Group Representation Theory

Ed Segal

based on notes laTexed by Fatema Daya and Zach Smith

2014

This course will cover the representation theory of finite groups over $\mathbb{C}$. We assume the reader knows the basic properties of groups and vector spaces.

Contents

1 Representations **2**

1.1 Representations as matrices 2

1.2 Representations as linear maps 7

1.3 Constructing representations 8

1.4 G-linear maps and subrepresentations 13

1.5 Maschke's theorem 19

1.6 Schur's lemma and abelian groups 28

1.7 Vector spaces of linear maps 33

1.8 More on decomposition into irreps 39

1.9 Duals and tensor products 49

2 Characters **55**

2.1 Basic properties 55

2.2 Inner products of characters 62

2.3 Class functions and character tables 72

3 Algebras and modules **78**

3.1 Algebras 78

3.2 Modules 83

3.3 Matrix algebras 91

3.4 Semi-simple algebras 99

3.5 Centres of algebras 106

A Revision on linear maps and matrices **108**

A.1 Vector spaces and bases 109

A.2 Linear maps and matrices 109

A.3 Changing basis 112

1 Representations

1.1 Representations as matrices

Informally, a **representation** of a group is a way of writing it down as a group of matrices.

Example 1.1.1. Consider C_4 (a.k.a. $\mathbb{Z}/4$), the cyclic group of order 4:

$$C_4 = \{e, \mu, \mu^2, \mu^3\}$$

where $\mu^4 = e$ (we'll always denote the identity element of a group by e). Consider the matrices

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad M = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$
$$M^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \qquad M^3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

Notice that $M^4 = I$. These 4 matrices form a subgroup of $GL_2(\mathbb{R})$ - the group of all 2×2 invertible matrices with real coefficients under matrix multiplication. This subgroup is isomorphic to C_4, the isomorphism is

$$\mu \mapsto M$$

(so $\mu^2 \mapsto M^2, \mu^3 \mapsto M^3, e \mapsto I$).

Example 1.1.2. Consider the group $C_2 \times C_2$ (the *Klein-four group*) generated by σ, τ such that

$$\sigma^2 = \tau^2 = e$$
$$\sigma\tau = \tau\sigma$$

Here's a representation of this group:

$$\sigma \mapsto S = \begin{pmatrix} 1 & -2 \\ 0 & -1 \end{pmatrix}$$
$$\tau \mapsto T = \begin{pmatrix} -1 & 2 \\ 0 & 1 \end{pmatrix}$$

To check that this is a representation, we need to check the relations:

$$S^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = T^2$$
$$ST = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = TS$$

So S and T generate a subgroup of $GL_2(\mathbb{R})$ which is isomorphic to $C_2 \times C_2$. Let's try and simplify by diagonalising S. The eigenvalues of S are ± 1, and the eigenvectors are

$$\begin{pmatrix}1\\0\end{pmatrix} \mapsto \begin{pmatrix}1\\0\end{pmatrix} \quad (\lambda_1 = 1)$$
$$\begin{pmatrix}1\\1\end{pmatrix} \mapsto \begin{pmatrix}-1\\-1\end{pmatrix} \quad (\lambda_2 = -1)$$

So if we let

$$P = \begin{pmatrix}1 & 1\\0 & 1\end{pmatrix}, \quad \hat{S} = \begin{pmatrix}1 & 0\\0 & -1\end{pmatrix}$$

Then

$$P^{-1}SP = \hat{S}$$

Now let's diagonalise T: the eigenvalues are ± 1, and the eigenvectors are

$$\begin{pmatrix}1\\0\end{pmatrix} \mapsto -\begin{pmatrix}1\\0\end{pmatrix} \quad (\lambda_1 = -1)$$
$$\begin{pmatrix}1\\1\end{pmatrix} \mapsto \begin{pmatrix}1\\1\end{pmatrix} \quad (\lambda_2 = 1)$$

Notice T and S have the same eigenvectors! Coincidence? Of course not, as we'll see later. So if

$$\hat{T} = \begin{pmatrix}-1 & 0\\0 & 1\end{pmatrix}$$

Then $P^{-1}TP = \hat{T}$.

