculate $\operatorname{tr}(\widetilde{\rho})$ differently. Note that $\operatorname{im} \widetilde{\rho} = V^G$ and

$$\begin{aligned} \widetilde{\rho} \circ \widetilde{\rho} &= \frac{1}{|G|} \sum_{g \in G} \left(\frac{1}{|G|} \sum_{h \in H} \rho(gh) \right) \\ &= \frac{1}{|G|} \sum_{g \in G} \widetilde{\rho} \\ &= \widetilde{\rho}. \end{aligned}$$

Thus, $\widetilde{\rho}$ is a projection onto V^G. The lemma now follows from the exercise below. ■

Exercise 13.4. Let $P\colon V \to V$ be a projection. Prove that $\operatorname{tr}(P) = \dim(\operatorname{im} P)$. ▶

With this in hand, we now give:

Proof of Proposition 13.2: We have

$$\begin{aligned} \langle \chi_V, \chi_W \rangle &= \frac{1}{|G|} \sum_{x \in G} \chi_V(x) \overline{\chi_W(x)} \\ &= \frac{1}{|G|} \sum_{x \in G} \chi_V(x) \chi_{W^*}(x) && \text{(Proposition 12.10(f))} \\ &= \frac{1}{|G|} \sum_{x \in G} \chi_{V \otimes W^*}(x) && \text{(Proposition 12.10(e))} \\ &= \frac{1}{|G|} \sum_{x \in G} \chi_{\operatorname{Hom}(W,V)}(x) && \text{(Theorem 5.2)} \\ &= \dim\ (\operatorname{Hom}(W, V))^G && \text{(Lemma 13.3)} \\ &= \dim \operatorname{Hom}_G(W, V). && \text{(Exercise 5.1)} \end{aligned}$$

[13] Our old friend: the averaging trick.

This shows that $\langle \chi_V, \chi_W \rangle$ is a nonnegative integer and proves the first equality in the proposition. The second equality follows from:

$$\langle \chi_V, \chi_W \rangle = \overline{\langle \chi_V, \chi_W \rangle} = \langle \chi_W, \chi_V \rangle = \dim \mathrm{Hom}_G(V, W). \qquad \blacksquare$$

It is now easy to prove our main result.

Theorem 13.5 (Orthogonality of Irreducible Characters)**.** Let χ_V and χ_W be *irreducible* characters of G. Then:

$$\langle \chi_V, \chi_W \rangle = \begin{cases} 1 & \text{if } V \cong W \\ 0 & \text{if } V \ncong W. \end{cases}$$

Proof: Combine Proposition 13.2 and Corollary 8.3. ■

Remark 13.6. This result is the nonabelian version of part (a) of Theorem 10.5. This raises the question of whether the analogue of part (b) holds. Namely, do the irreducible characters of G form a basis for $\mathcal{C}(G)$? The answer is *yes*, as we will prove next time.

13.3 Consequences

We can extract some remarkable results from Theorem 13.5.

Corollary 13.7. Let V and W be $\mathbb{C}G$-modules. Then:

(a) If W is irreducible, then $\mathrm{mult}(W, V) = \langle \chi_W, \chi_V \rangle$. (Multiplicity Formula)

(b) $V \cong W$ if and only if $\chi_V = \chi_W$. (Isomorphism Criterion)

(c) V is irreducible if and only if $\langle \chi_V, \chi_V \rangle = 1$. (Irreducibility Criterion)

Proof: Let $V = \bigoplus_i V_i^{\oplus m_i}$ be the isotypic decomposition of V. Then $\chi_V = \sum m_i \chi_{V_i}$ and therefore,

$$\langle \chi_W, \chi_V \rangle = \sum_i m_i \langle \chi_W, \chi_{V_i} \rangle .$$

If W is irreducible then, according to Theorem 13.5, each inner product in the sum above is zero except if $W \cong V_i$ in which case the inner product is 1. Part (a) follows.

The forwards direction of part (b) was proved in Proposition 12.10(b). The backwards direction follows from part (a) since if $V = \bigoplus_{U \in \mathrm{Irr}(G)} U^{\oplus m_U}$ and $W = \bigoplus_{U \in \mathrm{Irr}(G)} U^{\oplus n_U}$ then $V \cong W$ if and only if

$$m_U = n_U \text{ for all } U \in \mathrm{Irr}_{\mathbb{C}}(G) \quad \iff \quad \langle \chi_U, \chi_V \rangle = \langle \chi_U, \chi_W \rangle \text{ for all } U \in \mathrm{Irr}_{\mathbb{C}}(G).$$

Finally, for part (c), observe that

$$\langle \chi_V, \chi_V \rangle = \sum_{i,j} m_i m_j \langle \chi_{V_i}, \chi_{V_j} \rangle = \sum_i m_i^2.$$

Thus, V is irreducible if and only if the above sum consists of a single summand m_1 with $m_1 = 1$. ■

Example 13.8. To showcase the power of Corollary 13.7, we will give another proof of the fact that every $U \in \operatorname{Irr}_{\mathbb{C}}(G)$ occurs in the regular representation $\mathbb{C}\langle G\rangle$ with multiplicity equal to $\dim U$ (Theorem 11.5).

For this, we simply compute:

$$\begin{aligned}
\operatorname{mult}(U, \mathbb{C}\langle G\rangle) &= \langle \chi_U, \chi_{\text{reg}}\rangle && \text{(Corollary 13.7(a))}\\
&= \frac{1}{|G|}\sum_{x\in G} \chi_U(x)\overline{\chi_{\text{reg}}(x)}\\
&= \chi_U(e) && \text{(Example 12.9)}\\
&= \dim U. && \text{(Proposition 12.10(c))}
\end{aligned}$$

Example 13.9. The characters χ_{reg}, χ_{def}, χ_{sgn} and χ_{std} of the regular, defining, alternating and standard representations of S_3 are given in the following table.

	e	$(1\ 2)$	$(2\ 3)$	$(1\ 3)$	$(1\ 2\ 3)$	$(1\ 3\ 2)$
χ_{reg}	6	0	0	0	0	0
χ_{def}	3	1	1	1	0	0
χ_{sgn}	1	-1	-1	-1	1	1
χ_{std}	2	0	0	0	-1	-1

We have

$$\begin{aligned}
\langle \chi_{\text{reg}}, \chi_{\text{std}}\rangle &= \frac{1}{6}(6(2) + 0(0) + 1(0) + 1(0) + 0(-1) + 0(-1) = 2\\
\langle \chi_{\text{def}}, \chi_{\text{std}}\rangle &= \frac{1}{6}(3(2) + 1(0) + 1(0) + 1(0) + 0(-1) + 0(-1) = 1.
\end{aligned}$$

Thus, $\operatorname{mult}(V_{\text{std}}, V_{\text{reg}}) = 2$ and $\operatorname{mult}(V_{\text{std}}, V_{\text{def}}) = 1$, as we already know.

On the other hand,

$$\begin{aligned}
\langle \chi_{\text{std}}, \chi_{\text{std}}\rangle &= \frac{1}{6}(2^2 + 0^2 + 0^2 + 0^2 + (-1)^2 + (-1)^2) = 1\\
\langle \chi_{\text{def}}, \chi_{\text{def}}\rangle &= \frac{1}{6}(3^2 + 1^2 + 1^2 + 1^2 + 0^2 + 0^2) = 2
\end{aligned}$$

which confirms that V_{std} is irreducible and V_{def} is not.

Finally, notice that

$$\chi_{\text{std}\otimes\text{sgn}} = \chi_{\text{std}}\chi_{\text{sgn}} = \chi_{\text{std}}.$$

(Multiply the values of χ_{std} and χ_{sgn} in the above table.) This shows that $V_{\text{std}} \otimes V_{\text{sgn}} \cong V_{\text{std}}$.

Exercise 13.10. Give another (character-free) proof that $V_{\text{std}} \otimes V_{\text{sgn}} \cong V_{\text{std}}$. ▶

Example 13.11. Let's use the character values from the preceding example to determine the isotypic decomposition of $V = V_{\text{std}} \otimes V_{\text{std}}$. First, we calculate

$$\chi_V = \chi_{\text{std}}\chi_{\text{std}} = \begin{bmatrix} 4 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

Next, we determine the multiplicities of each $U \in \text{Irr}_{\mathbb{C}}(G)$ in V:

$$\begin{aligned}
\langle \chi_V, \chi_{\text{triv}} \rangle &= \frac{1}{6}(4+0+0+0+1+1) = 1 \\
\langle \chi_V, \chi_{\text{sgn}} \rangle &= \frac{1}{6}(4+0(-1)+0(-1)+0(-1)+1+1) = 1 \\
\langle \chi_V, \chi_{\text{std}} \rangle &= \frac{1}{6}(4(2)+0+0+1(-1)+1(-1)) = 1.
\end{aligned}$$

Thus,

$$V \cong V_{\text{triv}} \oplus V_{\text{sgn}} \oplus V_{\text{std}}.$$

Exercise 13.12. Determine the isotypic decomposition of $V_{\text{std}}^{\otimes 3} = V_{\text{std}} \otimes V_{\text{std}} \otimes V_{\text{std}}$. ▶

Lecture 13 Problems

13.1. Comb through the previous lectures and give character-theoretic arguments for as many results and problems as possible. (A non-obvious example is Problem 3 below.)

13.2. Let (V, ρ) be a $\mathbb{C}G$-module. Choose a basis $\mathcal{B}$ for V and let $r\colon G \to GL_n(\mathbb{C})$ be the corresponding matrix representation given by $r(g) = [\rho(g)]_{\mathcal{B}}$. Define a new representation $\overline{r}\colon G \to GL_n(\mathbb{C})$ by $\overline{r}(g) = \overline{r(g)}$ (complex conjugate each of the entries of $r(g)$).

(a) Show that carrying out this procedure using a different basis for V produces a matrix representation that is equivalent to $\overline{r}$. We thus obtain a $\mathbb{C}G$-module $(\overline{V}, \overline{\rho})$ that is well-defined up to isomorphism.

(b) Prove that $\overline{V} \cong V^*$. [Hint: What is $\chi_{\overline{V}}$?]

13.3. Let X be a finite G-set and let $V = F\langle X\rangle$ be the induced permutation representation.

(a) Show that the multiplicity of the trivial representation in V is given by

$$\frac{1}{|G|}\sum_{g\in G} \#\text{Fix}(g),$$

where $\text{Fix}(g) = \{x \in X\colon gx = x\}$ is the set of fixed points of g.

(b) Use part (a) to give a proof of Burnside's Lemma (Problem 1.2):

$$\frac{1}{|G|}\sum_{g\in G} \#\text{Fix}(g) = \text{number of } G\text{-orbits in } X.$$

[Hint: Problem 3.3.]

13.4. Let X be a G-set and assume $|X| \geq 2$. Let $V = \mathbb{C}\langle X \rangle$ be the associated permutation representation.

The action of G on X is said to be **2-transitive** if G can send any pair of distinct elements to any other such pair, i.e. given $(x, y), (x', y') \in X^2$ with $x \neq y$ and $x' \neq y'$, there exists a $g \in G$ such that $gx = x'$ and $gy = y$.

(a) Show that the action of G on X is 2-transitive if and only if the induced action on X^2 (via $g(x, y) = (gx, gy)$) has precisely two G-orbits.

(b) Prove that $\langle \chi_V, \chi_V \rangle = 2$ if and only if the G-action on X is 2-transitive.

(c) Deduce that $\chi_V - \chi_{\text{triv}}$ is irreducible if and only if the G-action on X is 2-transitive.

(d) Conclude that if V is the permutation representation induced by a 2-transitive G-action, then V decomposes as $V = V_{\text{triv}} \oplus U$ where U is an irreducible representation.

(e) Use part (d) to give another proof that the standard representation of S_n is irreducible. Show also that the restriction of the standard representation to A_n remains irreducible if $n \geq 3$.

Lecture 14 Completeness of Irreducible Characters

Our goal is to now prove the nonabelian version Theorem 10.5(b):

Theorem 14.1. The set $\{\chi_V : V \in \mathrm{Irr}_{\mathbb{C}}(G)\}$ is an orthonormal basis for $\mathcal{C}(G)$.

The difficulty lies in connecting $\mathcal{C}(G)$ to the representation theory of G. To this end, recall that $\mathcal{C}(G) \subseteq \ell^2(G)$ and $\ell^2(G)$ is isomorphic to the regular representation $\mathbb{C}\langle G\rangle$ of G via

$$\begin{aligned} \ell^2(G) &\xrightarrow{\sim} \mathbb{C}\langle G\rangle \\ f &\longmapsto \sum_{g\in G} f(g)g. \end{aligned}$$

Now, given any representation V of G, the element $\sum_{g\in G} f(g)g$ acts on V in a natural way. This prompts the following.

Lemma 14.2. Let (V,ρ) be a $\mathbb{C}G$-module. Given $f \in \mathcal{C}(G)$, define $\rho_f : V \to V$ by

$$\rho_f(v) = \sum_{g\in G} f(g)\rho(g)v.$$

Then:

(a) ρ_f is a G-linear map.

(b) If V is irreducible then $\rho_f = \lambda\,\mathrm{id}_V$, where $\lambda = \dfrac{|G|}{\dim V}\langle f, \chi_{V^*}\rangle$.

Proof: Let $h \in G$. Then:

$$\begin{aligned} \rho_f(\rho(h)v) &= \sum_{g\in G} f(g)\rho(g)\rho(h)v \\ &= \sum_{g\in G} f(g)\rho(gh)v \\ &= \sum_{g\in G} f(hgh^{-1})\rho(hgh^{-1}h)v && \text{(re-index } g \leftrightarrow hgh^{-1}\text{)} \\ &= \sum_{g\in G} f(g)\rho(hg)v && (f \in \mathcal{C}(G)) \\ &= \sum_{g\in G} f(g)\rho(h)\rho(g)v \\ &= \rho(h)\rho_f(v). \end{aligned}$$

This proves part (a). For part (b), Schur's Lemma tells us that $\rho_f = \lambda\,\mathrm{id}_V$. To determine λ, we take the trace of both sides:

$$\begin{aligned}
\lambda \dim V &= \operatorname{tr}(\lambda \operatorname{id}_V) \\
&= \operatorname{tr}(\rho_f) \\
&= \operatorname{tr}\left(\sum_{g\in G} f(g)\rho(g)\right) \\
&= \sum_{g\in G} f(g)\operatorname{tr}(\rho(g)) \\
&= \sum_{g\in G} f(g)\chi_V(g) \\
&= \sum_{g\in G} f(g)\overline{\chi_{V^*}(g)} && \text{(Proposition 12.10(f))} \\
&= |G| \langle f, \chi_{V^*}\rangle .
\end{aligned}$$

So $\lambda = \dfrac{|G|}{\dim V}\langle f, \chi_{V^*}\rangle$, as required. ■

Proof of Theorem 14.1: Let $S = \{\chi_V : V \in \operatorname{Irr}_{\mathbb{C}}(G)\}$. We proved in Theorem 13.5 that S is orthonormal, so all that remains is to prove that S spans $\mathcal{C}(G)$. Let $U = \operatorname{span} S$ and let $U^\perp$ be the orthogonal complement of U in $\mathcal{C}(G)$. We wish to show that $U^\perp = 0$.

Take $f \in U^\perp$ so that $\langle f, \chi_V\rangle = 0$ for all $V \in \operatorname{Irr}_{\mathbb{C}}(G)$. Given a $\mathbb{C}G$-module (V, ρ), let ρ_f be as in Lemma 14.2. If V is irreducible, then $\rho_f = 0$ by Lemma 14.2(b) as $\langle f, \chi_{V^*}\rangle = 0$ since V^* is irreducible (why?). Consequently, $\rho_f = 0$ for *any* (V, ρ) since we can decompose V into a direct sum $V = \bigoplus_i U_i$ of irreducible subspaces. (Note that $\rho_f = \sum f(g)\rho(g)$ sends the G-invariant subspace U_i to itself; hence $\rho_f|_{U_i} = 0$ for each i.)

In particular, if $V = \mathbb{C}\langle G\rangle$ is the regular representation, then $\rho_f(e) = 0 \in \mathbb{C}\langle G\rangle$. However, $\rho_f(e) = \sum_g f(g)ge = \sum_g f(g)g$ is zero in $\mathbb{C}\langle G\rangle$ if and only if $f(g) = 0$ for all $g \in G$. Thus, $f = 0$ and consequently $U^\perp = 0$, as desired. ■

Exercise 14.3. Prove that if V is irreducible then V^* is irreducible. ▶

We deduce that each $f \in \mathcal{C}(G)$ has a “Fourier series” expansion of the form

$$f = \sum_{V\in \operatorname{Irr}_{\mathbb{C}}(G)} \langle f, \chi_V\rangle \chi_V .$$

(Compare (8).) As another consequence, we can now finally prove our result concerning the size of $\operatorname{Irr}_{\mathbb{C}}(G)$.

Corollary 14.4. The number of irreducible complex representations of G is equal to the number of conjugacy classes of G.

Proof: On the one hand, $\dim \mathcal{C}(G)$ is equal to the number of conjugacy classes of G. On the other hand, $\dim \mathcal{C}(G)$ is equal to the number of irreducible representations. ■

Remark 14.5. Theorem 14.1 and Corollary 14.4 are two of the cornerstones of the subject. I want to sketch an alternative approach to both, as a preview of the second half of the course.

The idea is to start with the isotypic decomposition of the regular representation:

$$\ell^2(G) = \bigoplus_{V \in \mathrm{Irr}(G)} V^{\oplus d_V},$$

where we know that $d_V = \dim V$. If you squint, a direct sum of $\dim V$ copies of V looks a lot like $M_d(\mathbb{C})$. So our decomposition really takes the form

$$\ell^2(G) \cong \bigoplus_{i=1}^{r} M_{d_i}(\mathbb{C}).$$

The right-side, being a product of rings, is a ring. Can we view the left-side as a ring? Well yes, we can use pointwise product of functions—but this is certainly not the right thing here (it gives a commutative ring whereas the right-side is generally noncommutative). Amazingly, there is a natural way to turn $\ell^2(G)$ into a ring in such a way that the above decomposition is also *an isomorphism of rings*! This is a special case of the celebrated Artin–Wedderburn theorem. Moreover, the center of the ring $\ell^2(G)$ turns out to be the subring of class functions $\mathcal{C}(G)$. On the other hand, the center of each $M_{d_i}(\mathbb{C})$ is just scalar matrices $\mathbb{C}I_{d_i}$. Thus, we have an isomorphism of rings (and $\mathbb{C}$-vector spaces):

$$\mathcal{C}(G) \cong \mathbb{C}^r.$$

Upon taking dimensions, we arrive at $\dim \mathcal{C}(G) = r$, that is, $h(G) = |\mathrm{Irr}_{\mathbb{C}}(G)|$.

14.1 Some Complements

14.1.1 An Orthogonal Basis for $\ell^2(G)$

So far, in trying to generalize Theorem 10.5, we've attempted to determine the subspace of $\ell^2(G)$ spanned by the irreducible characters of G. However, an equally valid pursuit would be to search for an orthogonal basis for $\ell^2(G)$ that is of a representation-theoretic nature. This is indeed possible.

The starting point is the following. Given a $\mathbb{C}G$-module (V, ρ), pick a basis $\mathcal{B}$ for V and let $r\colon G \to GL_n(\mathbb{C})$ be the corresponding matrix representation given by $r(g) = [\rho(g)]_{\mathcal{B}}$ for $g \in G$. Write

$$r(g) = \begin{bmatrix} r_{11}(g) & \cdots & r_{1n}(g) \\ \vdots & & \vdots \\ r_{n1}(g) & \cdots & r_{nn}(g) \end{bmatrix}.$$

The functions $r_{ij}\colon G \to \mathbb{C}$ are called the **matrix coefficients** of r. They belong to $\ell^2(G)$ but generally not to $\mathcal{C}(G)$. Note also that

$$\chi_V(g) = r_{11}(g) + \cdots r_{nn}(g).$$

Theorem 14.6 (Schur's Orthogonality Relations)**.** Let (V,ρ) and (W,σ) be irreducible $\mathbb{C}G$-modules, and let $r\colon G \to GL_n(\mathbb{C})$ and $s\colon G \to GL_m(\mathbb{C})$ be associated matrix representations. Assume a basis for W has been chosen so that, for each $g \in G$, $s(g)$ is a unitary matrix.[14] Then:

(a) If $V \not\cong W$, $\langle r_{ij}, s_{kl}\rangle = 0$ for all i,j,k,l. (First Orthogonality Relation)

(b) $\langle s_{ij}, s_{kl}\rangle = \delta_{ik}\delta_{jl}\dfrac{1}{\dim W}$. (Second Orthogonality Relation)

Proof: See Serre, §2.2, Cors. 2 and 3. Our assumption on $s(g)$ gives $s_{kl}(g^{-1}) = \overline{s_{lk}(g)}$. ■

Exercise 14.7. Use Theorem 14.6 to give another proof of Theorem 13.5. ▸

This shows that matrix coefficients corresponding to different irreducible representations are orthogonal. On the other hand, the (unitary) matrix coefficients for a fixed $W \in \mathrm{Irr}_{\mathbb{C}}(G)$ form an orthogonal basis for the subspace of $\ell^2(G)$ that they span. The dimension of this subspace is equal to the number of matrix coefficients, i.e., $(\dim W)^2$. I claim that this subspace is the W^*-isotypic piece of $\ell^2(G)$. The dimensions certainly match up, since $\ell^2(G)$ contains $\dim W^* = \dim W$ copies of W^*.

Lemma 14.8. Let $W \in \mathrm{Irr}_{\mathbb{C}}(G)$. Choose a basis for W so that the corresponding matrix representation $s\colon G \to GL_n(\mathbb{C})$ consists of unitary matrices. Let W' be the subspace of $\ell^2(G)$ spanned by the matrix coefficients $\{s_{ij}\}_{i,j=1}^n$. If we view $\ell^2(G)$ as the representation space for the (left) regular representation, then:

(a) W' is a G-invariant subspace of $\ell^2(G)$.

(b) $W' \cong W^*$.

Proof: Let $\mathcal{B} = \{e_1, \ldots, e_n\}$ be the basis of W giving s. Then

$$s_{ij}(x) = \langle s(x)e_j, e_i\rangle \text{ for all } x \in G.$$

We now determine the action of $g \in G$ on s_{ij}:

$$(gs_{ij})(x) = s_{ij}(g^{-1}x) = \langle s(g)^*(x)e_j, e_i\rangle = \langle s(x)e_j, s(g)e_i\rangle = \sum_k \overline{s_{ki}(g)}\,\langle s(x)e_j, e_k\rangle\,.$$

Thus, gs_{ij} is a linear combination of other matrix coefficients s_{kj} hence belongs to W'. So W' is G-invariant. Next, let $\overline{W} = W$ but with G-action given by $g \cdot v = \overline{r(g)}v$. For each j,

[14] By Weyl's unitary trick (Proposition 7.9), it is always possible to find such a basis.

we can define a map

$$\begin{aligned} T_j \colon \overline{W} &\to W' \\ e_i &\mapsto s_{ij}. \end{aligned}$$

Each T_j is a linear isomorphism from $\overline{W}$ onto $\operatorname{span}\{s_{ij}\}_{i=1}^{n}$ since it maps a basis to a basis. (The second orthogonality relation tells us that the s_{ij} are linearly independent.) The map T_j is moreover G-linear, since

$$ge_i = \sum_k \overline{s_{ki}(g)} e_k$$

hence

$$T(ge_i) = \sum_k \overline{s_{ki}(g)} s_{kj} = g \cdot s_{ij}$$

by what we had calculated earlier. Since $\overline{W} \cong W^*$ (Problem 13.2), the proof is complete. ■

Remark 14.9. Had we given $\ell^2(G)$ the *right* regular representation, we would have found that $W' \cong W$. Compare Remark 11.2.

The preceding proof shows that we actually obtain $n = \dim W^*$ isomorphisms $T_1, \ldots, T_n$ from W^* into $\ell^2(G)$ whose images are pairwise orthogonal (by the second orthogonality relation). Hence the sum of the images is isomorphic to $\dim W^*$ copies of W^* in $\ell^2(G)$ which must therefore by the W^*-isotypic component of $\ell^2(G)$. Furthermore, we can do this for each $W \in \operatorname{Irr}_{\mathbb{C}}(G)$, and the totality of resulting subspaces in $\ell^2(G)$ are pairwise orthogonal by the first orthogonality relation. We conclude:

Theorem 14.10. For each $W \in \operatorname{Irr}_{\mathbb{C}}(G)$, fix a unitary representation $s^W \colon G \to GL_{n_W}(\mathbb{C})$, where $n_W = \dim W$, and let $\mathcal{B}_W = \{\sqrt{n_W}\, s_{ij}^W\}_{i,j=1}^{n_W}$ be the corresponding matrix coefficients. Then $\bigcup_{W \in \operatorname{Irr}_{\mathbb{C}}(G)} \mathcal{B}_W$ is an orthonormal basis for $\ell^2(G)$. ■

Remark 14.11. If G is abelian, then the matrix coefficients of each $\chi \in \widehat{G} = \operatorname{Irr}_{\mathbb{C}}(G)$ consist of only χ itself, so Theorem 14.10 reduces to Theorem 10.5.

14.1.2 Burnside's Irreducibility Theorem

In this section, I want to mention a beautiful result due to Burnside. Here is the statement:

Theorem 14.12 (Burnside's Irreducibility Theorem)**.** Let $r \colon G \to GL_n(\mathbb{C})$ be an irreducible matrix representation of G. Then

$$\operatorname{span}\{r(g) \colon g \in G\} = M_n(\mathbb{C}).$$

Proof: There is a very nice (and short!) proof due to T.Y. Lam in *A Theorem of Burnside on Matrix Rings*, Amer. Math. Monthly, Vol. 105 (1998), No. 7, 651–653. ■

One way to interpret this result is via matrix coefficients. The theorem says that if you have an irreducible representation r of G, then there cannot be any nontrivial linear relationships between the matrix coefficients of r. This is because such a relationship would force the matrices $r(g)$ to lie in a proper subspace of $M_n(\mathbb{C})$.

For example, there can be no irreducible representation of G whose image lands in the proper subspace

$$\left\{ \begin{bmatrix} a & b \\ c & a \end{bmatrix} : a, b, c \in \mathbb{C} \right\}.$$

In terms of matrix coefficients, the relationship being implicitly imposed here is $r_{11} - r_{22} = 0$. Likewise, no irreducible representation can have image in

$$\left\{ \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} : a + b + c = d + e + f = g + h + i \right\}.$$

Lecture 14 Problems

14.1. Let $f \in \mathcal{C}(G)$. Prove that f is the character of some representation of G if and only if $\langle f, \chi_V \rangle \in \mathbb{Z}_{\geq 0}$ for all $V \in \mathrm{Irr}_{\mathbb{C}}(G)$.