Claim. $\hat{S}$ and $\hat{T}$ form a new representation of $C_2 \times C_2$

Proof.

$$\hat{S}^2 = P^{-1}S^2P = P^{-1}P = I$$
$$\hat{T}^2 = P^{-1}T^2P = P^{-1}P = I$$
$$\hat{S}\hat{T} = P^{-1}STP = P^{-1}TSP = \hat{T}\hat{S}$$

Hence, this forms a representation. □

This new representation is easier to work with because all the matrices are diagonal, but it carries the same information as the one using S and T. We say the two representations are **equivalent**.

Can we diagonalise the representation from Example 1.1.1? The eigenvalues of M are $\pm i$, so M cannot be diagonalised over $\mathbb{R}$, but it can be diagonalized over $\mathbb{C}$. So $\exists P \in GL_2(\mathbb{C})$ such that

$$P^{-1}MP = \hat{M} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

and $\mu \mapsto \hat{M}$ defines a representation of C_4 that is equivalent to $\mu \mapsto M$. As this example shows, it's easier to work over $\mathbb{C}$.

Definition 1.1.3 (*First version*)**.** Let G be a group. A **representation** of G is a homomorphism

$$\rho : G \to GL_n(\mathbb{C})$$

for some number n.

The number n is called the **dimension** (or the **degree**) of the representation. It is also possible to work over other fields ($\mathbb{R}, \mathbb{Q}, \mathbb{F}_p$, etc.) but we'll stick to $\mathbb{C}$. We'll also always assume that our groups are finite.

There's an important point to notice here: by definition, a representation ρ is a *homomorphism*, it is not just the image of that homomorphism. In particular we don't necessarily assume that ρ is an injection, i.e. the image of ρ doesn't have to be isomorphic to G.

If ρ is an injection, then we say that the representation is **faithful**. In our previous two examples, all the representations were faithful. Here's an example of a non-faithful representation:

Example 1.1.4. Let $G = C_6 = \langle \mu \mid \mu^6 = e \rangle$. Let $n = 1$. $GL_1(\mathbb{C})$ is the group of non-zero complex numbers (under multiplication). Define

$$\rho : G \to GL_1(\mathbb{C})$$

$$\rho : \mu \mapsto e^{\frac{2\pi i}{3}}$$

so $\rho(\mu^k) = e^{\frac{2\pi i k}{3}}$. We check $\rho(\mu)^6 = 1$, so this is a well-defined representation of C_6. But $\rho(\mu^3) = 1$ also, so

- the kernel of ρ is $\{e, \mu^3\}$.

- the image of ρ is $\left\{1, e^{\frac{2\pi i}{3}}, e^{\frac{4\pi i}{3}}\right\}$, which is isomorphic to C_3.

Example 1.1.5. Let G be any group, and n be any number. Define

$$\rho : G \to GL_n(\mathbb{C})$$

by

$$\rho : g \mapsto I_n \quad \forall\, g \in G$$

This is a representation, as

$$\rho(g)\rho(h) = I_n I_n = I_n = \rho(gh)$$

This is known as the **trivial representation** of G (of dimension n). The kernel is equal to G, and the image is the subgroup $\{I_n\} \subset GL_n$, which is isomorphic to the trivial group.

Let P be any invertible matrix. The map 'conjugate by P'

$$c_P : GL_n(\mathbb{C}) \to GL_n(\mathbb{C})$$

given by

$$c_P : M \mapsto P^{-1}MP$$

is a homomorphism. So if

$$\rho : G \to GL_n(\mathbb{C})$$

is a homomorphism, then so is $c_P \circ \rho$ (because composition of homomorphisms is a homomorphism).

Definition 1.1.6. Two representations of G

$$\rho_1 : G \to GL_n(\mathbb{C}) \qquad\qquad \rho_2 : G \to GL_n(\mathbb{C})$$

are **equivalent** if $\exists P \in GL_n(\mathbb{C})$ such that $\rho_2 = c_P \circ \rho_1$.

Equivalent representations really are 'the same' in some sense. To understand this, we have to stop thinking about matrices, and start thinking about linear maps.

1.2 Representations as linear maps

Let V be an n-dimensional vector space. The set of all invertible linear maps from V to V form a group which we call $GL(V)$.

If we pick a basis of V then every linear map corresponds to a matrix (see Corollary A.3.2), so we get an isomorphism $GL(V) \cong GL_n(\mathbb{C})$. However, this isomorphism depends on which basis we chose, and often we don't want to choose a basis at all.