14.2. Let $g, h \in G$.

(a) Show that if $\chi(g) = \chi(h)$ for all irreducible characters χ of G then g and h must be conjugate in G.

(b) Show that the character value $\chi(g)$ is real for all irreducible characters χ if and only if g is conjugate to g^{-1}.

14.3. Let V be a $\mathbb{C}G$-module and W a $\mathbb{C}H$-module. In what follows, we view $V \otimes W$ as a $\mathbb{C}(G \times H)$-module with action given by $(g, h) \cdot (v \otimes w) = gv \otimes hw$.

(a) Show that $\chi_{V \otimes W}(g, h) = \chi_V(g)\chi_W(h)$.

(b) Prove that if V is irreducible and W is irreducible then $V \otimes W$ is irreducible.

(c) Prove that every irreducible $\mathbb{C}(G \times H)$-module is of the form $V \otimes W$ for some irreducible $\mathbb{C}G$-module V and irreducible $\mathbb{C}H$-module W. [Hint: Count irreps.]

The above can be summarized as "$\mathrm{Irr}_{\mathbb{C}}(G \times H) = \mathrm{Irr}_{\mathbb{C}}(G) \otimes \mathrm{Irr}_{\mathbb{C}}(H)$."

14.4. (Challenging) Prove, without appealing to Burnside's theorem, that there can be no irreducible representation $r \colon G \to GL_n(\mathbb{C})$ whose image lands in

$$\left\{ \begin{bmatrix} a & b \\ c & a \end{bmatrix} : a, b, c \in \mathbb{C} \right\}.$$

Lecture 15 The Character Table

Since every $\mathbb{C}G$-module V is the direct sum of irreducible representation (say $V = \oplus_i V_i$), every character is the direct sum of irreducible characters ($\chi_V = \sum_i \chi_{V_i}$). Furthermore, since every character χ is constant on each conjugacy class C of G, we may write $\chi(C)$ to unambiguously denote the value of χ at any $g \in C$. It follows that the fundamental character-theoretic information is contained in the values of the irreducible characters of G on the conjugacy classes of G. We tabulate this information as follows.

Definition 15.1. The **character table** of G is the table whose columns are indexed by the conjugacy classes C of G, whose rows are indexed by the irreducible characters χ of G, and where the (χ, C) entry is the character value $\chi(C)$:

	$\cdots$	C	$\cdots$
$\vdots$			
χ		$\chi(C)$	
$\vdots$			

By convention, representatives for the conjugacy classes are used to label the columns, the trivial character is placed in the first row, and the conjugacy class $\{e\}$ is placed in the first column. Additionally, we sometimes record the size of the conjugacy class at the top of each column.

Note that since the number of irreducible representations of G is equal to the number of conjugacy classes of G, the character table is square.

Example 15.2. The character tables of $C_3 = \langle a \rangle$ and $C_4 = \langle b \rangle$ are given below.

	e	a	a^2
χ_0	1	1	1
χ_1	1	ω	ω^2
χ_2	1	ω^2	ω

	e	b	b^2	b^3
χ_0	1	1	1	1
χ_1	1	i	-1	$-i$
χ_2	1	-1	1	-1
χ_3	1	$-i$	-1	i

In the above, ω is a primitive third root of unity. More generally, if ζ is a primitive nth root of unity, then the character table of $C_n = \langle c \rangle$ is given by

	e	c	c^2	$\cdots$	c^{n-1}
χ_0	1	1	1	$\cdots$	1
χ_1	1	ζ	ζ^2	$\cdots$	ζ^{n-1}
χ_2	1	ζ^2	ζ^4	$\cdots$	ζ^{n-2}
$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$
χ_{n-1}	1	ζ^{n-1}	ζ^{2n-1}	$\cdots$	ζ

(Refer to Example 8.7.)

Exercise 15.3. Determine the character table of the Klein four-group $C_2 \times C_2$. ▶

Example 15.4. The character table of S_3 is:

	1	3	2
	e	$(1\ 2)$	$(1\ 2\ 3)$
χ_{triv}	1	1	1
χ_{sgn}	1	−1	1
χ_{std}	2	0	−1

We have chosen representatives for the conjugacy classes and we have recorded the sizes of the conjugacy classes at the top of each column. Notice that the first column gives the degrees of the respective characters. We will be interested in learning what other information can be gleaned from the character table.

Example 15.5. The character table of $D_8 = \langle a, b \colon a^4 = b^2 = e, ba = a^{-1}b \rangle$ is:

	1	1	2	2	2
	e	a^2	a	b	ab
$\chi_{1,1}$	1	1	1	1	1
$\chi_{1,-1}$	1	1	1	−1	−1
$\chi_{-1,1}$	1	1	−1	1	−1
$\chi_{-1,-1}$	1	1	−1	−1	1
χ_V	2	−2	0	0	0

(Refer to Example 11.11.) Let's determine the character table of the other nonabelian group of order 8, namely the quaternion group

$$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}.$$

(See Problem 11.5.) By direct calculation, we find that:

- The conjugacy classes of Q_8 are $\{1\}$, $\{-1\}$, $\{\pm i\}$, $\{\pm j\}$, $\{\pm k\}$.
- The derived subgroup is $[Q_8, Q_8] = \{\pm 1\}$ with quotient $Q_8/[Q_8, Q_8] \cong C_2 \times C_2$ generated by the images of i and j.

This gives the partial character table:

	1	1	2	2	2
	1	−1	i	j	k
χ_0	1	1	1	1	1
χ_1	1	1	1	−1	−1
χ_2	1	1	−1	1	−1
χ_3	1	1	−1	−1	1
χ_4	?	?	?	?	?

The dimension formula (Corollary 11.7(b)) gives the degree of the remaining character: $\chi_4(e) = 2$. We can easily determine the remaining values of χ_4 using the orthogonality relations (see below), but for now let's appeal to Problem 11.5(d) and let χ_4 be the character of the representation defined there. A direct calculation gives:

$$\chi_4 = \begin{bmatrix} 2 & -2 & 0 & 0 & 0 \end{bmatrix}.$$

Thus, the character table of Q_8 is identical to the character table of D_8!

Remark 15.6. The groups Q_8 and D_8 are not isomorphic. For instance, Q_8 has six elements of order 4 (namely $\pm i, \pm j, \pm k$) whereas D_8 only has two (namely a and a^3). So the previous example shows that we **cannot** use the character table of G to determine:

- The isomorphism class of G.
- The subgroup lattice of G.
- The orders of the elements of G.

On the other hand, we **can** determine:

- The order of G: $|G| = \sum_{i=1}^{h} \chi_i(e)^2$ (the sum of the squares of the entries in the first column).
- The order of $G/[G,G]$: $|G/[G,G]| =$ the number of characters of degree 1 (i.e. the number of rows that have a first entry of 1).

We will expand the second list soon.

15.1 The Orthogonality Relations

If you stare at the character tables we've determined above, you will eventually start to notice some striking general phenomena. For instance:

Theorem 15.7. Let $\chi_1, \ldots, \chi_h$ and $C_1, \ldots, C_h$ be the irreducible characters and conjugacy classes of G, respectively. Then:

(a) $$\frac{1}{|G|} \sum_{k=1}^{h} |C_k| \chi_i(C_k) \overline{\chi_j(C_k)} = \delta_{ij}. \qquad \text{(Row Orthogonality)}$$

(b) $$\frac{1}{|G|} \sum_{k=1}^{h} \chi_k(C_i) \overline{\chi_k(C_j)} = \frac{1}{|C_i|} \delta_{ij}. \qquad \text{(Column Orthogonality)}$$

Proof: Part (a) is Theorem 13.5 re-written using the fact that characters are constant on conjugacy classes. We can derive part (b) from part (a), as follows.

Let X be the $h \times h$ matrix whose (i, j)th entry is

$$X_{ij} = \frac{|C_j|^{1/2}}{|G|^{1/2}} \chi_i(C_j).$$

If X^* is the conjugate-transpose of X, then the (i, j)th entry of XX^* is given by

$$\sum_{k=1}^{h} \frac{|C_k|}{|G|} \chi_i(C_k)\overline{\chi_j(C_k)} = \delta_{ij},$$

by part (a). Thus, $XX^* = I_h$. Hence $X^*X = I_h$ and the column orthogonality relations follow from this, as you can check. ■

Example 15.8. Consider the partially completed character table of Q_8:

	1	1	2	2	2
	1	-1	i	j	k
χ_0	1	1	1	1	1
χ_1	1	1	1	-1	-1
χ_2	1	1	-1	1	-1
χ_3	1	1	-1	-1	1
χ_4	a	b	c	d	e

The column orthogonality relation applied to the first column gives the dimension formula

$$\frac{1}{|Q_8|}(1^2 + 1^2 + 1^2 + 1^2 + a^2) = \frac{1}{|C_1|} = 1.$$

Thus, $a = 2$. (Note: Technically, the relation only gives $a^2 = 4$, but we know that a is a positive integer since $\chi_4(e) = \deg \chi_4$.) If we apply the orthogonality relation to the "inner product" of the first and second columns, we get:

$$\frac{1}{8}(1^2 + 1^2 + 1^2 + 1^2 + 2b) = 0, \quad \text{hence } b = -2.$$

Likewise, applying it to the inner products of the first column with the third, fourth and fifth columns, we find that $c = d = e = 0$.

Example 15.9. Consider the character table of S_3:

	1	3	2
	e	$(1\ 2)$	$(1\ 2\ 3)$
χ_{triv}	1	1	1
χ_{sgn}	1	-1	1
χ_{std}	2	0	-1

The row orthogonality relation says that "inner products" of the third row with itself and with the first row are given by

$$\frac{1}{6}((1)2^2 + (3)0^2 + (2)(-1)^2) = 1$$
$$\frac{1}{6}((1)1 \cdot 2 + (3)1 \cdot 0 + (2)1 \cdot (-1)) = 0.$$

It is important to remember to include the sizes of the conjugacy classes in these calculations.

Lecture 15 Problems

15.1. Determine the character table of the dihedral group

$$D_{2n} = \langle a, b \colon a^n = b^2 = e, ab = ba^{-1} \rangle.$$

[Hint: Consider the cases $n = 2m$ and $n = 2m + 1$ separately.]

15.2. The character table of a certain group G is given below.

	$\{e\}$	C_1	C_2	C_3	C_4	C_5
χ_0	1	1	1	1	1	1
χ_1	1	1	1	-1	-1	1
χ_2	1	-1	1	i	$-i$	-1
χ_3	1	-1	1	$-i$	i	-1
χ_4	2	2	-1	0	0	-1
χ_5	2	-2	-1	0	0	1

Determine the order of G and the sizes of the conjugacy classes $C_1, \ldots, C_5$.

15.3. The partial character table of a certain group G of order 24 is given below.

	$\{e\}$	C_1	C_2	C_3	C_4	C_5	C_6
χ_1	1	1	ω	ω^2	1	ω	ω^2
χ_2	2	-2	-1	-1	0	1	1

Determine the complete the character table. [Note: $\omega = \exp(2\pi i/3)$.]

15.4. Let $X = [\chi_i(C_j)]$ be the matrix whose entries are the entries of the character table of G. Determine $|\det X|^2$.

Lecture 16 Inflation and Kernels

16.1 Inflation from Quotients

We begin with an example.

Example 16.1 (Character table of S_4)**.** The conjugacy classes of the symmetric group S_n consist of the cycles of a given cycle type. In S_4, the cycle types are $(1,1,1,1)$ (i.e. four 1-cycles), $(2,1,1)$ (one 2-cycle and two 1-cycles), $(3,1)$ (one 3-cycle and one 1-cycle), (4) (one 4-cycle) and $(2,2)$ (two 2-cycles). The sizes of the corresponding conjugacy classes are 1, 6, 8, 6 and 3 (exercise) and representatives are given by e, (1 2), (1 2 3), (1 2 3 4) and (1 2)(3 4), resp. The only one-dimensional representations are the trivial and alternating representations. The dimension formula (Corollary 11.7(b)) then reads

$$24 = 1^2 + 1^2 + d_3^2 + d_4^2 + d_5^2,$$

where $d_3, d_4, d_5 > 1$ are the degrees of the remaining irreducible characters. The only possibility here is $d_3 = 2$ and $d_4 = d_5 = 3$.

The standard representation of S_4 (Problem 9.3) is irreducible and of degree 3. Explicitly, if we let $V_{\text{def}} = \mathbb{C}^4$ be the permutation representation induced by the action of S_4 on $\{1,2,3,4\}$, then since $\chi_{\text{def}}(\pi) = |\text{Fix}(\pi)|$ (Example 12.7), we find that

$$\chi_{\text{def}} = \begin{bmatrix} 4 & 2 & 1 & 0 & 0 \end{bmatrix}.$$

Hence

$$\chi_{\text{std}} = \chi_{\text{def}} - \chi_{\text{triv}} = \begin{bmatrix} 3 & 1 & 0 & -1 & -1 \end{bmatrix}.$$

(As confirmation that the standard representation is irreducible, we can calculate that $\langle \chi_{\text{std}}, \chi_{\text{std}} \rangle = 1$.) Thus, we have the following partial character table:

	1	6	8	6	3
	e	(1 2)	(1 2 3)	(1 2 3 4)	(1 2)(3 4)
χ_{triv}	1	1	1	1	1
χ_{sgn}	1	-1	1	-1	1
χ_U	2				
χ_V	3				
χ_{std}	3	1	0	-1	-1

There is an obvious candidate for χ_V: Let $V = V_{\text{std}} \otimes V_{\text{sgn}}$ so that

$$\chi_V = \chi_{\text{std}}\chi_{\text{sgn}} = \begin{bmatrix} 3 & -1 & 0 & 1 & -1 \end{bmatrix}.$$

This is irreducible since V is the tensor product of an irreducible representation and a 1-dimensional representation. (Alternatively, note that $\langle \chi_V, \chi_V \rangle = 1$.)

We can determine the remaining character using the orthogonality relations. Suppose

$$\chi_U = \begin{bmatrix} 3 & a & b & c & d \end{bmatrix}.$$

Then, since the second column is orthogonal to the first, we obtain

$$1 + (-1) + 2a + 3 + (-3) = 0$$

whence $a = 0$. A similar argument with the other columns gives $b = -1,\ c = 0,\ d = 2$. Thus, the character table of S_4 is:

	1	6	8	6	3
	e	$(1\ 2)$	$(1\ 2\ 3)$	$(1\ 2\ 3\ 4)$	$(1\ 2)(3\ 4)$
χ_{triv}	1	1	1	1	1
χ_{sgn}	1	-1	1	-1	1
χ_U	2	0	-1	0	2
$\chi_{\text{std}\otimes\text{sgn}}$	3	-1	0	1	-1
χ_{std}	3	1	0	-1	-1

At this point, we have determined χ_U without describing the representation U. However, the first three entries of χ_U should remind you of the standard representation of S_3. If we let $N = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ then N is a normal subgroup of S_4 with $S_4/N \cong S_3$. Consequently, the composition

$$S_4 \xrightarrow{q} S_4/N \xrightarrow{\rho} GL_2(\mathbb{C})$$

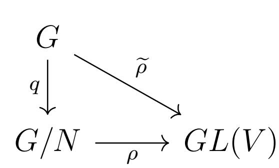
of the quotient map q with the standard representation ρ of S_3 gives a representation of S_4 of degree 2, which turns out to be irreducible (as we will prove in a more general setting below). This representation is the *inflation* of the standard representation from $S_3 = S_4/N$ to S_3.

Exercise 16.2. Show that the size of the conjugacy class of $\pi \in S_n$ is given by

$$\frac{n!}{1^{k_1}k_1!2^{k_2}k_2!\cdots n^{k_n}k_n!},$$

where k_i is the number of i-cycles in the cycle decomposition of π. ▶

Definition 16.3. Suppose $N \trianglelefteq G$ is a normal subgroup of G and let $q\colon G \to G/N$ denote the quotient map. Let (V, ρ) be a representation of G/N. The **inflation** of (V, ρ) to G is the representation $(V, \widetilde{\rho})$ of G given by $\widetilde{\rho} = \rho \circ q$.



Proposition 16.4. Let $N \trianglelefteq G$ be a normal subgroup of G, let (V, ρ) be a representation of G/N and let $(V, \widetilde{\rho})$ be the inflation of V to G. Then:

(a) $N \subseteq \ker \widetilde{\rho}$.

(b) (V, ρ) is irreducible if and only if $(V, \widetilde{\rho})$ is irreducible.

(c) $\chi_{\widetilde{\rho}}(g) = \chi_\rho(gN)$ for all $g \in G$.

(d) The inflation map

$$\begin{aligned} \mathrm{Irr}_{\mathbb{C}}(G/N) &\mapsto \{(W, \sigma) \in \mathrm{Irr}_{\mathbb{C}}(G) \colon N \subseteq \ker \sigma\} \\ (V, \rho) &\mapsto (V, \widetilde{\rho}) \end{aligned}$$

is a bijection.

Proof: Since $\widetilde{\rho}(g) = \rho(gN)$, part (a) follows from the fact that N is the identity element of G/N. For part (b), we prove more generally that a subspace $U \subseteq V$ is G/N-invariant if and only if it is G-invariant. This follows immediately from the definition of $\widetilde{\rho}$:

$$\rho(gN)U \subseteq U \quad \iff \quad \widetilde{\rho}(g)U \subseteq U.$$

Part (c) follows from the definition of $\widetilde{\rho}$. Finally, for part (d), parts (a) and (b) show that the inflation map sends irreducibles to irreducibles with N in their kernel, so the given map is well-defined. To show that it's a bijection, we will describe the inverse map. Given $(W, \sigma) \in \mathrm{Irr}_{\mathbb{C}}(G)$ with $N \subseteq \ker \sigma$, define $\rho \colon G/N \to GL(W)$ by $\rho(gN) = \sigma(g)$. Since $N \subseteq \ker \sigma$, the map ρ is a well-defined homomorphism. By construction, $\widetilde{\rho} = \sigma$. ■

This result confirms that the inflation of the standard representation from $S_3 = S_4/N$ to S_4, as described in Example 16.1, is indeed irreducible. As another example, the trivial and alternating representations are the inflations of the two distinct irreducible representations of $C_2 = S_4/[S_4, S_4]$ to S_4. More generally, Proposition 11.8 shows that all of the one-dimensional representations of G are inflations of one-dimensional representations of $G/[G, G]$.

16.2 Kernels, Normal Subgroups and the Character Table

In the previous section we saw how to use irreducible representations of quotients G/N to construct representations of G. Phrased differently, we can use the character table of G/N to help construct the character table of G. In this section, we go the other way and show how the character table of G can be used to determine all of the normal subgroups of G.

Definition 16.5. The **kernel** of a character χ of G is

$$\ker(\chi) = \{g \in G \colon \chi(g) = \chi(e)\}.$$

The justification for using this name comes from:

Proposition 16.6. Let (V, ρ) be a representation of G with character χ_V. Then:

$$\ker(\chi_V) = \ker(\rho).$$

Proof: If $g \in \ker(\rho)$ then $\rho(g) = \text{id}$ so $\chi_V(g) = \text{tr}(\text{id}) = \dim V = \chi_V(e)$, by Proposition 12.10(c). Conversely, assume $g \in \ker(\chi_V)$. We know that $\chi_V(g) = \text{tr}(\rho(g))$ is the sum of the $n = \dim V$ eigenvalues λ_i of $\rho(g)$:

$$\chi_V(g) = \lambda_1 + \cdots + \lambda_n.$$

Since each λ_i is a $|G|$th root of unity, it follows that

$$n = \chi_V(e) = |\chi_V(g)| \leq \sum_{i=1}^{n} |\lambda_i| = n.$$

Thus, equality holds in the triangle inequality, so the eigenvalues λ_i must be positive multiples of each other hence must be equal (since they are roots of unity). So $\rho(g) = \lambda\,\text{id}$ and, upon taking the trace of both sides, we must in fact have $\lambda = 1$. Thus, $g \in \ker(\rho)$. ∎

In particular, the kernel of any character of G is a normal subgroup.

Example 16.7. Let's adopt the notation g^G for the conjugacy class in G containing g. Referring to the character table of S_4 (Example 16.1), we see that

$$\begin{aligned} \ker(\chi_{\text{triv}}) &= S_4 \\ \ker(\chi_{\text{sgn}}) &= A_4 \\ \ker(\chi_U) &= \{e\} \cup (1\ 2)(3\ 4)^{S_4} \\ \ker(\chi_{\text{std}\otimes\text{sgn}}) &= \{e\} \\ \chi_{\text{std}} &= \{e\}. \end{aligned}$$

In particular, $\ker(\chi_U)$ is what we called N in Example 16.1, which should not too surprising since χ_U was constructed by inflation from S_4/N.

It is a fact that the only normal subgroups of S_4 are the ones determined in the preceding example. This might suggest that, in general, the normal subgroups of G are the kernels of the irreducible characters of G. This is not quite correct.

Proposition 16.8.

(a) Every normal subgroup N of G is the kernel of some character χ of G: $N = \ker \chi$.

(b) Every normal subgroup N of G is the intersection of the kernels of some *irreducible* characters of G: $N = \bigcap_{i=1}^{s} \ker \chi_i$.

Proof: Consider the regular representation ρ of G/N. Since ρ is faithful, we have

$$g \in \ker \widetilde{\rho} \iff gN \in \ker \rho \iff gN = N \iff g \in N.$$

Thus, $\ker \widetilde{\rho} = N$. This proves part (a).

For part (b), let $\chi_1, \ldots, \chi_s$ be all of the irreducible characters of G/N, and let $\widetilde{\chi}_1, \ldots, \widetilde{\chi}_s$ denote the characters of their inflations so that $\widetilde{\chi}_i(g) = \chi_i(gN)$. I claim that $N = \bigcap_{i=1}^s \ker \widetilde{\chi}_i$. Indeed,

$$g \in \ker \widetilde{\chi}_i \iff \widetilde{\chi}_i(g) = \widetilde{\chi}_i(e) \iff \chi_i(gN) = \chi_i(N) \iff gN \in \ker \chi_i.$$

Thus,

$$\begin{aligned} g \in \bigcap_{i=1}^s \ker \widetilde{\chi}_i &\iff gN \in \bigcap_{i=1}^s \ker(\chi_i) \\ &\iff \chi_i(gN) = \chi_i(N) \text{ for all } i \\ &\iff gN \text{ is conjugate to } N \text{ in } G/N \qquad \text{(Problem 14.2(a))} \\ &\iff gN = N \text{ in } G/N \\ &\iff g \in N, \end{aligned}$$

as claimed. ■

Remark 16.9. The above proposition shows that the character table of G can be used to determine the set of normal subgroups of G as well as all inclusions between normal subgroups. Thus, the character table knows if G is:

- Simple.
- Solvable. (We can determine all normal series in G and the orders of all normal subgroups. Now use the fact that a group is solvable if and only if it has a normal series whose successive quotients are p-groups.)

The character table of G can also be used to determine if G is nilpotent, but this requires a bit more work.

Example 16.10. The character table of the group $G = GL_2(\mathbb{F}_3)$ is given below.

	1	1	12	8	6	8	6	6
	C_0	C_1	C_2	C_3	C_4	C_5	C_6	C_7
χ_0	1	1	1	1	1	1	1	1
χ_1	1	1	-1	1	1	1	-1	-1
χ_2	2	2	0	-1	2	-1	0	0
χ_3	2	-2	0	-1	0	1	$-2i$	$2i$
χ_4	2	-2	0	-1	0	1	$2i$	$-2i$
χ_5	3	3	-1	0	-1	0	1	1
χ_6	3	3	1	0	-1	0	-1	-1
χ_7	4	-4	0	1	0	-1	0	0

The only proper, nontrivial normal subgroups of G are

$$\ker \chi_1 = C_0 \cup C_1 \cup C_3 \cup C_4 \cup C_5, \quad \ker \chi_2 = C_0 \cup C_1 \cup C_4 \quad \text{and} \quad \ker \chi_5 = C_0 \cup C_1$$

with orders 24, 8 and 2, resp. This gives the normal series

$$G \trianglerighteq \ker \chi_1 \trianglerighteq \ker \chi_2 \trianglerighteq \ker \chi_5 \trianglerighteq \{e\}$$

where the successive quotients have orders 2, 3, 4 and 2, resp; in particular, the quotients are abelian (and, incidentally, p-groups), so G is solvable.

Lecture 16 Problems

16.1. Determine the character table of A_4.

16.2. Let $\chi_1, \ldots, \chi_h$ be all of the irreducible characters of G. Prove that $\bigcap_{i=1}^{h} \ker \chi_i = \{e\}$.

16.3. Let χ and ψ be characters of G. Prove that $\ker(\chi + \psi) = \ker(\chi) \cap \ker(\psi)$. [As a first step, you should figure out what is meant by $\ker(\chi + \psi)$.]

16.4. Prove that G is simple if and only if $\chi(g) \neq \chi(e)$ for all $g \neq e$ and all irreducible characters $\chi \neq \chi_{\text{triv}}$.

16.5. The character table of a certain group G is given below.

	1	1	2	4	4	2	2
	C_0	C_1	C_2	C_3	C_4	C_5	C_6
χ_0	1	1	1	1	1	1	1
χ_1	1	1	1	1	-1	-1	-1
χ_2	1	1	1	-1	1	-1	-1
χ_3	1	1	1	-1	-1	1	1
χ_4	2	2	-2	0	0	0	0
χ_5	2	-2	0	0	0	$\sqrt{2}$	$-\sqrt{2}$
χ_6	2	-2	0	0	0	$-\sqrt{2}$	$\sqrt{2}$

Describe all of the normal subgroups of G and give their orders. [Hint: There are 7 in total, including G and $\{e\}$.]

Lecture 17 Symmetric and Alternating Powers

17.1 Symmetric Square and Alternating Square

Example 17.1 (Character table of S_5)**.** The symmetric group S_5 has seven conjugacy classes and therefore seven irreps. We know three right off the bat: the trivial, alternating and standard representations. So we have the following partial character table.

	1	10	20	15	30	20	24
	$\{e\}$	(1 2)	(1 2 3)	(1 2)(3 4)	(1 2 3 4)	(1 2 3)(4 5)	(1 2 3 4 5)
χ_{triv}	1	1	1	1	1	1	1
χ_{sgn}	1	-1	1	1	-1	-1	1
χ_{std}	4	2	1	0	0	-1	-1

Another irreducible character immediately jumps out, namely:

$$\chi_{\text{sgn}\otimes\text{std}} = \chi_{\text{sgn}}\chi_{\text{std}} = \begin{bmatrix} 4 & -2 & 1 & 0 & 0 & 1 & -1 \end{bmatrix}.$$

But now what? Well, we can try to tensor the standard representation with itself, giving

$$\chi_{\text{std}\otimes\text{std}} = \chi_{\text{std}}^2 = \begin{bmatrix} 16 & 4 & 1 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

This character, however, is not irreducible since

$$\langle \chi_{\text{std}\otimes\text{std}}, \chi_{\text{std}\otimes\text{std}} \rangle = \frac{1}{120}(16^2 \cdot 1 + 4^2 \cdot 10 + 1^2 \cdot 20 + 1^2 \cdot 20 + 1^2 \cdot 24) = 4 \neq 1.$$

This computation tells us something more. If $\chi_{\text{std}\otimes\text{std}} = \sum a_i \chi_i$, where the χ_i are irreducible characters, then we get

$$4 = \langle \chi_{\text{std}\otimes\text{std}}, \chi_{\text{std}\otimes\text{std}} \rangle = \sum a_i^2.$$

Since $4 = 1^2 + 1^2 + 1^2 + 1^2 = 2^2$ are the only ways of writing 4 as the sum of squares, it follows that $V_{\text{std}} \otimes V_{\text{std}}$ decomposes into the direct sum of either four distinct irreps or one irrep with multiplicity two. We calculate:

$$\begin{aligned}
\langle \chi_{\text{std}\otimes\text{std}}, \chi_{\text{triv}} \rangle &= 1 \\
\langle \chi_{\text{std}\otimes\text{std}}, \chi_{\text{sgn}} \rangle &= 0 \\
\langle \chi_{\text{std}\otimes\text{std}}, \chi_{\text{std}} \rangle &= 1 \\
\langle \chi_{\text{std}\otimes\text{std}}, \chi_{\text{sgn}\otimes\text{std}} \rangle &= 0.
\end{aligned}$$

Thus, each of V_{triv} and V_{std} occur in $V_{\text{std}} \otimes V_{\text{std}}$ with multiplicity one. From this we conclude that

$$V_{\text{std}} \otimes V_{\text{std}} = V_{\text{triv}} \oplus V_{\text{std}} \oplus ? \oplus ??,$$

What are these two mystery representations? We at least know that their dimensions add up to $4^2 - 1 - 4 = 11$.

We now introduce a bit of linear algebra that will, among other things, help complete the character table of S_5.

Let V be a vector space. The tensor square $V^{\otimes 2} := V \otimes V$ decomposes into the direct sum of two subspaces

$$V \otimes V = \mathrm{Sym}^2(V) \oplus \mathrm{Alt}^2(V)$$

consisting of the so-called **symmetric** and **alternating** tensors. This is most cleanly seen as follows. Consider the action of the cyclic group $C_2 = \langle a \rangle$ on $V \otimes V$ via $a(x \otimes y) = y \otimes x$, and let $\mathrm{Sym}^2(V)$ and $\mathrm{Alt}^2(V)$ be the isotypic pieces. More precisely, we define:

$$\begin{aligned} \mathrm{Sym}^2(V) &= \{v \in V^{\otimes 2} \colon av = v\} \\ \mathrm{Alt}^2(V) &= \{v \in V^{\otimes 2} \colon av = -v\}. \end{aligned}$$

Although we are working over $\mathbb{C}$, this construction works for any field of characteristic $\neq 2$.

Proposition 17.2. Suppose $\{v_1, \ldots, v_d\}$ is a basis for V. Then:

(a) $\{v_i \otimes v_j + v_j \otimes v_i \colon 1 \le i \le j \le d\}$ is a basis for $\mathrm{Sym}^2(V)$.

(b) $\{v_i \otimes v_j - v_i \otimes v_j \colon 1 \le i \lneq j \le d\}$ is a basis for $\mathrm{Alt}^2(V)$.

(c) If V is a $\mathbb{C}G$-module, then $\mathrm{Sym}^2(V)$ and $\mathrm{Alt}^2(V)$ are G-invariant subspaces of $V^{\otimes 2}$.

Exercise 17.3. Prove Proposition 17.2. ▶

Corollary 17.4. If $\dim V = d$, then

$$\dim \mathrm{Sym}^2(V) = \binom{d+1}{2} = \frac{d(d+1)}{2} \quad \text{and} \quad \dim \mathrm{Alt}^2(V) = \binom{d}{2} = \frac{d(d-1)}{2}. \qquad \blacksquare$$

It is convenient to use the short-hand notation

$$\begin{aligned} v_i v_j &:= v_i \otimes v_j + v_j \otimes v_i \\ v_i \wedge v_j &:= v_i \otimes v_j - v_j \otimes v_i \end{aligned}$$

for the basis vectors of $\mathrm{Sym}^2(V)$ and $\mathrm{Alt}^2(V)$. Notice that $v_i v_j = v_j v_i$ while $v_i \wedge v_j = -v_j \wedge v_i$.

Proposition 17.5. Let (V, ρ) be a $\mathbb{C}G$-module. Then

$$\chi_V(g)^2 = \chi_{\mathrm{Sym}^2(V)}(g) + \chi_{\mathrm{Alt}^2(V)}(g),$$

where

$$\chi_{\mathrm{Sym}^2(V)}(g) = \frac{1}{2}(\chi_V(g)^2 + \chi_V(g^2)) \quad \text{and} \quad \chi_{\mathrm{Alt}^2(V)}(g) = \frac{1}{2}(\chi_V(g)^2 - \chi_V(g^2)).$$

Proof: The first assertion follows from the decomposition $V^{\otimes 2} = \mathrm{Sym}^2(V) \oplus \mathrm{Alt}^2(V)$ and the fact that $\chi_{V\otimes V} = \chi_V \chi_V$.

Let's determine $\chi_{\mathrm{Alt}^2(V)}$. Let $g \in G$ and choose a basis $\mathcal{B} = \{v_1, \ldots, v_n\}$ in which $[\rho(g)]_{\mathcal{B}}$ is diagonal, say $[\rho(g)]_{\mathcal{B}} = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$. Then

$$\chi_V(g) = \sum_{i=1}^{n} \lambda_i.$$

Consider now the basis $\mathcal{C} = \{v_i \wedge v_j\}_{i<j}$ of $\mathrm{Alt}^2(V)$. Note that

$$g(v_i \wedge v_j) = gv_i \otimes gv_j - gv_j \otimes gv_i = \lambda_i v_i \otimes \lambda_j v_j - \lambda_j v_j \otimes \lambda_i v_i = \lambda_i \lambda_j (v_i \wedge v_j).$$

Thus, the $\mathcal{C}$-matrix of g acting on $\mathrm{Alt}^2(V)$ is diagonal with diagonal entries $\lambda_i \lambda_j$. So

$$\begin{aligned}
\chi_{\mathrm{Alt}^2(V)}(g) &= \sum_{i<j} \lambda_i \lambda_j \\
&= \frac{1}{2}\left(\left(\sum_i \lambda_i\right)^2 - \sum_i \lambda_i^2\right) \\
&= \frac{1}{2}(\chi_V(g)^2 - \chi_V(g^2)),
\end{aligned}$$

as claimed. The expression for $\chi_{\mathrm{Sym}^2(V)}$ then follows from

$$\chi_{\mathrm{Sym}^2(V)} = \chi_{V\otimes V} - \chi_{\mathrm{Alt}^2(V)} = \chi_V^2 - \chi_{\mathrm{Alt}^2(V)}.$$ ■

Example 17.6 (Character table of S_5)**.** We can now complete what we had begun in Example 17.1. Let $S = \mathrm{Sym}^2(V_{\mathrm{std}})$ and $A = \mathrm{Alt}^2(V_{\mathrm{std}})$. Using Proposition 17.5, we compute

$$\begin{aligned}
\chi_S &= \begin{bmatrix} 10 & 4 & 1 & 2 & 0 & 1 & 0 \end{bmatrix} \\
\chi_A &= \begin{bmatrix} 6 & 0 & 0 & -2 & 0 & 0 & 1 \end{bmatrix}.
\end{aligned}$$

Recall that we are missing an 11-dimensional piece in the isotypic decomposition of $V_{\mathrm{std}}^{\otimes 2}$. So S is not irreducible since it is 10-dimensional and we have already accounted for all one-dimensional irreps in $V_{\mathrm{std}}^{\otimes 2}$. Alternatively, we can compute directly that

$$\langle \chi_S, \chi_S \rangle = 3.$$

Since $3 = 1^2 + 1^2 + 1^2$ is the only way to write 3 as a sum of squares, it follows that χ_S is the sum of three distinct irreducible characters. A quick computation shows that $\langle \chi_S, \chi_{\mathrm{triv}} \rangle = 1$ and $\langle \chi_S, \chi_{\mathrm{std}} \rangle = 1$. Thus,

$$\chi_? := \chi_S - \chi_{\mathrm{triv}} - \chi_{\mathrm{std}} = \begin{bmatrix} 5 & 1 & -1 & 1 & -1 & 1 & 0 \end{bmatrix}$$

must be an irreducible character (as we can confirm by calculating $\langle \chi_?, \chi_? \rangle = 1$). Note that tensoring $\chi_?$ with the alternating rep gives another irreducible character:

$$\chi_{?\otimes \text{sgn}} = \begin{bmatrix} 5 & -1 & -1 & 1 & 1 & -1 & 0 \end{bmatrix}.$$

So all that's left is a 6-dimensional irrep. Conveniently, χ_A has degree 6. We now calculate $\langle \chi_A, \chi_A \rangle = 1$, which shows that χ_A is irreducible. Our character table is now complete.

	1	10	20	15	30	20	24
	$\{e\}$	(1 2)	(1 2 3)	(1 2)(3 4)	(1 2 3 4)	(1 2 3)(4 5)	(1 2 3 4 5)
χ_{triv}	1	1	1	1	1	1	1
χ_{sgn}	1	-1	1	1	-1	-1	1
χ_{std}	4	2	1	0	0	-1	-1
$\chi_{\text{std}\otimes\text{sgn}}$	4	-2	1	0	0	1	-1
$\chi_?$	5	1	-1	1	-1	1	0
$\chi_{?\otimes\text{sgn}}$	5	-1	-1	1	1	-1	0
χ_A	6	0	0	-2	0	0	1

Remark 17.7. There remains the issue of constructing the representation whose character is $\chi_?$. One approach is given in Problem 17.2. Next lecture will contain a discussion of the problem of constructing the irreducible representations of S_n.

17.2 Higher Symmetric and Alternating Powers

I want to close this lecture by briefly indicating how to generalize the decomposition

$$V^{\otimes 2} = \text{Sym}^2(V) \oplus \text{Alt}^2(V)$$

to the n-fold tensor power

$$V^{\otimes n} := V \otimes \cdots \otimes V.$$

We can analogously define symmetric and alternating tensors, but for $n \geq 3$ we will have

$$V^{\otimes n} = \text{Sym}^n(V) \oplus \text{Alt}^n(V) \oplus \text{some other stuff}.$$

The setup is as follows. Let S_n act on $V^{\otimes n}$ by

$$\pi \cdot (v_1 \otimes \cdots \otimes v_n) = v_{\pi^{-1}(1)} \otimes \cdots \otimes v_{\pi^{-1}(n)}$$

and extending linearly. Note that if $n = 2$ then $S_2 = C_2$ and this reduces to what we had from earlier. Consider now the isotypic decomposition of $V^{\otimes n}$ under this action. We have:

$$V^{\otimes n} = \bigoplus_{\lambda} U_\lambda,$$

where the sum is indexed by the set of irreducible representations of S_n and U_λ is the λ-isotypic piece of $V^{\otimes n}$. We let $\text{Sym}^n(V)$ and $\text{Alt}^n(V)$ be the isotypic pieces indexed by $\lambda = \text{triv}$

and $\lambda = \operatorname{sgn}$, respectively. That is,

$$\begin{aligned}\operatorname{Sym}^n(V) &= \{x \in V^{\otimes n} : \pi \cdot x = x \text{ for all } \pi \in S_n\} \\ \operatorname{Alt}^n(V) &= \{x \in V^{\otimes n} : \pi \cdot x = \operatorname{sgn}(\pi)x \text{ for all } \pi \in S_n\}.\end{aligned}$$

We obtain, as before, the following concrete descriptions.

Proposition 17.8. Suppose $\{v_1, \ldots, v_d\}$ is a basis for V. Then:

(a) $\left\{ \sum_{\pi \in S_n} v_{i_{\pi(1)}} \otimes v_{i_{\pi(n)}} : 1 \leq i_1 \leq \cdots \leq i_n \leq d \right\}$ is a basis for $\operatorname{Sym}^n(V)$.

(b) $\left\{ \sum_{\pi \in S_n} \operatorname{sgn}(\pi) v_{i_{\pi(1)}} \otimes v_{i_{\pi(n)}} : 1 \leq i_1 \lneq \cdots \lneq i_n \leq d \right\}$ is a basis for $\operatorname{Alt}^n(V)$.

(c) If V is a $\mathbb{C}G$-module, $\operatorname{Sym}^n(V)$ and $\operatorname{Alt}^n(V)$ are G-invariant subspaces of $V^{\otimes n}$. ■

Corollary 17.9. If $\dim V = d$, then

$$\dim \operatorname{Sym}^n(V) = \binom{d+n-1}{n-1} \quad \text{and} \quad \dim \operatorname{Alt}^2(V) = \binom{d}{n}.$$

In particular, $\operatorname{Alt}^n(V) = 0$ if $n > d$. ■

There is also an analogue of Proposition 17.5. Here is the case $n = 3$.

Proposition 17.10. Let V be a $\mathbb{C}G$-module. Then:

(a) $\chi_{\operatorname{Sym}^3(V)}(g) = \frac{1}{6}(\chi_V(g)^3 + 3\chi_V(g)\chi_V(g^2) + 2\chi_V(g^3))$.

(b) $\chi_{\operatorname{Alt}^3(V)}(g) = \frac{1}{6}(\chi_V(g)^3 - 3\chi_V(g)\chi_V(g^2) + 2\chi_V(g^3))$. ■

For $\lambda \notin \{\operatorname{triv}, \operatorname{sgn}\}$, the λ-isotypic pieces of $V^{\otimes n}$ are not as easy to describe. They are best understood by bringing the representation theory of $GL(V)$ into the picture. Alas, to get into this will take us too far afield (look up *Schur–Weyl duality* if you are curious). Here is a very brief summary. Suppose $\operatorname{Irr}_{\mathbb{C}}(S_n) = \{V_\lambda\}_\lambda$. Then to each index λ there corresponds an irreducible representation of $GL(V)$ denoted by $\mathbb{S}_\lambda(V)$. In the case where $\lambda = \operatorname{triv}$ (resp. sgn), $\mathbb{S}_\lambda(V) = \operatorname{Sym}^n(V)$ (resp. $\operatorname{Alt}^n(V)$). In general, we have

$$V^{\otimes n} = \bigoplus_\lambda (\mathbb{S}_\lambda(V))^{\oplus d_\lambda},$$

where $d_\lambda = \dim V_\lambda$. For example,

$$\begin{aligned}V^{\otimes 3} &= \mathbb{S}_{\operatorname{triv}}(V) \oplus \mathbb{S}_{\operatorname{sgn}}(V) \oplus (\mathbb{S}_{\operatorname{std}}(V))^{\oplus 2} \\ &= \operatorname{Sym}^3(V) \oplus \operatorname{Alt}^3(V) \oplus (\mathbb{S}_{\operatorname{std}}(V))^{\oplus 2}.\end{aligned}$$

Of course, I haven't told you what $\mathbb{S}_{\text{std}}(V)$ is, but suffice it to say that if V is a $\mathbb{C}G$-module, then $\mathbb{S}_{\text{std}}(V)$ is G-invariant, and we can determine its character from Proposition 17.10 as

$$\chi(g) = \frac{1}{3}(\chi_V(g)^3 - \chi_V(g^3)).$$

So these modules $\mathbb{S}_\lambda(V)$ and their characters allow us to construct novel representations and characters from known ones. A reference for this material is Fulton, *Young Tableaux* (LMS 35), Chapters 7 and 8.

Remark 17.11 (Sym^n and Alt^n as quotients)**.** In the above, I defined $\text{Sym}^n(V)$ and $\text{Alt}^n(V)$ as subspaces of $V^{\otimes n}$. Arguably, however, the "correct" thing to do is to define them as quotients of $V^{\otimes n}$, as follows.

The nth symmetric power $S^n(V)$ of V is the quotient of $V^{\otimes n}$ by the subspace generated by all vectors of the form

$$v_1 \otimes v_2 \otimes \cdots \otimes v_n - v_{\pi(1)} \otimes v_{\pi(2)} \otimes \cdots \otimes v_{\pi(n)} \text{ where } v_i \in V \text{ and } \pi \in S_n.$$

The image of $v_1 \otimes v_2 \cdots \otimes v_n$ in the quotient is denoted by $v_1 v_2 \cdots v_n$, and we have

$$v_1 v_2 \cdots v_n = v_{\pi(1)} v_{\pi(2)} \cdots v_{\pi(n)} \quad \text{for all } \pi \in S_n.$$

That is, the v_i "commute" with each other in $S^n(V)$. If G acts on V then the induced action on $V^{\otimes n}$ descends to an action on $S^n(V)$ that is given by

$$g(v_1 v_2 \cdots v_n) = (gv_1)(gv_2) \cdots (gv_n).$$

Similarly, the nth alternating power $A^n(V)$ of V is the quotient of $V^{\otimes n}$ by the subspace generated by all vectors of the form

$$v_1 \otimes v_2 \otimes \cdots \otimes v_n - \text{sgn}(\pi) v_{\pi(1)} \otimes \cdots \otimes v_{\pi(2)} \otimes \cdots \otimes v_{\pi(n)} \text{ where } v_i \in V \text{ and } \pi \in S_n.$$

(Actually, the above definition is useless in characteristic 2, so we should instead mod out by the subspace generated by $v_1 \otimes \cdots \otimes v_n$ with $v_i = v_{i+1}$ for some i. In characteristic zero this is the same as the above subspace.) The image of $v_1 \otimes v_2 \cdots \otimes v_n$ in the quotient is denoted by the so-called wedge product $v_1 \wedge v_2 \wedge \cdots \wedge v_n$, and we have

$$v_1 \wedge v_2 \wedge \cdots \wedge v_n = \text{sgn}(\pi) v_{\pi(1)} \wedge v_{\pi(2)} \wedge \cdots v_{\pi(n)} \quad \text{for all } \pi \in S_n.$$

If G acts on V then it acts on $A^n(V)$ by

$$g(v_1 \wedge \cdots \wedge v_n) = (gv_1) \wedge \cdots \wedge (gv_n).$$

In characteristic 0, there are canonical injections $\iota_S \colon S^n(V) \hookrightarrow V^{\otimes n}$ and $\iota_A \colon A^n(V) \hookrightarrow V^{\otimes n}$ defined by

$$\iota_S(v_1 \cdots v_n) = \sum_{\pi \in S_n} v_{\pi(1)} \otimes \cdots \otimes v_{\pi(n)}$$
$$\iota_A(v_1 \wedge \cdots \wedge v_n) = \sum_{\pi \in S_n} \operatorname{sgn}(\pi) v_{\pi(1)} \otimes \cdots \otimes v_{\pi(n)}.$$

The images of ι_A and ι_S are $\operatorname{Sym}^n(V)$ and $\operatorname{Alt}^n(V)$. Thus, we have canonical isomorphisms $S^n(V) \cong \operatorname{Sym}^n(V)$ and $A^n(V) \cong \operatorname{Alt}^n(V)$ (even as G-modules since ι_S and ι_A are G-linear). So the quotient-space definitions of the symmetric and exterior powers are equivalent to the subspace definitions.

One reason for choosing to work with the quotient-space definitions is that we get universal properties for $S^n(V)$ and $A^n(V)$ in terms of symmetric (resp. alternating) multilinear maps on V^n (just like $V^{\otimes 2}$ has a universal property in terms of bilinear maps on V^2); they also provide the convenient symmetric and exterior products $v_1 \cdots v_n$ and $v_1 \wedge \cdots \wedge v_n$ of vectors which can be useful in computations and other constructions (e.g. if $T \colon V \to W$ is a linear map, we can define $A^n(T) \colon A^n(V) \to A^n(W)$ by $A^n(T)(v_1 \wedge \cdots \wedge v_n) = Tv_1 \wedge \cdots \wedge Tv_n$, so we see that $V \rightsquigarrow A^n(V)$ is a functor; ditto for $V \rightsquigarrow S^n(V)$).

Lecture 17 Problems

17.1. (a) Determine the character table of A_5.

(b) Deduce that A_5 is simple.

17.2. This problem gives a construction of the 5-dimensional irreducible representation of S_5.

(a) Let X be the set of Sylow 5-subgroups of S_5. Show that $|X| = 6$.

(b) Show that the action of S_5 on X by conjugation is 2-transitive.

(c) Let V be the permutation representation induced by the action of S_5 on X by conjugation. Deduce from part (b) that $V = V_{\text{triv}} \oplus U$ where U is a 5-dimensional irreducible representation of S_5.

17.3. (a) Let V be the standard representation of S_3. Determine the isotypic decompositions of $\operatorname{Sym}^2(V)$ and $\operatorname{Alt}^2(V)$.

(b) Same problem but for S_4.

17.4. The **Frobenius–Schur indicator** of a character χ is the number

$$\varepsilon(\chi) = \frac{1}{|G|} \sum_{g \in G} \chi(g^2).$$

Assume V is irreducible and let $\chi = \chi_V$.

(a) Prove $\operatorname{mult}(V_{\text{triv}}, V \otimes V)$ is either 1 or 0 depending on whether $V \cong V^*$ or not.

(b) Express $\varepsilon(\chi)$ in terms of the characters of $\mathrm{Sym}^2(V)$ and $V \otimes V$.

(c) Hence show that

$$\varepsilon(\chi) = \begin{cases} \pm 1 & \text{if and only if } \chi_V \text{ is real valued} \\ 0 & \text{otherwise.} \end{cases}$$

[Note: $\varepsilon(\chi_V)$ is c_V from Problem 8.4. See the next problem.]

17.5. Let V be a $\mathbb{C}$-vector space.

(a) Show that the space of bilinear forms on V can be identified with $(V \otimes V)^* \cong V^* \otimes V^* \cong \mathrm{Sym}^2(V^*) \oplus \mathrm{Alt}^2(V^*)$.

(b) Show that if V is a $\mathbb{C}G$-module then the space of G-invariant bilinear forms on V can be identified with $(V^* \otimes V^*)^G \cong \mathrm{Sym}^2(V^*)^G \oplus \mathrm{Alt}^2(V^*)^G$.

(c) Assume V is an irreducible $\mathbb{C}G$-module.

(i) Show that if there exists a non-zero G-invariant bilinear form B on V then it must belong to either $\mathrm{Sym}^2(V^*)^G$ (in which case it is a symmetric form, i.e. $B(x,y) = B(y,x)$) or else it must belong to $\mathrm{Alt}^2(V^*)^G$ (in which case it is a skew-symmetric form, i.e. $B(x,y) = -B(y,x)$).

[Hint: What is $\dim (V^* \otimes V^*)^G$?]

(ii) Give a new solution to Problem 8.4(c) and deduce that c_V is the Frobenius–Schur indicator of χ_V. Hence conclude that

$$\varepsilon(\chi_V) = \begin{cases} 1 & \text{if } V \text{ has a nonzero symmetric } G\text{-invariant bilinear form} \\ -1 & \text{if } V \text{ has a nonzero skew-symmetric } G\text{-invariant bilinear form} \\ 0 & \text{if } V \text{ has no nonzero } G\text{-invariant bilinear forms.} \end{cases}$$

17.6. (a) Let (V, ρ) be a $\mathbb{C}G$-module and suppose $d = \dim V$. Show that the action of G on $\mathrm{Alt}^d(V) \subseteq V^{\otimes n}$ is given by $g \cdot x = \det(\rho(g))x$. [Note: $\dim \mathrm{Alt}^d(V) = 1$.]

(b) Let V be the standard representation of S_n. Show that $\mathrm{Alt}^{n-1}(V)$ is isomorphic to the alternating representation.

Lecture 18 The Representation Theory of S_n

The main goal of this lecture and the next is to describe how to construct all of the irreducible representations of S_n (over $\mathbb{C}$). The material here is quite rich and can take up a full course on its own. As such, some results will be given without proof. Two general references are James, *The Representation Theory of the Symmetric Group* (LNM 682) and Fulton, *Young Tableaux* (LMS 35).

18.1 Young Diagrams

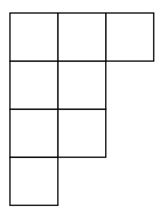
We have bijections

$$\mathrm{Irr}_{\mathbb{C}}(S_n) \longleftrightarrow \{\text{conjugacy classes in } S_n\} \longleftrightarrow \{\text{partitions of } n\}.$$

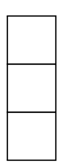
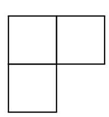
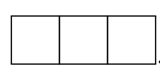
For instance, the conjugacy class in S_5 of a permutation whose cycle decomposition consists of one 2-cycle and three 1-cycles corresponds to the partition $5 = 2 + 1 + 1 + 1$. We will record partitions of n as tuples $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k)$ where $n = \lambda_1 + \lambda_2 + \cdots + \lambda_k$ and $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_k > 0$. We will write $\lambda \vdash n$ to indicate that λ is a partition of n.

> **Goal.** Construct an irreducible representation $V_\lambda \in \mathrm{Irr}_{\mathbb{C}}(S_n)$ for each $\lambda \vdash n$.

We can display a partition $\lambda = (\lambda_1, \ldots, \lambda_k)$ of n diagrammatically by means of a **Young diagram**, which is a left-justified stack of n boxes consisting of λ_i boxes in the ith row. For example, the Young diagram of $\lambda = (3, 2, 2, 1)$ is:



We will identify each partition $\lambda \vdash n$ with its Young diagram.

> **Example 18.1.** The conjugacy classes of S_3, which have representatives $e = (1)(2)(3)$, $(1\ 2)(3)$ and $(1\ 2\ 3)$, correspond to the Young diagrams
>
> ,  and .
>
> We will see later that our general construction gives
>
> $$V_{\square\square\square} = V_{\mathrm{triv}}, \quad V_{\substack{\square\\\square\\\square}} = V_{\mathrm{sgn}} \quad \text{and} \quad V_{\substack{\square\square\\\square}} = V_{\mathrm{std}}.$$

Likewise, the conjugacy classes of S_4 correspond to the Young diagrams

$$\ydiagram{4}\,, \quad \ydiagram{1,1,1,1}\,, \quad \ydiagram{3,1}\,, \quad \ydiagram{2,1,1} \quad \text{and} \quad \ydiagram{2,2}$$

and it will turn out that

$$V_{\ydiagram{4}} = V_{\text{triv}}, \quad V_{\ydiagram{1,1,1,1}} = V_{\text{sgn}}, \quad V_{\ydiagram{3,1}} = V_{\text{std}} \quad \text{and} \quad V_{\ydiagram{2,1,1}} = V_{\text{std}} \otimes V_{\text{sgn}}$$

while $V_{\ydiagram{2,2}}$ is the inflation to S_4 of the standard representation of S_3. (See Example 16.1.)