Definition 1.2.1 (*Second draft of Definition 1.1.3*)**.** A **representation** of a group G is a choice of a vector space V and a homomorphism

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

If we pick a basis of V, we get a representation in the previous sense. If we need to distinguish between these two definitions, we'll call a representation in the sense of Definition 1.1.3 a **matrix representation**.

Notice that if we set the vector space V to be $\mathbb{C}^n$ then $GL(V)$ is exactly the same thing as $GL_n(\mathbb{C})$. So if we have a matrix representation, then we can think of it as a representation (in our new sense) acting on the vector space $\mathbb{C}^n$.

Lemma 1.2.2. *Let $\rho : G \to GL(V)$ be a representation of a group G. Let $\mathcal{A} = \{a_1, \ldots, a_n\}$ and $\mathcal{B} = \{b_1, \ldots, b_n\}$ be two bases for V. Then the two associated matrix representations*

$$\rho^{\mathcal{A}} : G \to GL_n(\mathbb{C})$$
$$\rho^{\mathcal{B}} : G \to GL_n(\mathbb{C})$$

are equivalent.

Proof. For each $g \in G$ we have a linear map $\rho(g) \in GL(V)$. Writing this linear map with respect to the basis $\mathcal{A}$ gives us the matrix $\rho^{\mathcal{A}}(g)$, and writing it with respect to the basis $\mathcal{B}$ gives us the matrix $\rho^{\mathcal{B}}(g)$. Then by Corollary A.3.2 we have

$$\rho^{\mathcal{B}}(g) = P^{-1}\rho^{\mathcal{A}}(g)P$$

where P is the change-of-basis matrix between $\mathcal{A}$ and $\mathcal{B}$. This is true for all $g \in G$, so

$$\rho^{\mathcal{B}} = c_P \circ \rho^{\mathcal{A}}$$

□

Conversely, suppose ρ_1 and ρ_2 are equivalent matrix representations of G, and let P be the matrix such that $\rho_2 = c_P \circ \rho_1$. If we set V to be the vector space $\mathbb{C}^n$ then we can think of ρ_1 as a representation

$$\rho_1 : G \to GL(V)$$

Now let $\mathbb{C} \subset \mathbb{C}^n$ be the basis consisting of the columns of the matrix P, so P is the change-of-basis matrix between the standard basis and $\mathbb{C}$ (see Section A.3). For each group element g, if we write down the linear map $\rho_1(g)$ using the basis $\mathbb{C}$ then we get the matrix

$$P^{-1}\rho_1(g)P = \rho_2(g)$$

So we can view ρ_2 as the matrix representation that we get when we take ρ_1 and write it down using the basis $\mathbb{C}$.

MORAL: Two matrix representations are equivalent if and only if they describe the same representation in different bases.

1.3 Constructing representations

Recall that the symmetric group S_n is defined to be the set of all permutations of a set of n symbols. Suppose we have a subgroup $G \subset S_n$. Then we can write down an n-dimensional representation of G, called the **permutation representation**. Here's how:

Let V be an n-dimensional vector space with a basis $\{b_1, \ldots, b_n\}$. Every element $g \in G$ is a permutation of the set $\{1, \ldots, n\}$ (or, if you prefer, it's a permutation of the set $\{b_1, \ldots, b_n\}$). Define a linear map

$$\rho(g) : V \to V$$

by definining

$$\rho(g) : b_k \mapsto b_{g(k)}$$

and extending this to a linear map. Now

$$\rho(g) \circ \rho(h) : b_k \mapsto b_{gh(k)}$$

so

$$\rho(g) \circ \rho(h) = \rho(gh)$$

(since they agree on a basis). Therefore

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

is a homomorphism.

Example 1.3.1. Let $G = \{(1), (123), (132)\} \subset S_3$. G is a subgroup, and it's isomorphic to C_3. Let $V = \mathbb{C}^3$ with the standard basis. The permutation representation of G (written in the standard basis) is

$$\rho((1)) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$
$$\rho((123)) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$
$$\rho((132)) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

[Aside: the definition of a permutation representation works over any field.]

But remember Cayley's Theorem! Every group of size n is a subgroup of the symmetric group S_n.