18.2 Statement of Results

The following definition is crucial to all that will follow.

Definition 18.2. Let $\lambda \vdash n$. A **Young tableau T of shape λ** (or **λ-tableau**) is a filling of the Young diagram of λ with the integers $1, 2, \ldots, n$ without repetition. The set of all λ-tableaux will be denoted by $\mathrm{YT}(\lambda)$.

Example 18.3. If $\lambda = (2, 1)$, we have

$$\mathrm{YT}(\lambda) = \left\{ \ytableaushort{12,3}\,, \ytableaushort{21,3}\,, \ytableaushort{13,2}\,, \ytableaushort{31,2}\,, \ytableaushort{23,1}\,, \ytableaushort{32,1} \right\}.$$

Definition 18.4. A **standard** Young tableau is one whose entries are strictly increasing across each row (from left to right) and across each column (from top to bottom). The set of standard λ-tableaux will be denoted by $\mathrm{SYT}(\lambda)$.

Example 18.5. If $\lambda = (2, 1)$, we have

$$\mathrm{SYT}(\lambda) = \left\{ \ytableaushort{12,3}\,, \ytableaushort{13,2} \right\}.$$

Note that if $\lambda \vdash n$, then $|\mathrm{YT}(\lambda)| = n!$ while $|\mathrm{SYT}(\lambda)|$ is considerably smaller in general.

Exercise 18.6. Let $\lambda = (3, 2)$. Show that $|\mathrm{SYT}(\lambda)| = 5$ by finding all of the standard λ-tableaux. ▶

We are now able to define the underlying vector space for our desired $V_\lambda \in \mathrm{Irr}_{\mathbb{C}}(S_n)$: it is the free $\mathbb{C}$-vector space on $\mathrm{SYT}(\lambda)$. That is,

$$V_\lambda := \mathbb{C}\langle \mathrm{SYT}(\lambda) \rangle.$$

So an element of V_λ is a formal linear combination of standard λ-tableaux with complex coefficients. What remains is to define an S_n-action that turns V_λ into an irreducible $\mathbb{C}S_n$-module. *It is not at all obvious how to do this.*

Theorem 18.7. Let $\lambda \vdash n$. It is possible to define linear action of S_n on V_λ so that:

(a) V_λ becomes an irreducible $\mathbb{C}S_n$-module.

(b) For $\lambda \neq \lambda'$, $V_\lambda \ncong V_{\lambda'}$ as $\mathbb{C}S_n$-modules.

I will explain how this works next time. For now, here is an example.

Example 18.8. Let $\lambda = (2, 1)$. Then

$$V_\lambda = \left\{ a \begin{array}{|c|c|}\hline 1 & 2 \\ \hline 3 & \multicolumn{1}{c}{} \\ \cline{1-1}\end{array} + b \begin{array}{|c|c|}\hline 1 & 3 \\ \hline 2 & \multicolumn{1}{c}{} \\ \cline{1-1}\end{array} : a, b \in \mathbb{C} \right\}.$$

The recipe for the S_n-action, which we will see later, gives:

$$(1\ 2) \cdot \begin{array}{|c|c|}\hline 1 & 2 \\ \hline 3 & \multicolumn{1}{c}{} \\ \cline{1-1}\end{array} = \begin{array}{|c|c|}\hline 1 & 2 \\ \hline 3 & \multicolumn{1}{c}{} \\ \cline{1-1}\end{array} - \begin{array}{|c|c|}\hline 1 & 3 \\ \hline 2 & \multicolumn{1}{c}{} \\ \cline{1-1}\end{array}$$

$$(1\ 2) \cdot \begin{array}{|c|c|}\hline 1 & 3 \\ \hline 2 & \multicolumn{1}{c}{} \\ \cline{1-1}\end{array} = -\begin{array}{|c|c|}\hline 1 & 3 \\ \hline 2 & \multicolumn{1}{c}{} \\ \cline{1-1}\end{array}$$

$$(1\ 2\ 3) \cdot \begin{array}{|c|c|}\hline 1 & 2 \\ \hline 3 & \multicolumn{1}{c}{} \\ \cline{1-1}\end{array} = -\begin{array}{|c|c|}\hline 1 & 3 \\ \hline 2 & \multicolumn{1}{c}{} \\ \cline{1-1}\end{array}$$

$$(1\ 2\ 3) \cdot \begin{array}{|c|c|}\hline 1 & 3 \\ \hline 2 & \multicolumn{1}{c}{} \\ \cline{1-1}\end{array} = \begin{array}{|c|c|}\hline 1 & 2 \\ \hline 3 & \multicolumn{1}{c}{} \\ \cline{1-1}\end{array} - \begin{array}{|c|c|}\hline 1 & 3 \\ \hline 2 & \multicolumn{1}{c}{} \\ \cline{1-1}\end{array}.$$

Thus, the matrices for $\sigma = (1\ 2)$ and $\tau = (1\ 2\ 3)$ in the basis $\mathcal{B} = \mathrm{SYT}(\lambda)$ are given by

$$[\sigma]_{\mathcal{B}} = \begin{bmatrix} 1 & 0 \\ -1 & -1 \end{bmatrix} \quad \text{and} \quad [\tau]_{\mathcal{B}} = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}.$$

You can now check (e.g., by calculating χ_{V_λ}) that $V_\lambda \cong V_{\mathrm{std}}$, as claimed in Example 18.1.

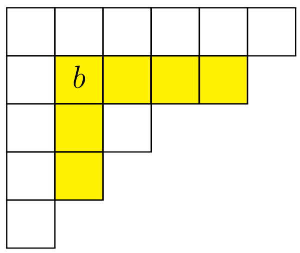
Next, I want to state (without proof) two complementary results. The first concerns the dimension of V_λ, which by construction is equal to the number of standard λ-tableaux.

Theorem 18.9 (Hook Length Formula)**.** For $\lambda \vdash n$,

$$\dim V_\lambda = \frac{n!}{\prod_b h_b},$$

where the denominator is the product of the hook lengths of all boxes b in λ (see below).

The **hook length** of a box b in λ is the number of boxes at and to the right of b plus the number of boxes strictly below b. The diagram on the left highlights the hook at the box b whose hook length is 6. In the diagram on the right, the number in each box is the hook length of that box.



10	8	6	4	3	1
8	6	4	2	1	
5	3	1			
3	1				
1					

Example 18.10. The hook lengths of the boxes in $\lambda = (3, 2)$ are given below.

4	3	1
2	1	

Thus, the Hook Length Formula gives

$$\dim V_{(3,2)} = \frac{5!}{4 \cdot 3 \cdot 1 \cdot 2 \cdot 1} = 5.$$

This confirms the earlier result (Exercise 18.3) that $|\mathrm{SYT}(3, 2)| = 5$.

Next, we turn our attention to the the character χ_λ of V_λ.

Theorem 18.11 (Frobenius Character Formula)**.** Let $\lambda = (\lambda_1, \ldots, \lambda_k)$ and let C be the conjugacy class in S_n of permutations whose cycle decomposition consists of i_j j-cycles for $1 \leq j \leq n$. Let $l = (l_1, \ldots, l_k)$, where $l_i = \lambda_i + k - i$. Then $\chi_\lambda(C)$ is equal to the coefficient of $x_1^{l_1} \cdots x_k^{l_k}$ in

$$\prod_{1 \leq i < j \leq k} (x_i - x_j) \cdot \prod_{j=1}^{n} (x_1^j + \cdots + x_k^j)^{i_j}.$$

Example 18.12. Let's determine χ_λ where $\lambda = (2, 1)$. By Example 18.8, this is the character of the standard representation of S_3, so we know what to expect.

First note that $l = (2 + 2 - 1, 1 + 2 - 2) = (3, 1)$. Now let C be the conjugacy class of $e = (1)(2)(3)$ so that $i_1 = 3$ and $i_2 = i_3 = 0$. Then $\chi_\lambda(C)$ is the coefficient of $x_1^3 x_2$ in

$$\begin{aligned}(x_1 - x_2)(x_1 + x_2)^3 &= (x_1 - x_2)(x_1^3 + 3x_1^2 x_2 + 3x_1 x_2^2 + x_2^3) \\ &= \cdots 3x_1^3 x_2 - x_1^3 x_2 + \cdots \\ &= \cdots + 2x_1^3 x_2 + \cdots .\end{aligned}$$

Thus, $\chi_\lambda(C) = 2$.

Next, let C be the conjugacy class of $(1\ 2)$ so that $i_1 = i_2 = 1$ and $i_3 = 0$. Then $\chi_\lambda(C)$ is the coefficient of $x_1^3 x_2$ in

$$(x_1 - x_2)(x_1 + x_2)(x_1^2 + x_2^2) = (x_1^2 - x_2^2)(x_1^2 + x_2^2)$$

which is clearly 0.

It remains to calculate $\chi_\lambda(1\ 2\ 3)$, which should be 1. I will leave this for you as an exercise.

The Frobenius formula seems rather unwieldy. However, when wielded properly, it can lead to interesting results (such as a proof of the Hook Length Formula).

18.3 Towards the Construction of V_λ

We will arrive at V_λ in a roundabout way. We will first define, for each $\lambda \vdash n$, a $\mathbb{C}S_n$-module M_λ that is generally *not* irreducible. Our V_λ will be isomorphic to a submodule $S_\lambda \subseteq M_\lambda$. The definition of M_λ requires some set-up.

First, note that S_n acts on $\mathrm{YT}(\lambda)$ by permuting entries. For instance,

$$(1\ 3\ 5) \cdot \begin{array}{|c|c|c|}\hline 1 & 2 & 3 \\ \hline 4 & 5 & \\ \cline{1-2}\end{array} = \begin{array}{|c|c|c|}\hline 3 & 2 & 5 \\ \hline 4 & 1 & \\ \cline{1-2}\end{array}.$$

We single out two special types of permutation with respect to this action.

Definition 18.13. For $\lambda \vdash n$ and $T \in \mathrm{YT}(\lambda)$, the **row subgroup** $R(T)$ is the subgroup of S_n consisting of permutations that permute the entries within each row of T among themselves. Likewise, the **column subgroup** $C(T)$ is the subgroup of S_n consisting of permutations that permute the entries within each column.

For example, if

$$T = \begin{array}{|c|c|c|}\hline 1 & 2 & 3 \\ \hline 4 & 5 & \\ \cline{1-2}\end{array}$$

then

$$R(T) = S_{\{1,2,3\}} \times S_{\{4,5\}} \quad \text{and} \quad C(T) = S_{\{1,4\}} \times S_{\{2,5\}} \times S_{\{3\}}.$$

To be more explicit, we have

$$\begin{aligned}R(T) = \{&e, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2), (4\ 5), (1\ 2)(4\ 5),\\ &(1\ 3)(4\ 5), (2\ 3)(4\ 5), (1\ 2\ 3)(4\ 5), (1\ 3\ 2)(4\ 5)\},\\ C(T) = \{&e, (1\ 4), (2\ 5), (1\ 4)(2\ 5)\}.\end{aligned}$$

Definition 18.14. We say $T, T' \in \mathrm{YT}(\lambda)$ are **row equivalent**, and we write $T \sim T'$, if $T = \sigma \cdot T'$ for some $\sigma \in R(T)$. That is, $T \sim T'$ if and only if T and T' have the same entries, up to permutation, in each row.

The row equivalence class of T will be denoted by $\{T\}$ and will be represented by the tableau of T with the vertical lines removed. A row equivalence class of λ-tableaux is called a **λ-tabloid**. The set of all λ-tabloids will be denoted by $\mathrm{YTD}(\lambda)$.

For example,

$$T = \begin{array}{|c|c|c|}\hline 1 & 2 & 3\\ \hline 4 & 5 \\ \cline{1-2}\end{array} \sim \begin{array}{|c|c|c|}\hline 2 & 1 & 3\\ \hline 4 & 5 \\ \cline{1-2}\end{array} \not\sim \begin{array}{|c|c|c|}\hline 4 & 2 & 3\\ \hline 1 & 5 \\ \cline{1-2}\end{array}.$$

The row equivalence class of T is the tabloid

$$\begin{aligned}\{T\} &= \begin{array}{ccc}\hline 1 & 2 & 3\\ \hline 4 & 5 \\ \cline{1-2}\end{array}\\ &= \left\{\begin{array}{|c|c|c|}\hline 1 & 2 & 3\\ \hline 4 & 5 \\ \cline{1-2}\end{array}, \begin{array}{|c|c|c|}\hline 2 & 1 & 3\\ \hline 4 & 5 \\ \cline{1-2}\end{array}, \dots\right\}.\end{aligned}$$

It's easy to check that

$$T \sim T' \implies \sigma \cdot T \sim \sigma \cdot T' \text{ for all } \sigma \in S_n.$$

Thus, we can define an S_n-action on $\mathrm{YTD}(\lambda)$ by $\sigma \cdot \{T\} = \{\sigma \cdot T\}$. The above shows that this is well-defined.

We are finally ready to define M_λ.

Definition 18.15. Let $\lambda \vdash n$. The **Young module** M_λ corresponding to λ is the permutation representation induced by the action of S_n on $\mathrm{YTD}(\lambda)$.

That is, M_λ is the free vector space $\mathbb{C}\langle \mathrm{YTD}(\lambda)\rangle$ on $\mathrm{YTD}(\lambda)$ and the S_n-action is given by

$$\sigma \cdot \left(\sum_i a_i \{T_i\}\right) = \sum_i a_i \{\sigma \cdot T_i\}.$$

We will look at examples next time. For now, I will leave you with the following exercise.

Exercise 18.16. Show that if $\lambda = (n)$ then the Young module M_λ is the trivial representation of S_n. ▶

Lecture 18 Problems

18.1. Let $n = 4$. Determine $\mathrm{SYT}(\lambda)$ for each $\lambda \vdash n$.

18.2. Let $T, T' \in \mathrm{YT}(\lambda)$. Prove:

(a) $T \sim T' \implies \sigma \cdot T \sim \sigma \cdot T'$ for all $\sigma \in S_n$.

(b) $R(T) \cap C(T) = \{e\}$.

(c) $R(\sigma \cdot T) = \sigma R(T) \sigma^{-1}$ and $C(\sigma \cdot T) = \sigma C(T) \sigma^{-1}$ for all $\sigma \in S_n$.

18.3. For $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k) \vdash n$, define $\lambda! := \lambda_1!\lambda_2! \cdots \lambda_k!$. Show that $|\mathrm{YT}(\lambda)| = n!/\lambda!$. [Note that $\dim M_\lambda = |YT(\lambda)|$.]

18.4. Determine the dimension of $V_{(n-1,1)} \in \mathrm{Irr}_{\mathbb{C}}(S_n)$ by using:

(a) The Hook Length formula.

(b) The Frobenius character formula.

Lecture 19 Specht Modules

Let $\lambda \vdash n$. Last time we defined the Young module M_λ to be the permutation representation induced by the action of S_n on λ-tabloids. You checked that $M_{(n)}$ is the trivial representation of S_n. Here are two more examples.

Example 19.1.

(a) $M_{(1,1,\ldots,1)}$ is isomorphic to the regular representation of S_n.

(b) $M_{(n-1,1)}$ is isomorphic to the defining representation of S_n.

Proof:

(a) There are $n!$ tabloids of shape $(1, 1, \ldots, 1)$:

$$\begin{array}{c} \hline i \\ \hline j \\ \hline \vdots \\ \hline k \\ \hline \end{array}$$

The above tabloid can be identified with the permutation $\pi \in S_n$ with $\pi(1) = i$, $\pi(2) = j$, $\ldots$, $\pi(n) = k$. In this way, $M_{(1,\ldots,1)}$ can be viewed as the free vector space on the set S_n. The action of $\sigma \in S_n$ on the tabloid associated to π gives the tabloid associated to the composition $\sigma\pi$. Thus, $M_{(1,\ldots,1)}$ is isomorphic to the regular representation of S_n.

(b) There are n tabloids of shape $(n-1, 1)$:

$$\begin{array}{l} \hline * \;\; * \; \cdots \; * \\ \hline 1 \\ \hline \end{array}, \quad \begin{array}{l} \hline * \;\; * \; \cdots \; * \\ \hline 2 \\ \hline \end{array}, \quad \ldots, \quad \begin{array}{l} \hline * \;\; * \; \cdots \; * \\ \hline n \\ \hline \end{array}.$$

We can identify them with the integers $1, 2, \ldots, n$. The action of $\pi \in S_n$ on the tabloid corresponding to i is the tabloid corresponding to $\pi(i)$. Thus, $M_{(n-1,1)}$ is isomorphic to the permutation representation induced by the natural action of S_n on $\{1, \ldots, n\}$, which is the defining representation of S_n.

The preceding example shows that M_λ is not irreducible in general. (Permutation representations, if non-trivial, are never irreducible since they always contain a copy of the trivial representation.) However, each M_λ contains a special irreducible submodule S_λ. To define S_λ, we single out some special elements of M_λ.

Definition 19.2. For $\lambda \vdash n$ and $T \in \mathrm{YT}(\lambda)$, the **polytabloid of** T is the element $e_T \in M_\lambda$ given by

$$e_T = \sum_{\pi \in C(T)} \mathrm{sgn}(\pi)\, \pi\{T\}.$$

For instance, if $T = \begin{array}{|c|c|c|}\hline 1&2&3\\\hline 4&5\\\cline{1-2}\end{array}$ then

$$e_T = \begin{array}{ccc}\hline 1&2&3\\\hline 4&5&\\\cline{1-2}\end{array} - \begin{array}{ccc}\hline 4&2&3\\\hline 1&5&\\\cline{1-2}\end{array} - \begin{array}{ccc}\hline 1&5&3\\\hline 4&5&\\\cline{1-2}\end{array} + \begin{array}{ccc}\hline 4&5&3\\\hline 1&2&\\\cline{1-2}\end{array}.$$

Warning: The polytabloid e_T depends on the tableau T and not the tabloid $\{T\}$. Indeed, you should show that if we take $T' = \begin{array}{|c|c|c|}\hline 2&1&3\\\hline 4&5\\\cline{1-2}\end{array}$, which is row equivalent to the above T, then $e_{T'} \neq e_T$.

Definition 19.3. The **Specht module** corresponding to $\lambda \vdash n$ is the subspace S_λ of M_λ spanned by all polytabloids of shape λ:

$$S_\lambda = \operatorname{span}\{e_T \colon T \in \mathrm{YT}(\lambda)\}.$$

Each Specht module is in fact an S_n-invariant subspace. This follows at once from:

Lemma 19.4. For $\lambda \vdash n$, $T \in \mathrm{YT}(\lambda)$ and $\sigma \in S_n$, we have $\sigma \cdot e_T = e_{\sigma \cdot T}$.

Exercise 19.5. Prove Lemma 19.4. ▶

Example 19.6.

(a) $S_{(n)}$ is isomorphic to the trivial representation of S_n.

(b) $S_{(1,1,\dots,1)}$ is isomorphic to the alternating representation of S_n.

(c) $S_{(n-1,1)}$ is isomorphic to the standard representation of S_n.

Proof:

(a) $S_{(n)} = M_{(n)}$ and $M_{(n)}$ is the trivial representation.

(b) Let $T = \begin{array}{|c|}\hline 1\\\hline 2\\\hline \vdots\\\hline n\\\hline\end{array}$. Then $C(T) = S_n$ so

$$e_T = \sum_{\pi \in S_n} \operatorname{sgn}(\pi)\pi\{T\}.$$

If T' is any other tableau of shape $(1, \dots, 1)$, then $T' = \sigma T$ for some $\sigma \in S_n$, and we have

$$e_{T'} = e_{\sigma T} = \sum_{\pi \in S_n} \operatorname{sgn}(\pi)\pi\sigma\{T\} = \sum_{\pi \in S_n} \operatorname{sgn}(\pi\sigma^{-1})\pi\sigma^{-1}\sigma T = \operatorname{sgn}(\sigma)e_T,$$

where in the third equality we used the fact that $\pi \mapsto \pi\sigma^{-1}$ is a bijection of S_n to re-index the sum.

Thus, every polytabloid in $S_{(1,\ldots,1)}$ is a scalar multiple of e_T. Furthermore, the action of $\sigma \in S_n$ of e_T is given by $\sigma e_T = e_{\sigma T} = \operatorname{sgn}(\sigma) e_T$, as we've calculated above. So $S_{(1,\ldots,1)}$ is the alternating representation.

(c) Let

$$T_i = \begin{array}{|c|c|c|c|} \hline 1 & 2 & \cdots & n \\ \hline i \\ \cline{1-1} \end{array},$$

where the first row is missing the entry i. The tabloids $\{T_i\}$ form a basis for $M_{(n-1,1)}$. For $2 \leq i \leq n$, we have

$$e_{T_i} = \{T_i\} - \{T_1\},$$

while

$$e_{T_1} = \{T_1\} - \{T_2\} = -e_{T_2}.$$

The polytabloids $\{e_{T_i}\}_{i=2}^{n}$ form a basis for S_λ and show that

$$S_{(n-1,1)} = \{a_1\{T_1\} + \cdots + a_n\{T_n\} \colon a_1 + \cdots + a_n = 0\}.$$

Since we saw in Example 19.1 that $M_{(n-1,1)}$ is the defining representation of S_n, it follows that $S_{(n-1,1)}$ is the standard representation (see Problem 9.3).

Here is our main result.

Theorem 19.7. Let $\lambda \vdash n$. Then:

(a) S_λ is an irreducible $\mathbb{C}S_n$-module. (Irreducibility)

(b) $S_\lambda \ncong S_\mu$ if $\lambda \neq \mu$. (Inequivalence)

(c) The set $\{e_T \colon T \in \mathrm{SYT}(\lambda)\}$ is a basis for S_λ. (Standard Basis Theorem)

Proof (sketch): Parts (a) and (b) will be proved below (Corollary 19.15 and Corollary 19.17). I will only sketch the proof of part (c).

Linear independence: The idea is to define a partial order $\geq$ on tabloids such that if T is standard then $\{T\} \geq \pi\{T\}$; in particular, $\{T\}$ is greater than all tabloids that appear in $e_T = \sum_\pi \operatorname{sgn}(\pi)\pi\{T\}$. So if $\sum c_i e_{T_i} = 0$, where the T_i are standard, then we can read off the coefficients of the maximal tabloids one at a time to get that $c_i = 0$ for all i.

Spanning: This is more difficult. One non-constructive approach is as follows. Set $f_\lambda := |\mathrm{SYT}(\lambda)|$. By the dimension formula and assuming linear independence has been established, we have

$$n! = \sum_{\lambda \vdash n} (\dim S_\lambda)^2 \geq \sum_{\lambda \vdash n} f_\lambda^2.$$

We get our result if we can prove that $\sum f_\lambda^2 = n!$. This can be done by means of the *Robinson correspondence* (see §4.3 of Fulton).

Alternatively, one can develop the so-called *straightening algorithm* (§7.4 of Fulton) to show that any polytabloid can be expressed as a linear combination of standard polytabloids (with integer coefficients!). ■

Part (c) of the preceding theorem tells us that S_λ has a basis indexed by the standard Young tableaux of shape λ. Thus, as a vector space, S_λ is isomorphic to the free vector space V_λ on $\mathrm{SYT}(\lambda)$ which we defined in the previous lecture. By carrying over the action on tabloids, we can now make sense of the computations in Example 18.8. For instance, the computation

$$(1\ 2)\cdot \begin{array}{|c|c|}\hline 1 & 2 \\ \hline 3 \\ \cline{1-1}\end{array} = \begin{array}{|c|c|}\hline 1 & 2 \\ \hline 3 \\ \cline{1-1}\end{array} - \begin{array}{|c|c|}\hline 1 & 3 \\ \hline 2 \\ \cline{1-1}\end{array}$$

comes from letting $(1\ 2)$ act on the polytabloid of the tableau $T = \begin{array}{|c|c|}\hline 1 & 2 \\ \hline 3 \\ \cline{1-1}\end{array}$ and then re-writing the result in terms of standard polytabloids (a simple instance of the straightening algorithm!):

$$\begin{aligned}
(1\ 2)\cdot e_T &= (1\ 2)\cdot\left(\begin{array}{cc}\hline 1 & 2 \\ \hline 3 & \\ \cline{1-1}\end{array} - \begin{array}{cc}\hline 3 & 2 \\ \hline 1 & \\ \cline{1-1}\end{array}\right) \\
&= \begin{array}{cc}\hline 2 & 1 \\ \hline 3 & \\ \cline{1-1}\end{array} - \begin{array}{cc}\hline 3 & 1 \\ \hline 2 & \\ \cline{1-1}\end{array} \\
&= \begin{array}{cc}\hline 1 & 2 \\ \hline 3 & \\ \cline{1-1}\end{array} - \begin{array}{cc}\hline 1 & 3 \\ \hline 2 & \\ \cline{1-1}\end{array} \\
&= \left(\begin{array}{cc}\hline 1 & 2 \\ \hline 3 & \\ \cline{1-1}\end{array} - \begin{array}{cc}\hline 3 & 2 \\ \hline 1 & \\ \cline{1-1}\end{array}\right) - \left(\begin{array}{cc}\hline 1 & 3 \\ \hline 2 & \\ \cline{1-1}\end{array} - \begin{array}{cc}\hline 3 & 2 \\ \hline 1 & \\ \cline{1-1}\end{array}\right) \\
&= e_T - e_{T'},
\end{aligned}$$

where $T' = \begin{array}{|c|c|}\hline 1 & 3 \\ \hline 2 \\ \cline{1-1}\end{array}$. You should confirm the four other calculations in Example 18.8.

19.1 Irreducibility of S_λ

The proof consists of a sequence of fun little lemmas interspersed with some definitions.

Definition 19.8. Let $\lambda = (\lambda_1, \ldots, \lambda_k)$ and $\mu = (\mu_1, \ldots, \mu_l)$ be partitions of n. We say λ **dominates** μ, and write $\lambda \trianglerighteq \mu$, if

$$\lambda_1 \geq \mu_1, \quad \lambda_1 + \lambda_2 \geq \mu_1 + \mu_2, \quad \ldots.$$

(If $k \neq l$, pad λ and μ with 0s so that they have the same length.)

Dominance defines a partial order on the set of partitions of n. For instance, if $n = 6$, we have $(4, 2) \trianglerighteq (3, 1, 1)$ but $(4, 1, 1)$ and $(3, 3)$ are incomparable since $4 > 3$ but $4 + 1 < 3 + 3$.

Lemma 19.9. Suppose $\lambda, \mu \vdash n$ and take $T \in \mathrm{YT}(\lambda)$ and $S \in \mathrm{YT}(\mu)$. If, for each i, the numbers in the ith row of S belong to different columns in T, then $\lambda \trianglerighteq \mu$.