Proof. Think about the set of elements of G as abstract set $\mathcal{G}$ of n symbols. Left multiplication by $g \in G$ defines a bijection

$$\mathcal{L}_g : \mathcal{G} \to \mathcal{G}$$
$$\mathcal{L}_g : h \mapsto gh$$

and a bijection from a set of size n to itself is exactly a permutation. So we have a map

$$G \to S_n$$

defined by

$$g \to \mathcal{L}_g$$

This is in fact an injective homomorphism, so its image is a subgroup of S_n which is isomorphic to G. $\square$

So for any group of size n we automatically get an n-dimensional representation of G. This is called the **regular representation**, and it's very important.

Example 1.3.2. Let $G = C_2 \times C_2 = \{e, \sigma, \tau, \sigma\tau\}$ where $\sigma^2 = \tau^2 = e$ and $\tau\sigma = \sigma\tau$. Left multiplication by σ gives a permutation

$$\begin{aligned} \mathcal{L}_\sigma : &\mathcal{G} \to \mathcal{G} \\ &e \mapsto \sigma \\ &\sigma \mapsto e \\ &\tau \mapsto \sigma\tau \\ &\sigma\tau \mapsto \tau \end{aligned}$$

Let V be the vector space with basis $\{b_e, b_\sigma, b_\tau, b_{\sigma\tau}\}$. The regular representation of G is a homomorphism

$$\rho_{reg} : G \to GL(V)$$

With respect to the given basis of V, $\rho_{reg}(\sigma)$ is the matrix

$$\rho_{reg}(\sigma) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

The other two non-identity elements go to

$$\rho_{reg}(\tau) = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

$$\rho_{reg}(\sigma\tau) = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

The next lemma is completely trivial to prove, but worth writing down:

Lemma 1.3.3. *Let G be a group and let $H \subset G$ be a subgroup. Let*

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

be a representation of G. Then the restriction of ρ to H

$$\rho|_H : H \to GL(V)$$

is a representation of H.

Proof. Immediate. □

We saw an example of this earlier: for the group S_n we constructed an n-dimensional permutation representation, then for any subgroup $H \subset S_n$ we considered the restriction of this permutation representation to H.

Slightly more generally:

Lemma 1.3.4. *Let G and H be two groups, let*

$$f : H \to G$$

be a homomorphism, and let $\rho : G \to GL(V)$ be a representation of G. Then

$$\rho \circ f : H \to GL(V)$$

is a representation of H.

Proof. A composition of homomorphisms is a homomorphism. $\square$

Lemma 1.3.3 is a special case of this, where we let $f : H \hookrightarrow G$ be the inclusion of a subgroup.

Example 1.3.5. Let $H = C_6 = \langle \mu | \mu^6 = e \rangle$ and let $G = C_3 = \langle \nu | \nu^3 = e \rangle$. Let $f : H \to G$ be the homomorphism sending μ to ν. There's a faithful 1-dimensional representation of C_3 defined by

$$\rho : G \to GL_1(\mathbb{C})$$

$$\rho : \nu \to e^{\frac{2\pi i}{3}}$$

Then $\rho \circ f$ is the non-faithful representation of C_6 that we looked at in Example 1.1.4.

Example 1.3.6. Let $G = C_2 = \langle \mu | \mu^2 = e \rangle$, and let $H = S_n$ for some n. Recall that there is a homomorphism

$$sgn : S_n \to C_2$$

$$sgn(\sigma) = \begin{cases} e & \text{if } \sigma \text{ is an even permutation} \\ \mu & \text{if } \sigma \text{ is an odd permutation} \end{cases}$$

There's a 1-dimensional representation of C_2 given by

$$\rho : C_2 \to GL_1(\mathbb{C})$$

$$\rho : \mu \to -1$$

(this is a representation, because $(-1)^2 = 1$). Composing this with sgn, we get a 1-dimensional representation of S_n, which sends each even permutation to 1, and each odd permutation to -1. This is called the **sign representation** of S_n.

Finally, for some groups we can construct representations using geometry.

Example 1.3.7. D_4 is the symmetry group of a square. It has size 8, and consists of 4 reflections and 4 rotations. Draw a square in the plane with vertices at $(1, 1), (1, -1), (-1, -1)$ and $(-1, 1)$. Then the elements of D_4 naturally become linear maps acting on a 2-dimensional vector space. Using the standard basis, we get the matrices:

- rotate by $\frac{\pi}{2}$: $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$
- rotate by π: $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$
- rotate by $\frac{3\pi}{2}$: $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$
- reflect in x-axis: $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
- reflect in y-axis: $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$
- reflect in $y = x$: $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
- reflect in $y = -x$: $\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$

Together with I_2, these matrices give a 2-dimensional representation of D_4.