Proof: The μ_1 numbers in the first row of S go to distinct columns in T, so $\lambda_1 \geq \mu_1$. Likewise, the μ_2 numbers in the second row of S go to distinct columns of T. Thus, each column of T contains *at most* two numbers from the first two rows of S. To have enough space for this, we must have $\lambda_1 + \lambda_2 \geq \mu_2 + \mu_2$. (To see this, place the $\mu_1 + \mu_2$ numbers that are in the first two rows of μ into a diagram of shape λ and slide them up. They must all land somewhere in the first two rows.) Continue on to the third row, etc. ∎

We next introduce a construction that slightly generalizes our definition of λ-polytabloids.

Definition 19.10. Let $\lambda, \mu \vdash n$. For $T \in \mathrm{YT}(\lambda)$, the **(column) antisymmetrizer** A_T is the linear map

$$\begin{aligned} A_T \colon M_\mu &\to M_\mu \\ \{S\} &\mapsto \sum_{\pi \in C(T)} \operatorname{sgn}(\pi)\pi\{S\}. \end{aligned}$$

Since the formula for A_T is independent of μ, we may write $A_T = \sum_{\pi \in C(T)} \operatorname{sgn}(\pi)\pi$.

Note that $A_T\{T\} = e_T$, where e_T is the polytabloid associated to T.

Lemma 19.11. Suppose $\lambda, \mu \vdash n$ and take $T \in \mathrm{YT}(\lambda)$ and $S \in \mathrm{YT}(\mu)$. If $A_T\{S\} \neq 0$ then $\lambda \trianglerighteq \mu$ and, furthermore, if $\lambda = \mu$ then $A_T\{S\} = \pm e_T$.

Proof: Use Lemma 19.9. If $i \neq j$ occur in the same row of S and the same column of T then the transposition $(i\ j)$ belongs to $R(S) \cap C(T)$. It follows that

$$\begin{aligned} A_T\{S\} &= A_T\{(i\ j)S\} && ((i\ j) \in R(T)) \\ &= \sum_{\pi \in C(T)} \operatorname{sgn}(\pi)\pi(i\ j)\{S\} \\ &= \sum_{\pi \in (i\ j)C(T)} \operatorname{sgn}(\pi(i\ j)^{-1})\pi\{S\} && (\text{re-index: } \pi \leftrightarrow \pi(1\ j)^{-1}) \\ &= \sum_{\pi \in C(T)} \operatorname{sgn}(\pi(i\ j)^{-1})\pi\{S\} && ((i\ j) \in C(T)) \\ &= \operatorname{sgn}(i\ j) \sum_{\pi \in C(T)} \operatorname{sgn}(\pi)\pi\{S\} \\ &= -A_T\{S\}. \end{aligned}$$

This contradicts the assumption that $A_T\{S\} \neq 0$. Thus, the entries in any given row of S belong to different columns of T, so $\lambda \trianglerighteq \mu$; furthermore, if $\lambda = \mu$, then we can slide the entries of T up or down each column to make $\{T\}$ identical with $\{S\}$, i.e., there exists some $\sigma \in C(T)$ such that $\{S\} = \sigma\{T\}$. A calculation as above gives $A_T\{S\} = \operatorname{sgn}(\sigma^{-1})A_T\{T\} = \pm e_T$, as claimed. ■

Lemma 19.12. Let $v \in M_\lambda$ and $T \in \mathrm{YT}(\lambda)$. Then $A_T v = c e_T$ for some $c \in \mathbb{C}$.

Proof: Immediate from the previous lemma together with the fact that v is a linear combination of λ-tabloids $\{S\}$. ■

Next, define an inner product on M_λ by defining it on the basis of M_λ by

$$\langle \{S\}, \{T\} \rangle = \begin{cases} 1 & \text{if } \{S\} = \{T\} \\ 0 & \text{otherwise.} \end{cases}.$$

Thus, the basis $\mathrm{YTD}(\lambda)$ of M_λ is orthonormal with respect to $\langle\ ,\ \rangle$. Note also that $\langle\ ,\ \rangle$ is S_n-invariant. Indeed, $\sigma\{S\} = \sigma\{T\}$ if and only if $\{S\} = \{T\}$, so

$$\langle \sigma\{S\}, \sigma\{T\} \rangle = \langle \{S\}, \{T\} \rangle \quad \text{for all } \sigma \in S_n.$$

Remarkably, the antisymmetrizing operators A_T are self-adjoint with respect to $\langle\ ,\ \rangle$:

Lemma 19.13. For $u, v \in M_\lambda$, $\langle A_T v, u \rangle = \langle v, A_T u \rangle$.

Proof: We have

$$\begin{aligned} \langle A_T v, u \rangle &= \sum_{\pi \in C(T)} \operatorname{sgn}(\pi) \langle \pi v, u \rangle \\ &= \sum_{\pi \in C(T)} \operatorname{sgn}(\pi) \langle v, \pi^{-1} u \rangle && (S_n\text{-invariance}) \\ &= \left\langle v, \sum_{\pi \in C(T)} \operatorname{sgn}(\pi) \pi^{-1} u \right\rangle \\ &= \left\langle v, \sum_{\pi \in C(T)} \operatorname{sgn}(\pi^{-1}) \pi u \right\rangle && (\text{re-index: } \pi \leftrightarrow \pi^{-1}) \\ &= \langle v, A_T u \rangle && (\operatorname{sgn}(\pi^{-1}) = \operatorname{sgn}(\pi)) \end{aligned}$$

as required. ■

Theorem 19.14 (James Submodule Theorem)**.** If $U \subseteq M_\lambda$ is an S_n-invariant subspace, then either $U \supseteq S_\lambda$ or $U \subseteq (S_\lambda)^\perp$.

Proof: Let $u \in U$ and $T \in \mathrm{YT}(\lambda)$. Then $A_T u = c e_T$ for some $c \in \mathbb{C}$ by Lemma 19.12. If $c \neq 0$, then $e_T \in U$ hence $e_{\sigma T} = \sigma e_T \in U$ for all $\sigma \in S_n$ since U is S_n-invariant. It follows that $e_{T'} \in U$ for all $T' \in \mathrm{YT}(\lambda)$ since the S_n-action on λ-tableau is transitive. Thus, $S_\lambda = \operatorname{span}\{e_{T'}\}_{T'} \subseteq U$.

On the other hand, if $A_T u = 0$ for all $u \in U$ and $T \in \mathrm{YT}(\lambda)$, then

$$0 = \langle A_T u, \{T\} \rangle = \langle u, A_T\{T\} \rangle = \langle u, e_T \rangle \quad \text{for all } u \in U \text{ and } T \in \mathrm{YT}(\lambda).$$

Thus, U is orthogonal to all e_T and so $U \subseteq (S_\lambda)^\perp$. ■

Applying this theorem to an S_n-invariant subspace $U \subseteq S_\lambda$, we deduce:

Corollary 19.15 (Irreducibility of Specht Modules)**.** For each $\lambda \vdash n$, the Specht module S_λ is an irreducible $\mathbb{C}S_n$-module.

19.2 Inequivalence of S_λ and S_μ

One more fun lemma!

Lemma 19.16. Let $\lambda, \mu \vdash n$. If there is a nonzero $\varphi \in \mathrm{Hom}_{S_n}(S_\lambda, M_\mu)$ then $\lambda \trianglerighteq \mu$.

Proof: If $\varphi \neq 0$ then $\varphi(e_T) \neq 0$ for some $T \in \mathrm{YT}(\lambda)$. Since $M_\lambda = S_\lambda \oplus (S_\lambda)^\perp$, we can extend φ to M_λ by defining it to be zero on $(S_\lambda)^\perp$; this gives an S_n-linear map $\varphi\colon M_\lambda \to M_\mu$. Now,

$$0 \neq \varphi(e_T) = \varphi(A_T\{T\}) = A_T\varphi(\{T\}) = A_T \sum_S c_S\{S\}.$$

So $A_T\{S\} \neq 0$ for some $S \in \mathrm{YT}(\mu)$. Thus, $\lambda \trianglerighteq \mu$ by Lemma 19.11. ■

Corollary 19.17 (Inequivalence of Specht Modules)**.** Let $\lambda, \mu \vdash n$. If $\lambda \neq \mu$ then $S_\lambda \ncong S_\mu$ as $\mathbb{C}S_n$-modules.

Proof: If there is an isomorphism $\varphi\colon S_\lambda \to S_\mu \subseteq M_\mu$ then the previous lemma gives $\lambda \trianglerighteq \mu$. Going the other way, we get $\mu \trianglerighteq \lambda$, so in fact $\lambda = \mu$. ■

19.3 The Isotypic Decomposition of M_μ

Lemma 19.16 shows that the only Specht modules S_λ that occur in M_μ are those with $\lambda \trianglerighteq \mu$. In fact, we can give a slightly more precise result as follows.

Theorem 19.18 (Isotypic Decomposition of M_μ)**.** Let $\mu \vdash n$. Then:

$$M_\mu = S_\mu \oplus \bigoplus_{\substack{\lambda \trianglerighteq \mu \\ \lambda \neq \mu}} (S_\lambda)^{\oplus K_{\lambda\mu}}$$

for some non-negative integers $K_{\lambda\mu}$. In particular, the multiplicity of S_μ in M_μ is 1.

Proof: By definition, S_μ does occur as a submodule of M_μ, and its multiplicity is given by $\dim \mathrm{Hom}_{S_n}(S_\mu, M_\mu)$. Now, given $\varphi \in \mathrm{Hom}_{S_n}(S_\mu, M_\mu)$, extend it to M_μ as in the proof of

Lemma 19.16 and note that for any polytabloid e_T with $T \in \mathrm{YT}(\mu)$, we have

$$\varphi(e_T) = \varphi(A_T\{T\}) = A_T\varphi(\{T\}) = ce_T,$$

for some $c \in \mathbb{C}$ by Lemma 19.12. If $e_{T'}$ is another polytabloid, we have $T' = \sigma T$ for some $\sigma \in S_n$ and so $e_{T'} = e_{\sigma T} = \sigma e_T$. Hence

$$\varphi(e_{T'}) = \sigma\varphi(e_T) = c\sigma e_T = ce_{T'}.$$

Thus, $\varphi = c\,\mathrm{id}$. Consequently, $\dim \mathrm{Hom}_{S_n}(S_\mu, M_\mu) = 1$. ■

The multiplicities $K_{\lambda\mu}$ are known as the **Kostka numbers**. They have an interesting combinatorial description, as follows.

Definition 19.19. Let $\lambda \vdash n$. A **semistandard Young tableau T of shape λ** is a numbering of the Young diagram for λ with the integers 1, 2, ..., n with repetitions allowed such that each row is weakly increasing and each column is strictly increasing. The **content** of T is the tuple $\mu = (\mu_1, \mu_2, \ldots, \mu_n)$ where μ_i is the number of i's in T.

For example,

$T =$
<table>
<tr><td>1</td><td>2</td><td>2</td><td>4</td></tr>
<tr><td>2</td><td>5</td><td></td><td></td></tr>
<tr><td>5</td><td></td><td></td><td></td></tr>
</table>
.

is a semistandard Young tableau of shape $\lambda = (4, 2, 1)$ and content $\mu = (1, 3, 0, 1, 2, 0, 0)$. (We usually omit the trailing 0s and write $\mu = (1, 3, 0, 1, 2)$.) Note that the entries of μ need not satisfy $\mu_1 \geq \mu_2 \geq \cdots$, so we generally do not have that $\mu \vdash n$. However, when we do...

Theorem 19.20. Suppose $\lambda, \mu \vdash n$. Then the number of semistandard Young tableau of shape λ and content μ is equal to the Kostka number $K_{\lambda\mu} = \mathrm{mult}(S_\lambda, M_\mu)$. ■

We won't prove this theorem, but we will look at a few examples.

Example 19.21. We have $K_{\lambda\lambda} = 1$ since the only way to write down λ_1 1's in a semistandard tableau of shape λ is to place them in the first row; likewise, the λ_2 2's must go in the second row, etc. This is inline with the fact that $\mathrm{mult}(S_\lambda, M_\lambda) = 1$, as proved in Theorem 19.18.

Example 19.22. If $\lambda = (n)$ then $K_{(n)\mu} = 1$ for all $\mu \vdash n$, since there is exactly one semistandard tableau of shape λ and content μ, given by listing out μ_1 1's, μ_2 2's and so on, in order from left to right.

In terms of representation theory, $K_{(n)\mu} = \mathrm{mult}(S_{(n)}, M_\mu)$ is the multiplicity of the trivial representation in M_μ. Since M_μ is the permutation representation for the S_n-set $\mathrm{YTD}(\mu)$, we know that $\mathrm{mult}(\mathrm{triv}, M_\mu)$ is the number of S_n-orbits in $\mathrm{YTD}(\mu)$. The number of orbits is 1 since S_n acts transitively on $\mathrm{YTD}(\mu)$.

Example 19.23. Let $\mu = (1,1,1)$. Then the partitions $\lambda \vdash 3$ that dominate μ are μ, $(2,1)$ and (3) (i.e., all partitions of 3 dominate μ!). Thus,

$$M_{(1,1,1)} = S_{(1,1,1)} \oplus S_{(2,1)}^{\oplus K} \oplus S_{(3)},$$

where $K = K_{(2,1)(1,1,1)}$ and we've used the previous two examples to determine the multiplicities $K_{(1,1,1)(1,1,1)} = K_{(3)(1,1,1)} = 1$.

We can calculate $K_{(2,1)(1,1,1)}$ easily. The only semistandard Young tableaux of shape $(2,1)$ and content $(1,1,1)$ are

$$\begin{array}{|c|c|}\hline 1 & 2 \\ \hline 3 \\ \cline{1-1}\end{array} \quad \text{and} \quad \begin{array}{|c|c|}\hline 1 & 3 \\ \hline 2 \\ \cline{1-1}\end{array}.$$

Thus, $K_{(2,1)(1,1,1)} = 2$—as expected! Indeed, $M_{(1,1,1)}$ is the regular representation and $S_{(2,1)}$ is the standard representation so $\operatorname{mult}(S_{(2,1)}, M_{(1,1,1)}) = \dim S_{(2,1)} = 2$.

Exercise 19.24. Determine the isotypic decomposition of $M_{(3,3)}$. ▶

Lecture 19 Problems

19.1. Find all pairs of partitions of 6 that are not comparable in the dominance ordering.

19.2. Let $X = \{\{i,j\} : 1 \le i,j \le n\}$ be the set of *unordered* pairs of integers in $\{1,2,\ldots,n\}$. Note that S_n acts on X by $\pi\{i,j\} = \{\pi(i),\pi(j)\}$. Let V denote the permutation representation induced by the S_n-action on X. Determine the isotypic decomposition of V. [Hint: Identify V with a certain M_μ. You should find that V decomposes into three irreps each with multiplicity 1.]

19.3. Show that χ_V is integer-valued for each $V \in \operatorname{Irr}_{\mathbb{C}}(S_n)$.

19.4. Let $V \in \operatorname{Irr}_{\mathbb{C}}(S_n)$. Show that $V^* \cong V$.

19.5. Let $\mu = (1,\ldots,1) \vdash n$. What is the Kostka number $K_{\lambda\mu}$?

19.6. Prove by counting semistandard tableaux that $K_{\lambda\mu} \neq 0$ if and only if $\lambda \trianglerighteq \mu$.

19.7. (Challenging.) Show that $\operatorname{Alt}^k(S_{(n-1,1)}) \cong S_{(n-k,1,\ldots,1)}$ for $1 \le k \le n-1$.

Lecture 20 Modules and Algebras

We now momentarily pause our discussion of representation theory to introduce some useful notions from (noncommutative) abstract algebra. We will study modules and algebras over arbitrary rings. In particular, we will drop our assumption on F from Lecture 12.

20.1 Motivating Example: The Group Ring

Our starting point is a comment made in Remark 14.5. Namely, is there a way to 'enhance' the isotypic decomposition

$$\begin{aligned}\mathbb{C}\langle G\rangle &\cong V_1^{\oplus d_i} \oplus \cdots \oplus V_h^{\oplus d_h} \\ &\cong M_{d_1}(\mathbb{C}) \oplus \cdots \oplus M_{d_h}(\mathbb{C}),\end{aligned}$$

of the regular representation of G so that it becomes an isomorphism of rings (in addition to being an isomorphism of vector spaces)?[15] For this to make sense, we need to put a ring structure on $\mathbb{C}\langle G\rangle$. Fortunately, there is a natural way of doing this.

We start a little more generally. Let G be a finite group, let F be an arbitrary field, and consider the representation space for the regular representation of G:

$$F\langle G\rangle = \left\{ \sum_{g\in G} a_g g \colon a_g \in F \right\}.$$

We can define a multiplication operation on $F\langle G\rangle$ by

$$\left(\sum_{g\in G} a_g g\right) \cdot \left(\sum_{h\in G} b_h h\right) = \sum_{g,h\in G} a_g b_h (gh),$$

where gh is the group product of g and h in G. For example, in $\mathbb{R}C_3$, we have

$$(2a + \sqrt{3}a^2)(1-a) = 2a - 2a^2 + \sqrt{3}a^2 - \sqrt{3}a^3 = 2a + (\sqrt{3}-2)a^2 - \sqrt{3}.$$

It's easy to check that this operation turns $F\langle G\rangle$ into a ring. We will write FG instead of $F\langle G\rangle$ to signal that we are viewing $F\langle G\rangle$ as a ring. We call FG the **group ring** of G over F.

> **Exercise 20.1.** Use the vector space isomorphism $F\langle G\rangle \cong \mathcal{F}(G,F)$ given by identifying $g \in G$ with the indicator function at g to transport the ring multiplication above to $\mathcal{F}(G,F)$. Write down the product $f * g$ of $f, g \in \mathcal{F}(G,F)$ explicitly. If you do this correctly, you will have discovered the so-called **convolution** product of functions. ▶

The group ring FG acts on representations of G as follows. If $\rho\colon G \to GL(V)$ is a representation, then each $g \in G$ acts on $v \in V$ by $g \cdot v = \rho(g)v$. This action extends naturally from

[15] For category theory reasons, it is more appropriate to write $\times$ instead of $\oplus$ when talking about rings. So we are in search of a ring isomorphism $\mathbb{C}\langle G\rangle \cong M_{d_1}(\mathbb{C}) \times \cdots \times M_{d_h}(\mathbb{C})$.

G to the whole ring FG:

$$\left(\sum_{g\in G} a_g g\right)\cdot v = \sum_{g\in G} a_g \rho(g) v.$$

[Note: We have implicitly used this observation at several points in the preceding lectures (see, e.g., Lemma 13.3, the proof of Lemma 14.2 and Definition 19.10).]

In this way, the F-vector space V becomes what one might call an "FG-vector space." However, FG is merely a ring and not a field in general. A "vector space" over a ring R is called an R-*module* (see Definition 20.2 below). Thus, V is an example of an FG-module, which coincidentally (!) is exactly the terminology we have been using.

20.2 Modules

In what follows, our rings will be unital but possibly noncommutative. The unit element will be denoted by 1. We assume that $1 \neq 0$.

Definition 20.2. Let R be a ring. A **(left) R-module** is an abelian group M (written additively) together with a map $R \times M \to M$, written as $(r,m) \mapsto rm$, that satisfies:

(i) $1m = m$

(ii) $r(m+m') = rm + rm'$

(iii) $(r+r')m = rm + r'm$

(iv) $(rr')m = r(r'm)$

for all $r, r' \in R$ and $m, m' \in M$.

Remark 20.3.

(a) There is an obvious parallel notion of a **right R-module**. If R is commutative, then every left R-module becomes a right R-module if we define $mr := rm$. However, if R is noncommutative, then to get the analogue of axiom (iv) to hold we will need to bring in the **opposite ring** R^{opp} of R. The ring R^{opp} has the same additive group as R but the multiplication $*$ in R is the reverse of that in R: $a * b = ba$. (So $R^{\mathrm{opp}} = R$ if R is commutative.) If M is a left R-module then defining $mr := rm$ turns M into a right R^{opp}-module. In this way, the theories of left and right R-modules are essentially identical, and so picking a side is a matter of taste. We will work with left modules unless explicitly noted otherwise.

(b) Definition 20.2 should remind you of the definition of a group action on a set. Indeed, a module is an abelian group equipped with an action by a ring. We get an analogue of Proposition 1.9 in this setting, namely: Each $r \in R$ defines a group homomorphisms $\mu_r\colon M \to M$ by $\mu_r(m) = rm$. The module axioms show that the map $\varphi\colon R \to \mathrm{End}(M)$ defined by $\varphi(r) = \mu_r$, where $\mathrm{End}(M)$ is the *ring* of group homomorphism $M \to M$ (a.k.a. endomorphisms of M), is a ring homomorphism.

Conversely, given a ring homomorphism $\varphi\colon R \to \operatorname{End}(M)$, we can turn M into an R-module by defining $rm := \varphi(r)(m)$.

(c) A standard argument using the axioms shows that

$$r0_M = 0_M \quad \text{and} \quad 0_R m = 0_M \text{ for all } r \in R \text{ and } m \in M.$$

So we will just write 0 for both 0_R and 0_M. Likewise,

$$-(rm) = (-r)m = r(-m) \text{ for all } r \in R \text{ and } m \in M.$$

So we will write $-rm$ for this element.

Example 20.4.

(a) If F is a field, then an F-module is the same thing as an F-vector space.

(b) A $\mathbb{Z}$-module is the same thing as an abelian group.

(c) Every ring R is an R-module via $r \cdot r' = rr'$. We call R the **regular** R-module.

(d) If $R = FG$ is the group ring of G over F, then an FG-module is the same thing as a representation of G over F. (Be sure to check this carefully!)

(e) Let $R = F[x]$ be a polynomial ring over F. An R-module is the same thing as a pair (V, T) where V is an F-vector space and $T\colon V \to V$ is an F-linear map.

Indeed, given such a pair (V, T), we can define an $F[x]$-module structure on V by letting x act on V as T. More precisely, define

$$p(x)v := p(T)v \text{ for } p(x) \in F[x] \text{ and } v \in V. \tag{11}$$

Conversely, if V is an $F[x]$-module, then V is equipped with an action by $F \subseteq R$ that makes V into an F-module, i.e. an F-vector space. The action of the rest of $F[x]$ is determined once we specify how x acts. The module axioms show that left-multiplication by x defines a map $T\colon V \to V$ that is F-linear. The general element $p(x) = \sum a_i x^i$ of $F[x]$ then acts on $v \in V$ as in (11).

(f) Let $R = M_n(F)$ is the ring of $n \times n$ matrices with coefficients in F. Then F^n is an R-module via matrix-vector multiplication:

$$A(x_1, \ldots, x_n) := A \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}.$$

Some of the modules above are more than just modules: they are also rings, and the module structure is compatible with the ring structure. This gives rise to the following definition.

Definition 20.5. An R-**algebra** is a ring A that is also an R-module such that

$$r(ab) = (ra)b = a(rb)$$

for all $r \in R$ and $a, b \in A$.

The usual notions carry over in the obvious way. For example, a subalgebra is a subset this is an algebra; a homomorphism of algebras is a homomorphism of rings that is also a homomorphism of modules, etc. If F is a field, then an F-algebra A is in particular an F-vector space, and we define the **dimension** of A to be its dimension as an F-vector space.

Example 20.6.

(a) If R is commutative, then the regular module R is an R-algebra. For instance, every field F is an F-algebra. More generally, if $F \subseteq E$ are fields, then E is an F-algebra. So, for example, $\mathbb{C}$ is an $\mathbb{R}$-algebra.

(b) $M_n(F)$, FG and $F[x]$ are all F-algebras. The set of uppertriangular matrices is a subalgebra of $M_n(F)$.

The next example is quite important both for historical reasons and also for representation-theoretic reasons (as we will to come to see).

Example 20.7 (The Hamilton quaternions)**.** Let $\mathbb{H}$ be the 4-dimensional $\mathbb{R}$-vector space with basis $\{1, i, j, k\}$. Define a multiplication on $\mathbb{H}$ by declaring

$$i^2 = j^2 = k^2 = -1,$$

$$ij = k = -ji, \quad jk = i = -kj, \quad ki = j = ik$$

and extending linearly and associatively. It is straightforward (but tedious) to prove that this multiplication turns $\mathbb{H}$ into a ring; in fact, it turns it into an $\mathbb{R}$-algebra.

If $\alpha = a1 + bi + cj + dk \in \mathbb{H}$, define the **conjugate** of α by $\alpha^* = a1 - bi - cj - dk$. Then a calculation shows that

$$\alpha\alpha^* = \alpha^*\alpha = a^2 + b^2 + c^2 + d^2.$$

In particular, if $\alpha \neq 0$, then α has a two-sided inverse in $\mathbb{H}$ given by

$$\alpha^{-1} = \frac{\alpha^*}{a^2 + b^2 + c^2 + d^2}.$$

Thus, $\mathbb{H}$ is an example of a **division algebra** (i.e. an algebra that is also a division ring).

Remark 20.8. A classical theorem due to Frobenius (that we *might* prove later) asserts that, up to isomorphism, the only finite-dimensional division $\mathbb{R}$-algebras are $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{H}$.

20.3 Submodules and Modules Homomorphisms

The definitions and constructions here are exactly what you think they should be.

Definition 20.9. Let M be an R-module. A **submodule** of M is a subset $N \subseteq M$ that is an R-module with the same R-action.

Equivalently, a submodule N of M is an subgroup of the abelian group M that is closed under multiplication by R in the sense that $rn \in N$ for all $r \in R$ and $n \in N$.

Example 20.10.

(a) 0 and M are submodules of every module M.

(b) If F is a field, then a submodule of an F-module is the same thing as a subspace. A submodule of a $\mathbb{Z}$-module is the same thing as a subgroup.

(c) A submodule of the regular R-module R is the same thing as a left ideal of R.

(d) Let V be an FG-module, i.e. a representation of G. Then a submodule of V is the same thing as a G-invariant subspace $U \subseteq V$.

(e) Likewise, if (V, T) is an $F[x]$-module, then a submodule is a subspace $U \subseteq V$ that is T-invariant.

(f) Let $S \subseteq M$ be a subset of the R-module M. The **submodule of M generated by S**, denoted by $\langle S \rangle$ or RS, is the submodule consisting of all *finite* linear combinations $\sum_{i=1}^{n} r_i s_i$ with $r_i \in R$ and $s_i \in S$. As a special case, if $S = \{m\}$ is a singleton, then we write Rm for this submodule, and we have $Rm = \{rm \colon r \in R\}$.

 If $M = \langle S \rangle$, then we say that M is **generated by** S. If M is generated by a finite set, then we say that M is **finitely generated**. If $M = Rm$ is generated by a single element then we say M is **cyclic**.

(g) If $\{U_i\}_{i \in I}$ is a family of submodules of M, then their intersection $\bigcap_{i \in I} U_i$ is a submodule of M, as is their sum

$$\sum_{i \in I} U_i = \left\{ \sum_{i \in I} u_i \colon u_i \in U_i \text{ and } u_i = 0 \text{ for all but finitely many } i \in I \right\}.$$

Definition 20.11. Let M and N be R-modules. A function $f \colon M \to N$ is an **R-module homomorphism** if it satisfies

$$f(rm) = rf(m) \quad \text{and} \quad f(m + m') = f(m) + f(m')$$

for all $r \in R$ and $m, m' \in M$. (So f is **R-linear** and additive.)

The **kernel** of f is

$$\ker(f) = \{m \in M \colon f(m) = 0\}$$

and the **image**, or **range**, of f is

$$\operatorname{im}(f) = \{n \in N \colon n = f(m) \text{ for some } m \in M\}.$$

Note that $\ker(f)$ is a submodule of M and $\operatorname{im}(f)$ is a submodule of N. If $\ker(f) = 0$, we say f is **injective**. If $\operatorname{im}(f) = N$, we say f is **surjective**. If f is both injective and surjective, we say f is an **isomorphism** and we write $M \cong N$. In this case, f^{-1} is also an R-module homomorphism.

The set of all R-module homomorphisms from M to N will be denoted by $\operatorname{Hom}_R(M, N)$. If $M = N$, then we set $\operatorname{End}_R(M) := \operatorname{Hom}_R(M, M)$ and call this the **endomorphism ring** of M; it is a ring under pointwise addition and composition of homomorphisms. Be careful to note that there is also the ring $\operatorname{End}(M)$ consisting of *group* homomorphisms $M \to M$; for clarity, we will denote this latter ring by $\operatorname{End}_{\mathbb{Z}}(M)$.

Example 20.12. A module homomorphism between F-modules (i.e. F-vector spaces) is the same thing as an F-linear map. Likewise, a module homomorphism between $\mathbb{Z}$-modules (i.e. abelian groups) is the same thing as a group homomorphism, and a module homomorphism between FG-modules (i.e. representations of G) is what we'd previously called a G-linear map.

If N is a submodule of the R-module M, then we can form the quotient M/N as an abelian group. This becomes an R-module if we define

$$r(m + N) = rm + N.$$

That fact that N is closed under multiplication by $r \in R$ ensures that this is well-defined. We call M/N the **quotient module** of M by N. The next result should come as no surprise.

Theorem 20.13 (First Isomorphism Theorem)**.** Let $f \colon M \to N$ be a homomorphism of R-modules. Then f induces an injective homomorphism

$$\begin{aligned} \bar{f} \colon M/\ker(f) &\to N \\ m + \ker(f) &\mapsto f(m). \end{aligned}$$

In particular,

$$M/\ker(f) \cong \operatorname{im}(f).$$

Proof: The well-definedness of $\bar{f}$, as well as its injectivity, come for free from the First Isomorphism Theorem for groups applied to the abelian groups M and N. So we just need to check that $\bar{f}$ is R-linear. This follows at once from the fact that f is R-linear:

$$\bar{f}(r(m + \ker(f))) = \bar{f}(rm + \ker(f)) = f(rm) = rf(m) = r\bar{f}(m + \ker(f)). \qquad \blacksquare$$

The Second and Third Isomorphism Theorems also hold for modules. I will let you formulate and prove the appropriate statements.

Lecture 20 Problems

20.1. Prove that $FC_n \cong F[x]/(x^n - 1)$ as rings.

20.2. Prove that there are ring isomorphisms:

(a) $\mathbb{H}^{\mathrm{opp}} \cong \mathbb{H}$.

(b) $(FG)^{\mathrm{opp}} \cong FG$.

20.3. (a) Show that a one-dimensional $\mathbb{R}$-algebra must be isomorphic to $\mathbb{R}$.

(b) Show that a two-dimensional $\mathbb{R}$-algebra must be isomorphic to one of

$$\mathbb{R}[x]/(x^2), \quad \mathbb{R}[x]/(x^2+1), \quad \text{or} \quad \mathbb{R}[x]/(x^2-1).$$

Show also that no two of these are isomorphic to each other. [Hint: Consider a basis of the form $\{1, a\}$ and then examine a^2.]

(c) Consider the two-dimensional subalgebra $A = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} : a, b \in \mathbb{R} \right\}$ of $M_2(\mathbb{R})$. Identify the algebra in (b) that is isomorphic to A.

20.4. (a) Show that $S = \{a + bi \colon a, b \in \mathbb{R}\}$ is a subring of $\mathbb{H}$ that is isomorphic to $\mathbb{C}$. Deduce that multiplication by elements in S allows us to view $\mathbb{H}$ as a $\mathbb{C}$-module. Is $\mathbb{H}$ a $\mathbb{C}$-algebra?

(b) Show that there is a bijection between the set of solutions to $x^2 + 1 = 0$ in $\mathbb{H}$ and the unit sphere $\{x^2 + y^2 + z^2 = 1\}$ in $\mathbb{R}^3$. In particular, there are infinitely many square roots of -1 in $\mathbb{H}$.

20.5. For $a, b \in \mathbb{R}^\times$, define the generalized quaternion algebra $\mathbb{H}_{a,b}$ to be the 4-dimensional $\mathbb{R}$-vector space with basis $1, i, j, k$ and multiplication satisfying

$$i^2 = a, \quad j^2 = b \quad \text{and} \quad ij = -ji = k.$$

Note that the Hamilton quaternion algebra is $\mathbb{H} = \mathbb{H}_{-1,-1}$.

(a) Convince yourself that the above really defines an $\mathbb{R}$-algebra. In particular, what are the products ik, ki, jk, kj? Show that $k^2 = -ab$.

(b) Show that there are isomorphisms of $\mathbb{R}$-algebras $\mathbb{H}_{a,b} \cong \mathbb{H}_{b,a}$ and $\mathbb{H}_{u^2a, v^2b} \cong \mathbb{H}_{a,b}$ for all $u, v \in \mathbb{R}^\times$. Hence deduce that $\mathbb{H}_{a,b}$ is isomorphic to one of $\mathbb{H}_{1,1}$, $\mathbb{H}_{1,-1}$ and $\mathbb{H}_{-1,-1}$.

(c) Show that $\mathbb{H}_{1,1} \cong \mathbb{H}_{1,-1} \cong M_2(\mathbb{R})$ and that $\mathbb{H}_{-1,-1} \not\cong M_2(\mathbb{R})$.

Lecture 21 Simple Modules

Just like we introduced irreducible representations to help us study arbitrary representations, we now introduce the analogous notion for modules.

Definition 21.1. An R-module M is said to be **simple** if $M \neq 0$ and if M has no proper, nontrivial submodules.

Example 21.2.

(a) Let F be a field. An F-module (i.e. F-vector space) V is simple if and only if $\dim_F V = 1$.

(b) A $\mathbb{Z}$-module (i.e. abelian group) A is simple if and only if $A \cong C_p$ where p is a prime.

(c) An FG-module V is simple if and only if V is an irreducible representation of G (over F).

(d) Let I be a left ideal in R. Then I is a simple R-module if and only if it is a *minimal* left ideal. Similarly, the quotient module R/I is simple if and only if I is a *maximal* left ideal, since submodules of R/I are submodules of R that contain I.

(e) Let $R = M_n(F)$ and $M = F^n$. Then M is a simple R-module. Indeed, suppose $N \subseteq M$ is a nonzero submodule, and take $x = (x_1, \ldots, x_n) \in M$ with $x_j \neq 0$ (say). Then if $E_{ij} \in R$ is the matrix with a 1 in the (i, j)th entry and 0s elsewhere, we have $\frac{1}{x_j} E_{ij} x = e_i$ (the ith standard basis vector of $M = F^n$). Thus, $e_i \in N$ for all i so $N = M$.

Part (d) of the preceding example describes the most general example of a simple module.

Proposition 21.3. Let $M \neq 0$ be a nonzero R-module. Then the following are equivalent.

(a) M is a simple R-module.

(b) $M = Rm$ for any $m \neq 0$ in M.

(c) $M \cong R/\mathfrak{m}$ where $\mathfrak{m}$ is a maximal left ideal in R.

Proof: (a) $\iff$ (b): Assume M is simple. Then, for all $m \neq 0$, Rm is a nonzero submodule of M hence must be equal to M. Conversely, assume that $M = Rm$ for all $m \neq 0$. If U is a nontrivial submodule of M, say containing $u \neq 0$, then $U \supseteq Ru = M$. Thus, $U = M$. So M is simple.

(a) $\iff$ (c): We have already noted that $R/\mathfrak{m}$ is simple whenever $\mathfrak{m}$ is a maximal left ideal. Conversely assume M is simple, and write $M = Rm$ for some $m \neq 0$ by (b). Define $\varphi\colon R \to M$ by $\varphi(r) = rm$. This is an R-module homomorphism that is, by construction, surjective. Thus, $R/\ker\varphi \cong M$. Since M is simple, it must be the case that $\ker\varphi$ is a maximal left ideal in R. This proves that $(a) \implies (c)$. ■

Let's close this section by showing how module theory can lead to interesting results in representation theory (a recurring phenomenon).

Example 21.4. Let $R = F[x]/(f(x))$, where F is a field and $\deg(f(x)) \geq 1$. Suppose that $f(x) = p_1(x)^{a_1} \cdots p_k(x)^{a_k}$ is the factorization of $f(x)$ into irreducible polynomials. In Problem 21.5 you are asked to prove that, up to isomorphism, the simple R-modules are given by $S_i = F[x]/(p_i(x))$ for $1 \leq i \leq k$.

In particular, consider $R = FC_n$, where C_n is the cyclic group of order n. Then the simple FC_n-module are precisely the irreducible representations of $C_n = \langle x \colon x^n = 1 \rangle$ over F. On the other hand, we have an isomorphism of rings

$$FC_n \cong F[x]/(x^n - 1).$$

Thus, we can now determine $\mathrm{Irr}_F(C_n)$ for all F—provided we can factor $x^n - 1$ over F.

For instance, if $F = \mathbb{C}$ then $x^n - 1$ splits into linear factors:

$$x^n - 1 = \prod_{i=1}^{n} (x - \zeta^i),$$

where ζ is a primitive nth root of unity. Thus, the simple FC_n-modules are given by $V_i = \mathbb{C}[x]/(x - \zeta^i)$ for $1 \leq i \leq n$. Note that $V_i \cong \mathbb{C}$ as a $\mathbb{C}C_n$-module, where the generator $x \in C_n$ acts on $\mathbb{C}$ as multiplication by $x = \zeta^i$. We have thus recovered $\mathrm{Irr}_C(C_n)$!

If $F = \mathbb{R}$, then $x^n - 1$ will generally have irreducible linear and quadratic factors, so $\mathrm{Irr}_{\mathbb{R}}(C_n)$ might contain irreducible two-dimensional representations. For example, consider the case $n = 4$. The factorization

$$x^4 - 1 = (x - 1)(x + 1)(x^2 + 1)$$

gives the simple $\mathbb{R}C_4$-modules $V_1 = \mathbb{R}[x]/(x-1)$, $V_2 = \mathbb{R}[x]/(x+1)$ and $V_3 = \mathbb{R}[x]/(x^2+1)$. The module V_3 is two-dimensional as an $\mathbb{R}$-vector space. By choosing a suitable basis, we can show that V_3 is isomorphic to the rotation-by-$\pi/2$ representation of C_4 on $\mathbb{R}^2$ (exercise!).

The situation over other fields can be more subtle. For example, if $F = \mathbb{Q}$, then the irreducible factors of $x^n - 1$ are the cyclotomic polynomials $\Phi_d(X)$ for $d \mid n$. In the special case where $n = p$ is prime, we have

$$x^p - 1 = \Phi_1(x)\Phi_p(x) = (x - 1)(x^{p-1} + x^{p-2} + \cdots + x + 1).$$

So there are two simple $\mathbb{Q}C_p$-modules: the trivial representation $V = \mathbb{Q}[x]/(x - 1)$ and a $(p - 1)$-dimensional irreducible representation $U = \mathbb{Q}[x]/(x^{p-1} + \cdots + x + 1)$.

Exercise 21.5. Prove the assertion made in the preceding example that $V = \mathbb{R}[x]/(x^2+1)$, as an $\mathbb{R}C_4$-module, is isomorphic to the rotation representation of C_4 on $\mathbb{R}^2$. ▶

21.1 Schur's Lemma

Schur's Lemma has played an important role in our earlier work. The version we had (Theorem 8.1) is the FG-module case of the following more general formulation.

Theorem 21.6 (Schur's Lemma – General Version)**.** Let M and N be simple R-modules.

(a) If $f \in \mathrm{Hom}_R(M, N)$ then f is either zero or else is an isomorphism. In particular, $\mathrm{End}_R(M)$ is a division ring.

(b) If R is an F-algebra, where F is an algebraically closed field, and if $\dim_F M < \infty$, then every $f \in \mathrm{End}_R(M)$ is of the form $f = \lambda\,\mathrm{id}$ for some $\lambda \in F$. In particular, $\mathrm{End}_R(M) \cong F$ is a field.

Proof: Identical to the proof of Theorem 8.1. ■

Remark 21.7. Part (b) fails if the simple R-module M is not finite-dimensional over F. For example, consider $F = \mathbb{C}$ and $R = M = \mathbb{C}(x)$, the field of rational functions in x viewed as a module over itself; M is a field, so it has no proper left ideals hence no proper submodules, so M is a simple R-module. On the other hand, multiplication by x is an R-module homomorphism $M \to M$ that isn't of the form $\lambda\,\mathrm{id}$.

Likewise, algebraic closure is crucial. Here is the same example we gave in Remark 8.6 but reformulated in our new language. Take $F = \mathbb{R}$, $R = \mathbb{R}[x]/(x^4 - 1) \cong \mathbb{R}C_4$ and consider the simple module $M = \mathbb{R}[x]/(x^2 + 1)$. Then multiplication by x is an endomorphism in $\mathrm{End}_R(M)$ that isn't of the form $\lambda\,\mathrm{id}$ with $\lambda \in \mathbb{R}$.

Lecture 21 Problems

21.1. Let M be an R-module, and let $m \in M$. We define the **annihilator** of m in R to be

$$\mathrm{Ann}(m) = \mathrm{Ann}_R(m) = \{r \in R \colon rm = 0\}.$$

Show that $\mathrm{Ann}(m)$ is a left ideal in R and that $R/\mathrm{Ann}(m) \cong Rm$ as R-modules.

21.2. Find an example of an R-module M such that $M = Rm$ for some nonzero $m \in M$ but M is not simple. [Hint: Take $M = F^2$ as an $F[x]$-module with an suitable action of x.]

21.3. Let M be an R-module and let N be a submodule of M. Prove that the quotient module M/N is simple if and only if N is a maximal submodule of M (in the sense that if there is a submodule L of M such that $N \subsetneq L$ then $L = M$).

21.4. Describe all simple $\mathbb{C}[x]$-modules. Show, in particular, that there are infinitely many pairwise nonisomorphic ones.

21.5. Let $R = F[x]/(f)$, where F is a field and $\deg f \geq 1$. Suppose $f(x) = p_1(x)^{a_1} \cdots p_k(x)^{a_k}$ is the factorization of f into distinct irreducibles $p_i \in F[x]$. Set $S_i := F[x]/(p_i)$.

(a) Show that S_i is a simple R-module.

(b) Show, conversely, that every simple R-module is isomorphic to some S_i.

(c) Conclude that there are k distinct simple R-modules up to isomorphism, and representatives for the isomorphism classes are given by S_i for $1 \leq i \leq k$.

21.6. Use the previous problem and the fact that $\mathbb{R}C_n \cong \mathbb{R}[x]/(x^n - 1)$ to prove:

(a) If n is odd, then $\mathrm{Irr}_{\mathbb{R}}(C_n)$ consists of the trivial representation and $\frac{n-1}{2}$ two-dimensional representations.

(b) If n is even, then $\mathrm{Irr}_{\mathbb{R}}(C_n)$ consists of two one-dimensional representations and $\frac{n-2}{2}$ two-dimensional representations.

21.7. Let p be a prime. Show that $\mathrm{Irr}_{\mathbb{F}_p}(C_p)$ consists of just the trivial representation. [See Problem 10.1 for a more general result.]

21.8. Let F be an algebraically closed field and let A be a commutative F-algebra (i.e., A is commutative as a ring). Note that every A-module is in particular an F-module (vector space) hence we can speak of its dimension. Show that every finite-dimensional simple A-module is one-dimensional.

Lecture 22 Semisimple Modules

The utility of irreducible representations comes from the fact that, in favorable circumstances, every representation is a direct sum of irreducible representations. This prompts the following definition.

Definition 22.1. An R-module M is **semisimple** if it is equal to the direct sum of simple submodules, that is, $M = \bigoplus_{i \in I} S_i$ where the S_i are simple submodules of M.

Remark 22.2.

(a) Direct sums of modules are defined just as for vector spaces. In particular, there is the notion of an internal direct sum of submodules and the notion of an external direct sum of modules; see Remark 3.15.

(b) One can equivalently define a semisimple R-module to be a module M that is isomorphic to an (external) direct sum of simple modules: $M \cong \bigoplus_{i \in I} N_i$. Indeed, if $f\colon \bigoplus_{i \in I} N_i \to M$ is an isomorphism, and if ι_i is the inclusion of N_i into $\bigoplus_{i \in I} N_i$, then $M = \bigoplus_{i \in I} f(\iota_i(N_i))$ and each $f(\iota_i(N_i))$ is a simple submodule of M.

Example 22.3.

(a) Every simple module is semisimple. The zero module is considered to be semisimple (being equal to the empty direct sum of simple submodules).

(b) If $\operatorname{char} F \nmid |G|$, then Maschke's theorem (Theorem 7.3) asserts that every FG-module V that is finite-dimensional as an F-vector space is semisimple. In fact, this is true even if V is infinite-dimensional (see Proposition 7.17 and Theorem 22.9). On the other hand, if $\operatorname{char} F$ divides $|G|$, then FG itself is *not* a semisimple FG-module (see Problem 7.2).

Exercise 22.4. Describe the semisimple F-modules and $\mathbb{Z}$-modules. ▶

In the definition of semisimplicity, we allow arbitrary (infinite) direct sums. However, here is a general result that guarantees that the sums will be finite.

Proposition 22.5. Let M be a semisimple R-module and suppose that $M = \bigoplus_{i \in I} S_i$ where the S_i are simple submodules. Then I is finite if and only if M is finitely generated.

Proof: Assume I is finite. By Proposition 21.3(b), each simple submodule S_i is generated by a single element m_i (say). Hence M is generated by the finite set $\{m_i\}_{i \in I}$.

Conversely, if M is generated by $\{m_1, \ldots, m_k\}$, then each m_i belongs to a finite sum of the S_j. Thus, the whole of M is contained in a finite sum of the S_j. Since the sum $M = \bigoplus_{i \in I} S_i$ is direct, I must be finite. ■

We now establish some useful facts about semisimple modules.

Lemma 22.6. Let M be an R-module. Assume $M = \sum_{i\in I} S_i$ is a sum (not necessarily direct) of simple R-modules. Let N be a submodule of M. Then there exists a subset $J \subseteq I$ such that

$$M = N \oplus \bigoplus_{j\in J} S_j.$$

This lemma implies, in particular, that every F-vector space has a basis. Indeed, if M is an F-module (vector space), then $M = \sum_{v\in M} \operatorname{span}\{v\}$ is a sum of simple modules (one-dimensional subspaces). Thus, applying the lemma with $N = 0$, we get that M is the direct sum of one-dimensional subspaces, hence M has a basis. So it should be no surprise that the proof of this lemma will involve some form of the Axiom of Choice!

Proof of Lemma 22.6: Use Zorn's Lemma (see Remark 22.7 below) to pick a maximal element J in

$$\begin{aligned}\mathcal{C} &= \{J \subseteq I : \text{the sum } \textstyle\sum_{j\in J} S_j \text{ is direct and } N \cap \sum_{j\in J} S_j = 0\} \\ &= \{J \subseteq I : \text{the sum } N + \textstyle\sum_{j\in J} S_j \text{ is direct}\}.\end{aligned}$$

[Details: $\mathcal{C}$ contains the empty set $J = \{\}$ so $\mathcal{C}$ is nonempty. Partially order $\mathcal{C}$ by inclusion. Let $\{J_\alpha\}_\alpha$ be a chain in $\mathcal{C}$ and consider $J' = \cup_\alpha J_\alpha \subseteq I$. Then $J' \in \mathcal{C}$ for otherwise the sum $\sum_{j\in J'} S_j$ would not be direct (since $N \cap \sum_{j\in J'} S_j = 0$ is clearly true). But then that means there is an index j_0 such that $S_{j_0} \cap \sum_{j\in J'\setminus\{j_0\}} S_j \neq 0$, hence there must be a finite set of indices in $J'\setminus\{j_0\}$ for which the former intersection also holds true and so this finite set belongs to some J_α (since $\{J_\alpha\}_\alpha$ is a chain), contradicting the fact $J_\alpha \in \mathcal{C}$. So $J' \in \mathcal{C}$ is an upper bound for $\{J_\alpha\}$. Hence, by Zorn's Lemma, $\mathcal{C}$ has a maximal element.]

We must have $N \oplus \bigoplus_{j\in J} S_j = M$. If not, then there must exist some simple S_k such that $S_k \not\subseteq N \oplus \bigoplus_{j\in J} S_j$. However, $S_k \cap N \oplus \bigoplus_{j\in J} S_j$ is either 0 or S_k since S_k is simple. The former allows us to construct a direct sum $N \oplus \bigoplus_{j\in J} S_j \oplus S_k$ which contradicts the maximality of J; the latter implies $S_k \subseteq N \oplus \bigoplus_{j\in J} S_j$. In either case, we've reached a contradiction. ■

Remark 22.7 (Zorn's Lemma). Let $(\mathcal{C}, \leq)$ be a partially ordered set. A **chain** in $\mathcal{C}$ is a subset $\{C_i\}_i \subseteq \mathcal{C}$ that is linearly ordered. An **upper bound** for the chain $\{C_i\}_i$ is an element U such that $C_i \leq U$ for all i. Zorn's Lemma states that if $\mathcal{C}$ is nonempty and if every chain in $\mathcal{C}$ has an upper bound that belongs to $\mathcal{C}$, then $\mathcal{C}$ has a **maximal element** M, that is, there exists $M \in \mathcal{C}$ such that $M \geq C$ for all $C \in \mathcal{C}$. Zorn's Lemma is equivalent to the Axiom of Choice. If you've never seen it before, the next exercise is a typical application. Be sure to attempt it and then read the solution.

Exercise 22.8. Let M be a nonzero finitely generated R-module. Show that M contains a maximal proper submodule (i.e. a proper submodule that is not contained in any other proper submodule). [Hint: Fix a generating set for M and let $\mathcal{C}$ be the set of all submodules of M that do not contain at least one of these generators.] ►

Theorem 22.9. Let M be an R-module. Then the following are equivalent.

(a) M is semisimple.

(b) M is a sum (not necessarily direct) of simple submodules.

(c) Every submodule $N \subseteq M$ has a complement in M. That is, there exists a module N' such that $M = N \oplus N'$.

(d) Every submodule of M is a sum of simple submodules.

Proof:

(a) $\Longrightarrow$ (b): Direct sums are sums.

(b) $\Longrightarrow$ (c): This follows from Lemma 22.6: Take $N' = \bigoplus_{j \in J} S_j$.

(c) $\Longrightarrow$ (d): Let N_0 be the sum of all simple modules in N. We will show that $N_0 = N$. First, by assumption there is a submodule N_0' in M such that $M = N_0 \oplus N_0'$. Hence, by Problem 22.5, there is a submodule $N_0'' \subseteq N$ such that $N = N_0 \oplus N_0''$. I claim that $N_0'' = 0$. If $N_0'' \neq 0$, pick a nonzero $x \in N_0''$ and consider the submodule $U = Rx \subseteq N_0''$. By the preceding exercise, there is a maximal submodule $V \subsetneq U$. In particular, the quotient module U/V is simple. By Problem 22.5 again, the submodule V has a complement in U, say $U = V \oplus W$, and since $W \cong U/V$, W must be simple. But now we've found a simple module W in $U \subseteq N_0'' \subseteq N$ such that $W \cap N_0 = 0$. This contradicts the fact that N_0 is the sum of all simple modules in N. Thus, our assumption that $N_0'' = 0$ must have been incorrect. Consequently, $N = N_0$, as desired.

(d) $\Longrightarrow$ (a): M is a sum of simple submodules. Hence, by Lemma 22.6 with $N = 0$, M is a direct sum of simple submodules. ■

Corollary 22.10. All submodules and quotients of a semisimple module are semisimple.

Proof: Assume M is semisimple. If $N \subseteq M$ is a submodule, then by part (d) of the proposition, N is a sum of simple submodules. Hence by the implication (b) $\Longrightarrow$ (a), N must be semisimple. On the other hand, Lemma 22.6 implies immediately that M/N is semisimple, since if $M = N \oplus \bigoplus_{j \in J} S_j$ then $M/N \cong \bigoplus_{j \in J} S_j$. ■

Corollary 22.11. If M is a semisimple R-module, say $M = \bigoplus_{i \in I} S_i$ where the S_i are simple submodules, then every simple submodule of M is isomorphic to some S_i.

Proof: Suppose S is a simple submodule of M. By Lemma 22.6, we have $M = S \oplus \bigoplus_{j \in J} S_j$ for some $J \subseteq I$. Consequently,

$$S \cong M / \bigoplus_{j \in J} S_j \cong \bigoplus_{i \in I \setminus J} S_i.$$

Since S is simple, the direct sum on the right must consist of a single summand. ■

Remark 22.12. It's important to note that the preceding corollary says that a simple submodule of M is *isomorphic to*—not equal to—some S_i. Indeed, we cannot guarantee equality. For instance, consider the semisimple $\mathbb{R}$-module $\mathbb{R}^2$. We have $\mathbb{R}^2 = S_1 \oplus S_2$ where $S_1 = \{(x, 0) : x \in \mathbb{R}\}$ and $S_2 = \{(0, y) : y \in \mathbb{R}\}$ are simple. Now consider the submodule $N = \{(x, x) : x \in \mathbb{R}\}$. It is also simple but not equal to either S_1 nor S_2.

Finally, we turn our attention to isotypic decompositions. If $M = \bigoplus_{i \in I} S_i$ is a semisimple R-module, then by grouping together the various isomorphic S_i, we can write

$$M \cong \bigoplus_{\alpha} S_\alpha^{\oplus m_\alpha},$$

where the S_α are pairwise nonisomorphic. The "multiplicity" m_α of S_α may be infinite. While it is possible to prove a uniqueness result in this generality, we will content ourself with the following finite version (compare Theorem 9.5).

Theorem 22.13 (Uniqueness of Isotypic Decompositions)**.** Let M be a finitely generated semisimple R-module and suppose that

$$M \cong \bigoplus_{i=1}^{k} S_i^{\oplus m_i} \quad \text{and} \quad M \cong \bigoplus_{j=1}^{l} T_j^{\oplus n_j},$$

where the S_i are pairwise nonisomorphic simple modules, the T_j are pairwise nonisomorphic simple modules, and m_i and n_j are finite for all i and j. Then $k = l$ and, after re-indexing if necessary, $S_i \cong T_i$ and $n_i = m_i$ for all i.

Proof: By Corollary 22.11, S_1 must be isomorphic to some T_j, say $j = 1$ (by re-indexing if necessary). Now consider $M/S_1 \cong M/T_1$ and proceed inductively. ∎

Lecture 22 Problems

22.1. Let D be a division ring. Describe all simple D-modules hence deduce that every D-module is semisimple.

22.2. Show that the following R-modules M are not semisimple.

(a) $R = \mathbb{R}[x]$ and $M = \mathbb{R}[x]/(x^3)$.

(b) $R = \mathbb{Z}$ and $M = \mathbb{Q}/\mathbb{Z}$.

(c) $R = \mathbb{C}[x]$ and $M = \mathbb{C}^2$ with x acting on M by $xe_1 = 0$, $xe_2 = e_1$. [Hint: Write down the matrix for x.]

22.3. True or false? If $N \subseteq M$ is semisimple and M/N is semisimple, then M is semisimple.

22.4. Let M be a semisimple R-module.

(a) Show that M is finitely generated if and only if every submodule of N is finitely generated.

(b) Show that part (b) is false if M is not semisimple by giving an example of a finitely generated module M and a submodule N that is not finitely generated. [Hint: Take $M = R = \mathbb{Z}[x_1, x_2, \ldots]$ and look for a suitable left ideal $N \subseteq M$.]

22.5. Let M be an R-module and let A, B, and C be submodules of M such that $C \subseteq A$. Prove:

(a) $A \cap (B + C) = (A \cap B) + C$.

(b) If there is a submodule C' such that $M = C \oplus C'$ then there is a submodule C'' such that $A = C \oplus C''$.

[So if C has a complement in M then it has a complement in every submodule of M that contains C. This observation was needed in the proof of Theorem 22.9.]

Lecture 23 The Artin–Wedderburn Theorem (Part 1)

"This extraordinary result has excited the fantasy of every algebraist and still does so in our day."

– E. Artin on Wedderburn's theorem[16]

23.1 Semisimple Rings

From the point of view of representation theory, semisimple modules are appealing because they are built out of simple modules, which perhaps are easier to study and classify. It's therefore tempting to look for rings R whose modules are all semisimple. For example, when $\operatorname{char} F \nmid |G|$, $R = FG$ is an example (by Mashcke's theorem).

Definition 23.1. A ring R is said to be **semisimple** if all R-modules are semisimple.

Recall that every ring R can be viewed as an R-module via left multiplication; this is what we had previously called the regular R-module. W denote this module by ${}_RR$ to distinguish it from the ring R. There is a subtle interplay between R and ${}_RR$. For example, we have the following (perhaps surprising) characterization of semisimplicity.

Theorem 23.2. A ring R is semisimple if and only if ${}_RR$ is a semisimple R-module.

Proof: If R is semisimple (as a ring), then by definition ${}_RR$ is semisimple. Conversely, suppose ${}_RR$ is semisimple (as a module). Note that every R-module M is a quotient of a direct sum of some of ${}_RR$. Indeed, let X be a generating set for M (for instance, take $X = M$), so that $M = \bigoplus_{x \in X} Rx$, and then define a map $f\colon \bigoplus_{x\in X} {}_RR \to M$ by $f(\sum_x r_x) = \sum_x r_x x$. This is a surjective R-module homomorphism. Thus, $M \cong (\bigoplus_{x\in X} {}_RR)/\ker f$. This proves that M is semisimple since a direct sum of semisimple modules is semisimple and a quotient of a semisimple module is semisimple (Corollary 22.10). ■

Example 23.3. Let $R = M_n(D)$ where D is a division ring. The argument in Example 21.2(e) shows that D^n is a simple R-module. For $1 \le i \le n$, let

$$C_i = \left\{ \begin{bmatrix} 0 & \cdots & * & \cdots & 0 \\ 0 & \cdots & * & \cdots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \cdots & * & \cdots & 0 \end{bmatrix} \right\} \subseteq M_n(D)$$

denote the set of matrices in $M_n(D)$ whose only nonzero entries are in the ith column. Then C_i is a left ideal in R that is isomorphic, as an R-module, to D^n. In particular, C_i

[16] E. Artin, E. *The influence of J. H. M. Wedderburn on the development of modern algebra.* Bull. American Math. Soc. **56** (1950) 65–72.

is a simple submodule of $M_n(D)$. Since $M_n(D) = C_1 \oplus \cdots \oplus C_n$ (as a module), it follows that $M_n(D)$ is a semisimple ring.

More generally, one can show that each ring R of the form $R = M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k)$, where the D_i are division rings, is semisimple (see Problem 23.6). Amazingly, the converse holds! Every semisimple ring is isomorphic to a ring of this form.

Theorem 23.4 (Artin–Wedderburn)**.** Let R be a semisimple ring. Then

$$R \cong M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k), \tag{12}$$

where the D_i are division rings.

The isomorphism (12) is called the Wedderburn decomposition of R. The integer k and the pairs (n_i, D_i) are determined uniquely up to isomorphism by R. We will state this more precisely and prove it next time. The plan for the rest of this lecture is to give a high-level outline of the proof of Theorem 23.4 followed by all the details.

23.2 Outline of the Proof

Assume R is semisimple. Then ${}_RR$ is finitely generated (by 1) and semisimple, so we have

$${}_RR \cong S_1^{\oplus n_1} \oplus \cdots \oplus S_k^{\oplus n_k}$$

for some simple modules S_i that are pairwise nonisomorphic. Next, we take the endomorphism rings of both sides to get

$$\begin{aligned}
R^{\mathrm{opp}} &\cong \mathrm{End}_R({}_RR) && \text{(Lemma 23.9)}\\
&\cong \mathrm{End}_R(S_1^{\oplus n_1} \oplus \cdots \oplus S_k^{\oplus n_k})\\
&\cong \mathrm{End}_R(S_1^{\oplus n_1}) \times \cdots \times \mathrm{End}_R(S_k^{\oplus n_k}) && \text{(Lemma 23.8)}\\
&\cong M_{n_1}(\mathrm{End}_R(S_1)) \times \cdots \times M_{n_k}(\mathrm{End}_R(S_k)). && \text{(Lemma 23.6)}
\end{aligned}$$

Set $E_i = \mathrm{End}_R(S_i)$ and take the opposite of both sides to get

$$\begin{aligned}
R &\cong (R^{\mathrm{opp}})^{\mathrm{opp}}\\
&\cong M_{n_1}(E_1)^{\mathrm{opp}} \times \cdots \times M_{n_k}(E_k)^{\mathrm{opp}}\\
&\cong M_{n_1}(E_1^{\mathrm{opp}}) \times \cdots \times M_{n_k}(E_k^{\mathrm{opp}}) && \text{(Lemma 23.5)}
\end{aligned}$$

By Schur's Lemma (Theorem 21.6(a)), $D_i := E_i^{\mathrm{opp}} = \mathrm{End}_R(S_i)^{\mathrm{opp}}$ is a division ring. This completes the proof (modulo a few lemmas).

23.3 The Details

We now supply all of the missing lemmas, starting from the bottom.

Lemma 23.5. Let D be a (possibly noncommutative) ring. Then $M_n(D^{\text{opp}}) \cong M_n(D)^{\text{opp}}$.

Proof: Define $\tau\colon M_n(D^{\text{opp}}) \to M_n(D)^{\text{opp}}$ by $\tau(A) = A^T$. It's clear that $\tau(A+B) = \tau(A) + \tau(B)$. The fact that $\tau(AB) = \tau(A)\tau(B)$ comes from the identity

$$(AB)^T = B^T A^T = A^T * B^T,$$

where $*$ is the (opposite) multiplication in $M_n(D)^{\text{opp}}$. Be careful to note that, for this identity to hold, the entries in AB must use the product in D^{opp} and not in D. ■

The next lemma is a generalization of the familiar linear algebra fact that

$$\text{End}_F(F^n) = M_n(F).$$

Lemma 23.6. Let S be an R-module. Then $\text{End}_R(S^{\oplus n}) \cong M_n(\text{End}_R(S))$.

Proof: Let $\iota_j\colon S \to S^{\oplus n}$ be the inclusion into the jth component and let $\pi_i\colon S^{\oplus n} \to S$ be the projection onto the ith component. These are module homomorphisms. For $f \in \text{End}_R(S^{\oplus n})$, set $f_{ij} = \pi_i \circ f \circ \iota_j \in \text{End}_R(S)$. The map

$$\begin{aligned} \text{End}_R(S^{\oplus n}) &\to M_n(\text{End}_R(S)) \\ f &\mapsto [f_{ij}] \end{aligned}$$

is clearly a homomorphism of rings. It is in fact an isomorphism (exercise). ■

Exercise 23.7. Describe the inverse to the map $\text{End}_R(S^{\oplus n}) \to M_n(\text{End}_R(S))$ given in the preceding proof. ▶

Lemma 23.8. Let $S_1, \dots, S_k$ be pairwise nonisomorphic simple R-modules. Then

$$\text{End}_R(S_1^{\oplus n_1} \oplus \cdots \oplus S_k^{\oplus n_k}) \cong \text{End}_R(S_1^{\oplus n_1}) \times \cdots \times \text{End}_R(S_k^{\oplus n_k}).$$

Proof: Let $V_i = S_i^{\oplus n_i}$. Let $\iota_j\colon V_j \to V_1 \oplus \cdots \oplus V_n$ be the inclusion into the jth component, and let $\pi_i\colon V_1 \oplus \cdots \oplus V_n \to V_i$ be the projection onto the ith component. Given f in $\text{End}_R(\oplus_i V_i)$, set $f_{ij} = \pi_i \circ f \circ \iota_j \in \text{Hom}_R(V_j, V_i)$. We have an isomorphism

$$\begin{aligned} \text{End}_R(\oplus_i V_i) = \text{Hom}_R(\oplus_j V_j, \oplus_i V_i) &\to \oplus_{j,i} \text{Hom}_R(V_j, V_i) \\ f &\mapsto (f_{ij}) \end{aligned}$$

of additive groups. However, by Schur's Lemma, $\text{Hom}_R(V_i, V_j) = 0$ if $i \neq j$. Thus, the above isomorphism restrict to an isomorphism

$$\begin{aligned} \text{End}_R(\oplus_i V_i) \to \oplus_i \text{Hom}_R(V_i, V_i) &= \oplus_i \text{End}_R(V_i) \\ f &\mapsto (f_{11}, \dots, f_{kk}) \end{aligned}$$

This is in fact an isomorphism of rings. The key point is that $\pi_j \circ \iota_j = \text{id}$ so $f_{jj} \circ g_{jj} = \pi_j \circ f \circ g \circ \iota_j = (f \circ g)_{jj}$. ■

Lemma 23.9. Let R be a ring. Then $\mathrm{End}_R({}_RR) \cong R^{\mathrm{opp}}$.

Proof: Define $\varphi\colon \mathrm{End}_R({}_RR) \to R^{\mathrm{opp}}$ by $T(f) = f(1)$. Clearly φ is additive, and since

$$\varphi(f \circ g) = f(g(1)) = f(g(1)1) = g(1)f(1) = \varphi(g)\varphi(f)$$

we see that φ is multiplicative if R is given the opposite multiplication. The inverse map is given by $\psi(r) =$ right multiplication by r (so $\psi(r)(x) = xr$). I'll let you fill in the details. ■

The proof of the Artin–Wedderburn theorem is now complete!

Lecture 23 Problems

23.1. Show that none of the following rings are semisimple.

(a) $\mathbb{Z}$.

(b) $\mathbb{R}[x]$.

(c) $\mathbb{F}_pG$, where $p \mid |G|$.

23.2. Show that a commutative ring R is semisimple if and only if R is isomorphic to a finite product of fields.

23.3. Let R be a semisimple ring and let M be a finitely generated R-module. Show that $\mathrm{End}_R(M)$ is semisimple.

23.4. Let R be a ring.

(a) Show that $M_n(M_m(R)) \cong M_{mn}(R)$ as rings.

(b) Show that if R is semisimple then $M_n(R)$ is semisimple.

23.5. Let $R = R_1 \times \cdots \times R_k$ be a product of rings. For $1 \le i \le k$, let $e_i = (0, \ldots, 1, \ldots, 0)$ (1 in the ith spot).

(a) Let M_i be an R_i-module M_i. Show that setting $(a_1, \ldots, a_k)m := a_i m$ turns M_i into an R-module which is simple if M_i is simple as an R_i-module.

(b) Conversely, let M be an R-module and set $M_i = e_iM$. Show that M_i is an R_i-module. If M is simple as an R-module, show that there is exactly one $i \in \{1, \ldots, k\}$ such that $M_i \neq 0$ and, for that i, M_i is a simple R_i-module.

(c) Deduce that every simple R-module is obtained from a simple R_i-module M_i as described in part (a).

23.6. Show that a product of rings $R_1 \times \cdots \times R_k$ is semisimple if and only if each factor R_i is semisimple. [Use the previous problem.]

23.7. Let $f \in F[x]$ have $\deg f \ge 2$ and suppose $f = p_1^{a_1} \cdots p_k^{a_k}$ is its factorization into distinct irreducibles $p_i \in F[x]$. Show that $R = F[x]/(f)$ is semisimple if and only if $a_1 = \cdots = a_k = 1$. [Hint: Use the Chinese Remainder Theorem to reduce to $R = F[x]/(p(x)^a)$. For $a \ge 2$, you know what all the submodules of ${}_RR$ look like.]

Appendix A: Solutions to Exercises

Lecture 1

1.4. Suppose C_n is generated by a. It suffices to determine where to send a, and all we need to guarantee is that $\rho(a)^n = 1$. The natural candidate is the rotation-by-$2\pi/n$ matrix. Explicitly: Define

$$\rho(a) = \begin{bmatrix} \cos(2\pi i/n) & -\sin(2\pi i/n) \\ \sin(2\pi i/n) & \cos(2\pi i/n) \end{bmatrix}$$

It follows that we should define $\rho(a^k)$ by

$$\rho(a^k) = \rho(a)^k = \begin{bmatrix} \cos(2\pi ik/n) & -\sin(2\pi ik/n) \\ \sin(2\pi ik/n) & \cos(2\pi ik/n) \end{bmatrix}$$

and from this we can easily see that ρ is injective.[17] ◀

1.5. For instance, the dihedral group D_{2n} acts on a regular n-gon by symmetries; $\mathbb{Z}$ act on $\mathbb{R}$ by translation (so n sends x to $x+n$); if V is an F-vector space, then $F^\times$ acts on V by scaling. There are plenty of other examples. ◀

1.8. Only the group action of G on itself is necessarily faithful.

The trivial action is obviously not faithful if $G \neq \{e\}$.

If G acts on H by conjugation, then anything in the centre of G will act trivially. So if G has non-trivial centre, then this action is not faithful.

Finally, in the action of G on G/H, anything in the intersection $\cap_x xHx^{-1}$ of all conjugates of H will act trivially. Indeed, if $g \in \cap_x xHx^{-1}$, then for each $x \in G$ we can write $g = xhx^{-1}$ for some $h \in H$. Thus, $g(xH) = xhx^{-1}xH = xhH = xH$. So if the intersection $\cap_x xHx^{-1}$ is non-trivial—which it may be (e.g. consider an abelian G)—then the action of G won't be faithful. ◀

1.10. Suppose G acts on X. To show that α is a homomorphism, we observe that

$$\alpha(gh)(x) = (gh)x = g(hx) = \alpha(g)(\alpha(h)x).$$

Thus, $\alpha(gh) = \alpha(g) \circ \alpha(h)$. The kernel of α consists of all $g \in G$ such that $\alpha(g)$ is the identity map on X, which is the case iff

$$gx = x \text{ for all } x \in X.$$

Thus, $\ker(\alpha)$ is trivial iff the action of G is faithful.

Conversely, if α is a homomorphism, and if we define gx by $\alpha(g)(x)$, then

$$ex = \alpha(e)(x) = x$$

[17] Click on ◀ to go to back to the exercise.

since $\alpha(e)$ must be the identity bijection $X \to X$. Next,

$$(gh)x = \alpha(gh)(x) = (\alpha(g) \circ \alpha(h))(x) = \alpha(g)(\alpha(h)(x)) = g(hx).$$

So our definition of gx satisfies the axioms for a group action. ◀

Lecture 2

2.4. Let $T\colon V \to W$ be a G-linear bijection. Since the inverse of a linear map is linear, it suffices to show that $T^{-1}\colon W \to V$ satisfies

$$T^{-1}(gw) = gT^{-1}(w) \quad \text{for all } g \in G \text{ and } w \in W.$$

To this end, note that $T(gT^{-1}(w)) = gT(T^{-1}(w)) = gw = T(T^{-1}(gw))$. Since T is injective, we're done. ◀

2.10. Let $\widetilde{A} = \varphi(a)$ and $\widetilde{B} = \varphi(b)$. A moment's thought will convince you that these are, resp., the matrices of the $2\pi/3$-rotation and reflection in the x-axis in the standard basis. Thus, $\widetilde{A}^3 = \widetilde{B}^2 = I$ and we can verify by direct computation that $\widetilde{B}\widetilde{A}\widetilde{B} = \widetilde{A}^2$, but actually this will follow from what we're going to do next (plus the fact that we know that $BAB = A^2$).

To show that $\rho \cong \varphi$, we just need to find a matrix C such that

$$A = C\widetilde{A}C^{-1} \quad \text{and} \quad B = C\widetilde{B}C^{-1}.$$

The natural candidate here is the change of basis matrix from the standard basis to the basis $\{v, u\}$, namely $C = \begin{bmatrix} 1 & -1/2 \\ 0 & \sqrt{3}/2 \end{bmatrix}$. I will let you compute and confirm that this works. Incidentally, we get

$$\widetilde{B}\widetilde{A}\widetilde{B} = (C^{-1}BC)(C^{-1}AC)(C^{-1}BC) = C^{-1}BABC = C^{-1}A^2C = \widetilde{A}^2,$$

confirming that φ is indeed a representation. ◀

Lecture 3

3.3. Suppose $X = \{x_1, \ldots, x_n\}$. For each i, let $e_i = e_{x_i}$ be the indicator function at x_i. The set $\{e_1, \ldots, e_n\}$ forms a basis for $\mathcal{F}(X, F)$. In fact, each $f \in \mathcal{F}(X, F)$ is given by

$$f = f(x_1)e_1 + \cdots + f(x_n)e_n.$$

We can define a vector space isomorphism $T\colon \mathcal{F}(X, F) \to F[X]$ by sending the basis vector e_i to the basis vector x_i. Explicitly, for $f \in \mathcal{F}(X, F)$, we define

$$T(f) = f(x_1)x_1 + \cdots + f(x_n)x_n.$$

Let's check that T is G-linear. First note that for $f \in \mathcal{F}(X, F)$, we have

$$\begin{aligned}(gf)(x) &= f(g^{-1}x) \\ &= f(g^{-1}x_1)e_1 + \cdots + f(g^{-1}x_n)e_n\end{aligned}$$

Thus,

$$\begin{aligned}T(gf) &= f(g^{-1}x_1)x_1 + \cdots + f(g^{-1}x_n)x_n \\ &= f(g^{-1}x_1)(gg^{-1}x_1) + \cdots + f(g^{-1}x_n)(gg^{-1}x_1) \\ &= g(f(g^{-1}x_1)(g^{-1}x_1) + \cdots + f(g^{-1}x_n)(g^{-1}x_1)).\end{aligned} \tag{13}$$

Since the map $x \mapsto g^{-1}x$ is a bijection of X, we see that

$$\sum_{i=1}^{n} f(g^{-1}x_i)(g^{-1}x_i) = \sum_{x \in X} f(x)x = \sum_{i=1}^{n} f(x_i)x_i.$$

Hence, (13) gives $T(gf) = gT(f)$, as desired. ◀

3.6. Letting $C_4 = \{1, a, a^2, a^3\}$, we have

$$r(1) = \begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix},\ r(a) = \begin{bmatrix}0&0&0&1\\1&0&0&0\\0&1&0&0\\0&0&1&0\end{bmatrix},\ r(a^2) = \begin{bmatrix}0&0&1&0\\0&0&0&1\\1&0&0&0\\0&1&0&0\end{bmatrix},\ r(a^3) = \begin{bmatrix}0&1&0&0\\0&0&1&0\\0&0&0&1\\1&0&0&0\end{bmatrix}.$$

These are examples of *circulant* matrices, i.e., matrices whose columns are cyclic permutations of the first column. ◀

3.9. The containment $gU \subseteq U$ follows by definition. Conversely, if $u \in U$, then $u = g(g^{-1}u)$ is in gU too. ◀

3.12. If $x \in \ker(T)$ then $gx \in \ker(T)$ too since $T(gx) = gT(x) = g0 = 0$. Likewise, if $y \in \operatorname{im}(T)$ so that $y = T(x)$ for some $x \in V$, then $gy = gT(x) = T(gx)$ is in $\operatorname{im}(T)$ too. ◀

3.17. In terms of the duality pairing $\langle\ ,\ \rangle \colon V \times V^* \to F$, we have

$$\langle \rho(g)v, \rho^*(g)f \rangle = \langle v, f \rangle \quad \Longleftrightarrow \quad \left\langle v, \rho(g)^t \rho^*(g)f \right\rangle = \langle v, f \rangle.$$

Thus, $\rho(g)^t = \rho^*(g)^{-1}$.

Alternatively, here is the direct proof. The (i, j)th entry of $r^*(g)$ is

$$(ge_j^*)(e_i) = e_j^*(g^{-1}e_i).$$

To determine $g^{-1}e_i$, we can look at the ith column of $r(g^{-1}) = [r_{ij}(g^{-1})]$, which tells us that

$$g^{-1}e_i = \sum_{k=1}^{n} r_{ki}(g^{-1})e_k.$$

Thus,

$$e_j^*(g^{-1}e_i) = e_j^*\left(\sum_{k=1}^{n} r_{ki}(g^{-1})e_k\right) = \sum_{k=1}^{n} r_{ki}(g^{-1})e_j^*(e_k) = r_{ji}(g^{-1}).$$

This shows that the (i, j)th entry of $r^*(g)$ is the (j, i)th entry of $r(g^{-1})$, which is exactly what we wanted to prove. ◀

Lecture 4

4.2. We have

$$v \otimes 0 = v \otimes (0 \cdot 0) = 0v \otimes 0 = 0 \otimes 0.$$

The other one is similar. ◀

4.6. An arbitrary tensor in $V_{\mathbb{C}}$ is of the form

$$\sum_{j=1}^{k}(a_j + ib_j) \otimes v_j = \sum_{j=1}^{k} a_j \otimes v_j + \sum_{j=1}^{k} ib_j \otimes v_j = 1 \otimes \sum_{j=1}^{k} a_j v_j + i \otimes \sum_{j=1}^{k} b_j v_j,$$

where $a_j, b_j \in \mathbb{R}$ and $v_j \in V$. Setting $v = \sum_{j=1}^{k} a_j v_j$ and $u = \sum_{j=1}^{k} b_j v_j$, we obtain the desired form. ◀

4.15. Let $T\colon V \to U$ and $S\colon W \to Z$ be linear maps. Let $\mathcal{B}_V, \mathcal{B}_U, \mathcal{B}_W$ and $\mathcal{B}_Z$ be bases for the indicated vector spaces. Let $\mathcal{B}_{V\otimes W}$ and $\mathcal{B}_{U\otimes Z}$ be the corresponding bases for $V \otimes W$ and $U \otimes Z$ as in Theorem 4.10. The claim here is that the $(\mathcal{B}_{V\otimes W}, \mathcal{B}_{U\otimes Z})$-matrix of $T \otimes S$ is equal to the Kronecker product of the $(\mathcal{B}_V, \mathcal{B}_U)$-matrix of T and the $(\mathcal{B}_W, \mathcal{B}_Z)$-matrix of S. (Of course, we have to explain how all these bases are ordered.)

To ease notation, I will sketch the main idea for the case where V, W, U and Z are 2-dimensional. Suppose $\mathcal{B}_V = \{v_1, v_2\}, \mathcal{B}_U = \{u_1, u_2\}, \mathcal{B}_W = \{w_1, w_2\}$ and $\mathcal{B}_Z = \{z_1, z_2\}$. Let

$$\begin{aligned}
\mathcal{B}_{V\otimes W} &= \{v_1 \otimes w_1, v_1 \otimes w_2, v_2 \otimes w_1, v_2 \otimes w_2\} \\
\mathcal{B}_{U\otimes Z} &= \{u_1 \otimes z_1, u_1 \otimes z_2, u_2 \otimes z_1, u_2 \otimes z_2\}
\end{aligned}$$

where we are viewing these as ordered bases. Let's work out the second column of the $(\mathcal{B}_{V\otimes W}, \mathcal{B}_{U\otimes Z})$-matrix $[T \otimes S]$ of $T \otimes S$. We must determine $(T \otimes S)(v_1 \otimes w_2) = T(v_1) \otimes S(w_2)$. If $A = [a_{ij}]$ is the $(\mathcal{B}_V, \mathcal{B}_U)$-matrix of T and $B = [b_{ij}]$ is the $(\mathcal{B}_W, \mathcal{B}_Z)$-matrix of S, we get:

$$\begin{aligned}
T(v_1) \otimes S(w_2) &= (a_{11}u_1 + a_{21}u_2) \otimes (b_{12}z_1 + b_{22}z_2) \\
&= a_{11}b_{12}(u_1 \otimes z_1) + a_{11}b_{22}(u_1 \otimes z_2) + a_{21}b_{12}(u_2 \otimes z_1) + a_{21}b_{22}(u_2 \otimes z_2).
\end{aligned}$$

Thus, the second column of $[T \otimes S]$ is

$$\begin{bmatrix} a_{11}b_{12} \\ a_{11}b_{22} \\ a_{21}b_{12} \\ a_{21}b_{22} \end{bmatrix}.$$

This is indeed the second column of

$$A \otimes B = \begin{bmatrix} a_{11}B & a_{12}B \\ a_{21}B & a_{21}B \end{bmatrix},$$

as desired. ◀

Lecture 5

5.1. Observe that $f \in \mathrm{Hom}(V, W)$ is fixed by $g \in G$ if and only

$$f(v) = (gf)(v) = gf(g^{-1}v) \text{ for all } v \in V,$$

or, equivalently, if and only if

$$f(g^{-1}v) = g^{-1}f(v) \text{ for all } v \in V.$$

Thus, f is fixed by *all* $g \in G$ if and only if f is G-invariant, which is exactly what we wanted to prove. ◀

5.3. With notation as in the proof of Theorem 5.2, an arbitrary tensor in $z \in V^* \otimes W$ can be written in the form $z = \sum_{i,j} a_{ij} e_i^* \otimes f_j$ for some $a_{ij} \in F$. Suppose now that $T(z) = 0$. Then, for all $v \in V$, we have

$$0 = T(z)(v) = \sum_{i,j} a_{ij} T(e_i^* \otimes f_j)(v) = \sum_{i,j} a_{ij} e_i(v) f_j.$$

In particular, for $v = e_k$, we get

$$0 = \sum_j a_{kj} f_j.$$

Since the f_j are independent, it follows that $a_{kj} = 0$ for all j; and for all k too since k was arbitrary. Thus, $z = 0$, which proves that $\ker T = 0$, as desired. ◀

5.5. Viewing A and B as operators on $V = F^n$, hence as tensors in $V^* \otimes V$, what we must do now is try to understand the tensors corresponding to the compositions $A \circ B$ and $B \circ A$. Let's figure out what happens in the case where $A = f \otimes v$ and $B = g \otimes w$ are pure tensors. Recall that the tensor $g \otimes w$ gives the linear map $u \mapsto g(u)w$. Applying $f \otimes v$ to this, we get $f(g(u)w)v = g(u)f(w)v$. Thus, the composition $(f \otimes v) \circ (g \otimes w)$ sends u to $g(u)f(w)v$. In other words,

$$(f \otimes v) \circ (g \otimes w) = g \otimes (f(w)v).$$

Consequently,

$$\mathrm{tr}(A \circ B) = \tau(g \otimes (f(w)v)) = g(f(w)v) = f(w)g(v).$$

Similarly, you can show that

$$(g \otimes w) \circ (f \otimes v) = f \otimes (g(v)w)$$

and therefore

$$\mathrm{tr}(B \circ A) = \tau(f \otimes (g(v)w)) = f(g(v)w) = g(v)f(w).$$

This shows that $\mathrm{tr}(AB) = \mathrm{tr}(BA)$ in the case of pure tensors. The general case follows from this since trace is linear and every tensor is the sum of pure tensors. ◀

Lecture 6

6.6. We can calculate the eigenspaces directly, but here is an alternative approach. Since $A^3 = I$, the eigenvalues λ of A must satisfy $\lambda^3 = I$. Likewise, the eigenvalues μ of B satisfy $\mu^2 = 1$. Since A has no real eigenvalues (it's a $2\pi/3$-rotation), it follows that $\lambda \neq 1$ must be a primitive third root of unity. Now suppose $Av = \lambda v$ and $Bv = \mu v$ where v is a non-zero common eigenvector. From $AB = BA^2$ we get

$$ABv = BA^2v \implies \lambda\mu v = \lambda^2\mu v \implies \lambda = 1.$$

Contradiction! ◀

6.8. Suppose W were to contain the 1-dimensional S_3-invariant subspace W_0 spanned by $v = a\mathbf{1} + b\mathbf{2} + c\mathbf{3}$, where $a + b + c = 0$. Then $\pi v \in W_0$ for all $\pi \in S_3$. In particular, $(1\ 3\ 2)v \in W_0$, so

$$b\mathbf{1} + c\mathbf{2} + a\mathbf{3} = \alpha(a\mathbf{1} + b\mathbf{2} + c\mathbf{3})$$

for some $\alpha \in F$. From this we get $b = \alpha a$ and $a = \alpha b$ hence $a = \alpha^2 a$. If $a = 0$ then $b = 0$ hence $c = -a - b = 0$, which is impossible since $v \neq 0$. So $a \neq 0$. Now consider $(2\ 3)v$ to get

$$a\mathbf{1} + c\mathbf{2} + b\mathbf{3} = \beta(a\mathbf{1} + b\mathbf{2} + c\mathbf{3})$$

for some $\beta \in F$. This gives $a = \beta a$ hence $\beta = 1$ and therefore $b = c = -a - b$. From earlier, we have $b = \alpha a$ where $\alpha^2 = 1$. Combining all this, we get

$$-a = 2b = 2\alpha a \implies -1 = 2\alpha \implies 1 = 4\alpha^2 \implies 1 = 4.$$

This is a contradiction if $\operatorname{char} F \neq 3$.

Now assume that $F = \mathbb{R}$. Let $a = (1\,2\,3)$ and $b = (1\,2)$; and keep in mind that these elements generate S_3. In order to prove that W is isomorphic to the standard representation, we can: pick a basis for W, write down the matrices A' and B' for a and b in this basis, and then try to show that there is an invertible matrix S such that $SA'S^{-1} = A$ and $SB'S^{-1} = B$, where A and B are the matrices of a and b in the standard representation given in Example 2.9. Alternatively, it suffices to give a basis for W for which the matrices A' and B' end up being *equal* to A and B. Here is such a basis: $\mathcal{B} = \{\mathbf{1} + \mathbf{2} + (-2)\mathbf{3}, (-2)\mathbf{1} + \mathbf{2} + \mathbf{3}\}$. I will let you confirm. ◀

6.10. Working with the given basis $\{v_i, bv_i\}$, we see that b acts via the matrix

$$r(b) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

On the other hand, since $av_i = \omega v_i$ and $a(bv_i) = \omega^2 v_i$, a acts via the matrix

$$r(a) = \begin{bmatrix} \omega & 0 \\ 0 & \omega^2 \end{bmatrix}.$$

In Problem 2.10, we saw that V_{std} has a matrix representation given by

$$\varphi(a) = \begin{bmatrix} \cos(2\pi/3) & -\sin(2\pi/3) \\ \sin(2\pi/3) & \cos(2\pi/3) \end{bmatrix} \quad \text{and} \quad \varphi(b) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

If we diagonalize $\varphi(a)$, we will end up with $r(a)$, and it turns out that this change of basis turns $\varphi(b)$ into $r(b)$. Explicitly, let

$$A = \begin{bmatrix} 1 & 1 \\ -i & i \end{bmatrix}.$$

I'll let you confirm that

$$Ar(a)A^{-1} = \varphi(a) \quad \text{and} \quad Ar(b)A^{-1} = \varphi(b).$$

Thus, the matrix representations r and φ are equivalent, and therefore $W_i \cong V_{\text{std}}$. ◀

Lecture 7

7.2. Suppose $T\colon \oplus_i U_i \to V$ is a G-linear isomorphism, where the U_i are irreducible G-modules. Let $W_i := T(U_i)$. Then W_i is an irreducible G-submodule of V and it's easy to check that $V = \oplus_i W_i$. Conversely, if V is a direct sum of irreducible submodules, then the identity map is a G-linear isomorphism from V to a direct sum of irreducible G-modules. ◀

7.8. Suppose $x \in U^\perp$. We want to show that $\langle gx, u\rangle = 0$ for all $u \in U$ and $g \in G$. Since U is a G-module, each $g \in G$ acts as an invertible linear map on U, so given $u \in U$ we can write $u = gu'$ for some $u' \in U$ (depending on g). Consequently,

$$\langle gx, u\rangle = \langle gx, gu'\rangle = \langle x, u'\rangle = 0,$$

as desired. ◀

7.12. Let's replace the dot product on $\mathbb{R}^2$ with the inner product

$$\begin{aligned}\left\langle \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}, \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} \right\rangle &= \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \cdot \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} + \left(\begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}\right) \cdot \left(\begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} y_1 \\ y_2 \end{bmatrix}\right) \\ &= \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \cdot \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} + \begin{bmatrix} x_1 + x_2 \\ -x_2 \end{bmatrix} \cdot \begin{bmatrix} y_1 + y_2 \\ -y_2 \end{bmatrix} \\ &= 2(x_1y_1 + x_2y_2) + x_1y_2 + x_2y_1 + x_2y_2\end{aligned}$$

as in the proof of Weyl's unitary trick (except I've dropped the factor $1/|C_2|$). Using this inner product, we can determine that the orthogonal complement of $U = \operatorname{span}(1, 0)$ is $U^\perp = \operatorname{span}(1, -2)$. This subspace is indeed C_2-invariant—in fact, $(1, -2)$ is an eigenvector of $\rho(a) = \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix}$. ◀

Lecture 8

8.5. Suppose (V, ρ) is irreducible. Each $\rho(g)$ is diagonalizable. Since G is abelian, we have

$$\rho(g)\rho(h) = \rho(gh) = \rho(hg) = \rho(h)\rho(g),$$

so the set $\{\rho(g) \colon g \in G\}$ is a commuting family of diagonalizable operators. So we can write $V = \oplus E_\lambda$ as a direct sum of simultaneous eigenspaces. In particular, there exists a non-zero simultaneous eigenvector $v \in V$. Hence $U = \operatorname{span}\{v\}$ is G-invariant subspace of V and so must be equal to V itself. Thus, $\dim V = \dim U = 1$. ◀

Lecture 9

9.10. The standard matrix of a in the regular representation is $A = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. The eigenvalues ± 1 each occur with multiplicity equal to 1. Thus, $(n, m) = (1, 1)$ in this case. For (ii), a quick inspection shows that $V_+ = \operatorname{span}\{(1, 1, 0), (0, 0, 1)\}$ and $V_- = \operatorname{span}\{(1, -1, 0)\}$. Thus, $(n, m) = (2, 1)$. ◀

Lecture 10

10.4. We have

$$\langle \delta_g, \delta_h \rangle = \frac{1}{|G|} \sum_{x \in G} \delta_g(x)\delta_h(x).$$

If $g \neq h$, then $\delta_g(x)\delta_h(x) = 0$ for all $x \in G$, and the result follows. ◀

10.9. Part (a) holds because $\chi(g)$ is a root of unity. Parts (b) and (c) are direct computations. Finally, we have

$$\chi(g)\overline{\psi(g)} = 1 \quad \iff \quad \chi(g)\psi(g)^{-1} = 1 \quad \iff \quad \chi(g) = \psi(g).$$

So if $\chi \neq \psi$ then $\chi\overline{\psi}$ is non-trivial. ◀

Lecture 11

11.9. The forward direction is Proposition 8.4.

Conversely, if all of the irreps of G are one-dimensional, and if say there are r of them, then the dimension formula implies that $r = |G|$. On the other had, Proposition 11.8 implies that $r = |G/[G, G]|$. It follows that $|G/[G, G]| = |G|$ so $[G, G]$ must be trivial and therefore G must be abelian. ◀

11.12. Every element in D_8 is of the form $a^i b^j$ for some $i \in \{0,1,2,3\}$ and $j \in \{0,2\}$. This shows that $|D_8| = 8$. By direct calculation, we find that the conjugacy classes are:

$$\{e\}, \{a^2\}, \{a, a^3\}, \{b, a^2b\}, \{ab, a^3b\}.$$

Another direct calculation shows that the commutator of any two elements is either e or a^2—for example,

$$[a^2, ab] = a^2(ab)a^{-2}(ab)^{-1} = a^3ba^{-2}ba^{-1} = a^{3+2-1} = e.$$

Thus, $[D_8, D_8] = \{e, a^2\}$. Finally, we know that $D_8/[D_8, D_8]$ has order 4; and since the cosets $a[D_8, D_8]$, $b[D_8, D_8]$ and $ab[D_8, D_8]$ are distinct and have order 2, we conclude that $D_8/[D_8, D_8] \cong C_2 \times C_2$. ◀

Lecture 12

12.1. Take two trivial representations of different degrees. For something more interesting, note first that $\det \circ \rho$ is a one-dimensional representation. So let's look for a group G with few one-dimensional representations. For instance, take $G = A_5$. Then since $A_5 = [A_5, A_5]$, the only one-dimensional representation of A_5 is the trivial representation (by Proposition 11.8). So *all* representations of A_5 have the same determinant! ◀

12.3. If $n = 2$, then

$$p(x) = x^2 - (\lambda_1 + \lambda_2)x + \lambda_1\lambda_2$$

and

$$\lambda_1\lambda_2 = \frac{1}{2}\left[(\lambda_1 + \lambda_2)^2 - (\lambda_1^2 + \lambda_2^2)\right],$$

gives us the constant term.

Next, if $n = 3$, we have

$$p(x) = x^3 - (\lambda_1 + \lambda_2 + \lambda_3)x^2 + (\lambda_1\lambda_2 + \lambda_2\lambda_3 + \lambda_1\lambda_3)x - \lambda_1\lambda_2\lambda_3,$$

and

$$\begin{aligned}
\lambda_1\lambda_2 + \lambda_2\lambda_3 + \lambda_1\lambda_3 &= \frac{1}{2}\left[(\lambda_1 + \lambda_2 + \lambda_3)^2 - (\lambda_1^2 + \lambda_2^2 + \lambda_3^2)\right] \\
\lambda_1\lambda_2\lambda_3 &= \frac{1}{6}(\lambda_1 + \lambda_2 + \lambda_3)^3 + \frac{1}{3}(\lambda_1^3 + \lambda_2^3 + \lambda_3^3) - \frac{1}{2}(\lambda_1 + \lambda_2 + \lambda_3)(\lambda_1^2 + \lambda_2^2 + \lambda_3^2),
\end{aligned}$$

as desired. ◀

12.8. The standard basis of V is the set $X = \{x_1, \ldots, x_n\}$ itself. If $gx_i = x_j$ then the ith column of the standard matrix of $\rho(g)$ will have a 1 in the jth component and zeroes elsewhere. In particular, the only way to get a non-zero entry in the (i, i) position is if $gx_i = x_i$, in which case the non-zero entry is equal to 1. ◀

Lecture 13

13.4. Let $U = \operatorname{im} P$ and $W = \ker P$ so that $V = \operatorname{im} P \oplus \ker P$. Choose bases for U and W and combine them to form the basis $\mathcal{B}$ for V. The matrix of P in this basis is given by

$$[P]_{\mathcal{B}} = \begin{bmatrix} I_d & 0 \\ 0 & 0 \end{bmatrix},$$

where I_d the identity matrix of size $d = \dim U$. Thus, $\operatorname{tr}(P) = \operatorname{tr}(I_d) = d$, as required. ◀

13.10. (This was Problem 6.5.) First, $V_{\text{std}} \otimes V_{\text{sgn}}$ is irreducible (being the tensor product of an irreducible representation and a 1-dimensional representation). Second, $\dim V_{\text{std}} \otimes V_{\text{sgn}} = 2$. However, V_{std} is the only 2-dimensional irreducible $\mathbb{C}S_3$-module (up to isomorphism). It is also possible to tackle this problem via computation with 2×2 matrices. ◀

13.12. Answer: $V_{\text{std}}^{\otimes 3} = V_{\text{triv}} \oplus V_{\text{sgn}} \oplus V_{\text{std}}^{\oplus 3}$. ◀

Lecture 14

14.3. This follows from our irreducibility criterion in Corollary 13.7 plus the fact that $\langle \chi_V, \chi_V \rangle = \langle \chi_{V^*}, \chi_{V^*} \rangle$. It is also possible to give a proof without using character theory (as you were asked to do in Problem 6.6(a)!). ◀

14.7. Let $V, W \in \operatorname{Irr}_{\mathbb{C}}(G)$. Choose unitary matrix representations $r\colon G \to GL_n(\mathbb{C})$ and $s\colon G \to GL_m(\mathbb{C})$ for V and W. Then

$$\chi_V = \sum_{i=1}^{n} r_{ii} \quad \text{and} \quad \chi_W = \sum_{j=1}^{m} s_{jj}.$$

Therefore,

$$\begin{aligned} \langle \chi_V, \chi_W \rangle &= \frac{1}{|G|} \sum_{g \in G} \chi_V(g) \overline{\chi_W(g)} \\ &= \frac{1}{|G|} \sum_{g \in G} \sum_{i=1}^{n} \sum_{j=1}^{m} r_{ii}(g) \overline{s_{jj}(g)} \\ &= \sum_{i,j} \langle r_{ii}, s_{jj} \rangle . \end{aligned}$$

If $V \ncong W$ then $\langle r_{ii}, s_{jj} \rangle = 0$ for all i, j and so in this case $\langle \chi_V, \chi_W \rangle = 0$. On the other hand, if $V \cong W$, we can (and will) choose identical matrix representations for V and W so that $r = s$ and $n = m = \dim V$. In this case, the second orthogonality relation reduces our calculation above to

$$\langle \chi_V, \chi_W \rangle = \sum_{i,j} \frac{\delta_{ij}}{\dim V} = \sum_{i=1}^{n} \frac{1}{\dim V} = 1,$$

exactly as in Theorem 14.1. ◀

Lecture 15

15.3. Suppose $C_2 \times C_2 = \{e, a, b, ab\}$. Then:

	e	a	b	ab
$\chi_{1,1}$	1	1	1	1
$\chi_{1,-1}$	1	1	-1	-1
$\chi_{-1,1}$	1	-1	1	-1
$\chi_{-1,-1}$	1	-1	-1	1

(See Example 10.8.) ◀

Lecture 16

16.2. The conjugacy class of π consists of all permutations with the same cycle type as π. There are $n!$ ways of writing down the integers $1, 2, \dots, n$ into the cycles. For example, if we have one 2-cycle and one 1-cycle, then the possibilities are

$$(1\ 2)(3), (1\ 3)(2), (2\ 1)(3), \text{ etc.}$$

Some of these give the same element of S_n. For example, $(1\ 2)(3) = (2\ 1)(3)$.

Each i-cycle can be written in i different ways. For example,

$$(a\ b\ c) = (b\ c\ a) = (c\ a\ b)$$

are the three different ways of writing the 3-cycle $(a\ b\ c)$. If there are multiple i-cycles then they can be permuted among each other without affecting the cycle type. Thus, if the number of i-cycles is k_i, there are $i^{k_i} k_i!$ different ways of writing them down, with each i-cycle contributing a factor of i to this count.

Thus, the number of *distinct* elements with the same cycle type as π is

$$\frac{n!}{\prod_i i^{k_i} k_i},$$

as desired. ◀

Lecture 17

17.3. We are decomposing $V^{\otimes 2}$ into ± 1-eigenspaces under the action of a. This can be done explicitly:

$$v = \frac{1}{2}(v + av) + \frac{1}{2}(v - av).$$

Applying this to the basis vector $v_i \otimes v_j$ of $V^{\otimes 2}$, this shows that the given sets span $\mathrm{Sym}^2(V)$ and $\mathrm{Alt}^2(V)$; their linear independence is evident. If V is a G-module then notice that the actions of $g \in G$ and $a \in C_2$ commute:

$$a(g(x \otimes y)) = a(gx \otimes gy) = gy \otimes gx = g(y \otimes x) = g(a(x \otimes y)).$$

Thus, each a-eigenspace is G-invariant.

If that last bit was too slick, suppose $gv_i = \sum_k a_{ik}v_k$ and compute:

$$\begin{aligned} g(v_i \otimes v_j + v_j \otimes v_i) &= gv_i \otimes gv_j + gv_j \otimes gv_i \\ &= \sum_{k,l} a_{ik}a_{jl}(v_i \otimes v_j) + \sum_{l,k} a_{jl}a_{ik}(v_j \otimes v_i) \\ &= \sum_{k,l} a_{ik}a_{jl}(v_i \otimes v_j + v_j \otimes v_i). \end{aligned}$$

Thus, g sends each basis vector of $\mathrm{Sym}^2(V)$ back into $\mathrm{Sym}^2(V)$, so $\mathrm{Sym}^2(V)$ is G-invariant. A similar argument applies to $\mathrm{Alt}^2(V)$. ◀

Lecture 18

18.6. Here they are:

$$\begin{array}{|c|c|c|}\hline 1 & 2 & 3 \\ \hline 4 & 5 \\ \cline{1-2}\end{array}, \quad \begin{array}{|c|c|c|}\hline 1 & 2 & 5 \\ \hline 3 & 4 \\ \cline{1-2}\end{array}, \quad \begin{array}{|c|c|c|}\hline 1 & 2 & 5 \\ \hline 3 & 4 \\ \cline{1-2}\end{array}, \quad \begin{array}{|c|c|c|}\hline 1 & 3 & 4 \\ \hline 2 & 5 \\ \cline{1-2}\end{array}, \quad \begin{array}{|c|c|c|}\hline 1 & 3 & 5 \\ \hline 2 & 4 \\ \cline{1-2}\end{array}.$$

◀

18.16. There is precisely one tabloid of shape (n), namely:

$$T = \begin{array}{c}\hline 1 \quad 2 \quad \cdots \quad n \\ \hline\end{array}.$$

So M_λ is one-dimensional. Furthermore, the S_n-action on $\{T\}$ is trivial: $\sigma \cdot \{T\} = \{T\}$. ◀

Lecture 19

19.5. We compute:

$$\begin{aligned} \sigma \cdot e_T &= \sigma \sum_{\pi \in C(T)} \mathrm{sgn}(\pi)\pi\{T\} \\ &= \sum_{\pi \in C(T)} \mathrm{sgn}(\pi)\sigma\pi\{T\} \\ &= \sum_{\pi \in \sigma C(T)\sigma^{-1}} \mathrm{sgn}(\sigma^{-1}\pi\sigma)\sigma(\sigma^{-1}\pi\sigma)\{T\} && \text{(re-index: } \pi \leftrightarrow \sigma^{-1}\pi\sigma) \\ &= \sum_{\pi\sigma C(T)\sigma^{-1}} \mathrm{sgn}(\pi)\pi\{\sigma \cdot T\} && (\sigma \cdot \{T\} = \{\sigma \cdot T\}) \\ &= \sum_{\pi \in C(\sigma \cdot T)} \mathrm{sgn}(\pi)\pi\{\sigma \cdot T\} && \text{(Problem 18.2(c))} \\ &= e_{\sigma \cdot T}, \end{aligned}$$

as claimed. ◀

19.24. The only partitions $\lambda \vdash 6$ that dominate $(3,3)$ are $(3,3)$, $(4,2)$, $(5,1)$ and (6). Thus,

$$M_{(3,3)} = S_{3,3} \oplus S_{(4,2)}^{\oplus K} \oplus \oplus S_{(5,1)}^{\oplus K'} \oplus S_{(6)},$$

where $K = K_{(4,2)(3,3)}$ and $K' = K_{(5,1)(3,3)}$, and we've used the fact that

$$K_{(3,3)(3,3)} = K_{(6)(3,3)} = 1.$$

The remaining Kostka numbers are both 1, since the only relevant tableaux are

$$\begin{array}{|c|c|c|c|c|}\hline 1 & 1 & 1 & 1 & 2 \\ \hline 2 & 2 \\ \cline{1-2}\end{array} \quad \text{and} \quad \begin{array}{|c|c|c|c|c|}\hline 1 & 1 & 1 & 2 & 2 \\ \hline 2 \\ \cline{1-1}\end{array}.$$

◀

Lecture 20

20.1. Let δ_x be the indicator function at $x \in G$. The product in FG suggests defining $\delta_x * \delta_y = \delta_{xy}$. Now, an arbitrary function $f \in \mathcal{F}(G, F)$ can be written as

$$f = \sum_{x \in G} f(x)\delta_x.$$

So we should define the product of $f, g \in \mathcal{F}(G, F)$ by

$$f * g = \left(\sum_{x \in G} f(x)\delta_x \right) * \left(\sum_{y \in G} g(y)\delta_y \right) = \sum_{x,y \in G} f(x)f(y)\delta_{xy},$$

or equivalently

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

which is how the convolution product is usually presented in textbooks. ◀

Lecture 21

21.5. We can take $\{1, x\}$ to be our $\mathbb{R}$-vector space basis for V. Note that $x^2 = -1$ in V. The generator $a \in C_4$ acts on V as multiplication by x. Observe that

$$\begin{aligned} a \cdot 1 &= x = 0 \cdot 1 + 1 \cdot x \\ a \cdot x &= x^2 = (-1) \cdot 1 + 0 \cdot x. \end{aligned}$$

Thus the matrix for a is $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$, which is the rotation-by-$\pi/2$ matrix. ◀

Lecture 22

22.4. Recall that a simple F-module is a one-dimensional vector space. So a semisimple F-module is the direct sum of one-dimensional vector spaces. Since every vector space has a basis, it follows that every vector space is the direct sum of one dimensional subspace, hence *every* F-module is semisimple.

On the other hand, the simple $\mathbb{Z}$-modules are the cyclic groups C_p where p is a prime. Hence a semisimple $\mathbb{Z}$-module is the direct sum of various copies of C_p. For instance, $\mathbb{Z}$ and C_4 are not semisimple, but $C_6 = C_2 \oplus C_3$ is. ◀

22.8. Suppose M is generated by nonzero $m_1, \ldots, m_k$. Let $\mathcal{C}$ be the set of submodules of M that do not contain at least one m_i. Order $\mathcal{C}$ by inclusion. Note that $\mathcal{C}$ is nonempty since $0 \in \mathcal{C}$. Given a chain $\{N_i\}_i$ in $\mathcal{C}$, consider $N = \cup_i N_i$. This is clearly a submodule of M. It also does not contain at least one of the m_i, since if otherwise it contained them all, then some N_j must also contain them all, contradicting the fact that $N_j \in \mathcal{C}$. Thus, each chain has an upper bound in $\mathcal{C}$ and so $\mathcal{C}$ has a maximal element M' by Zorn's Lemma. This M' is clearly a proper submodule of M. I claim that M' is a maximal submodule of M. Indeed, let L be a submodule such that $M' \subsetneq L \subseteq M$. Then L must contain all of the m_i since otherwise we would contradict the maximality of M' in $\mathcal{C}$. Thus, $L = M$. ◀

Lecture 23

23.7. Each matrix $A \in M_n(\mathrm{End}_R(S))$ defines in a natural way an element in $\widetilde{A} \in \mathrm{End}_R(S^{\oplus n})$ by matrix multiplication:

$$\widetilde{A}(x_1, \ldots, x_n) = A \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} \sum_{j=1}^n a_{1j} x_j \\ \vdots \\ \sum_{j=1}^n a_{nj} x_j \end{bmatrix},$$

where the product of $a_{ij} x$ is to be understood as the evaluation $a_{ij}(x_j)$. The map $A \mapsto \widetilde{A}$ is our desired inverse. Indeed, it's a ring homomorphism (by the standard argument: matrix multiplication is composition of functions), and for $f \in \mathrm{End}_R(S^{\oplus n})$, we have

$$\begin{aligned} f(x_1, \ldots, x_n) = (y_1, \ldots, y_n) &\iff \sum_{j=1}^n f \circ \iota_j(x_j) = (y_1, \ldots, y_n) \\ &\iff \sum_{j=1}^n \pi_i \circ f \circ \iota_j(x_j) = y_i \text{ for all } i \\ &\iff \sum_{j=1}^n f_{ij}(x) = y_j. \end{aligned}$$

Thus, if $A = [f_{ij}]$ then $\tilde{A} = f$. ◀