1.4 G-linear maps and subrepresentations

You should have noticed that whenever you meet a new kind of mathematical object, soon afterwards you meet the 'important' functions between the objects. For example:

Objects	Functions
Groups	Homomorphisms
Vector spaces	Linear maps
Topological spaces	Continuous maps
Rings	Ring Homomorphisms
$\vdots$	$\vdots$

So we need to define the important functions between representations.

Definition 1.4.1. Let

$$\rho_1 : G \to GL(V)$$
$$\rho_2 : G \to GL(W)$$

be two representations of G on vector spaces V and W. A **G-linear map** between ρ_1 and ρ_2 is a linear map $f : V \to W$ such that

$$f \circ \rho_1(g) = \rho_2(g) \circ f \qquad \forall\, g \in G$$

i.e. both ways round the square

$$\begin{array}{ccc} V & \xrightarrow{\rho_1(g)} & V \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f} \\ W & \xrightarrow{\rho_2(g)} & W \end{array}$$

give the same answer ('the square commutes').

So a G-linear map is a special kind of linear map that respects the group actions. For any linear map, we have

$$f(\lambda x) = \lambda f(x)$$

for all $\lambda \in \mathbb{C}$ and $x \in V$, i.e. we can pull scalars through f. For G-linear maps, we also have

$$f(\rho_1(g)(x)) = \rho_2(g)(f(x))$$

for all $g \in G$, i.e. we can also pull group elements through f.

Suppose f is a G-linear map, and suppose as well that f is an isomorphism between the vector spaces V and W, i.e. there is an inverse linear map

$$f^{-1} : W \to V$$

such that $f \circ f^{-1} = \mathbf{1}_W$ and $f^{-1} \circ f = \mathbf{1}_V$ (recall that f has an inverse iff f is a bijection).

Claim 1.4.2. *f^{-1} is also a G-linear map.*

In this case, we say f is a (G-linear) **isomorphism** and that the two representations ρ_1 and ρ_2 are **isomorphic**. Isomorphism is really the same thing as equivalence.

Proposition 1.4.3. *Let V and W be two vector spaces, both of dimension n. Let*

$$\begin{aligned}\rho_1 &: G \to GL(V)\\ \rho_2 &: G \to GL(W)\end{aligned}$$

be two representations of G. Let $\mathcal{A} = \{a_1, \ldots, a_n\}$ be a basis for V, and let $\mathcal{B} = \{b_1, \ldots, b_n\}$ be a basis for W, and let

$$\begin{aligned}\rho_1^{\mathcal{A}} &: G \to GL_n(\mathbb{C})\\ \rho_2^{\mathcal{B}} &: G \to GL_n(\mathbb{C})\end{aligned}$$

be the matrix representations obtained by writing ρ_1 and ρ_2 in these bases. Then ρ_1 and ρ_2 are isomorphic if and only if $\rho_1^{\mathcal{A}}$ and $\rho_2^{\mathcal{B}}$ are equivalent.

Proof. ($\Rightarrow$) Let $f : V \to W$ be a G-linear isomorphism. Then

$$f\mathcal{A} = \{f(a_1), \ldots, f(a_n)\} \subset W$$

is a second basis for W. Let $\rho_2^{f\mathcal{A}}$ be the matrix representation obtained by writing down ρ_2 in this new basis. Pick $g \in G$ and let $\rho_1^{\mathcal{A}}(g) = M$, i.e.

$$\rho_1(g)(a_k) = \sum_{i=1}^{n} M_{ik} a_i$$

(see Section A.2). Then by the G-linearity of f,

$$\begin{aligned}\rho_2(g)(f(a_k)) &= f(\rho_1(g)(a_k))\\ &= \sum_{i=1}^{n} M_{ik} f(a_i)\end{aligned}$$

So the matrix describing $\rho_2(g)$ in the basis $f\mathcal{A}$ is the matrix M, i.e. it is the same as the matrix describing $\rho_1(g)$ in the basis $\mathcal{A}$. This is true for all $g \in G$, so the two matrix representations $\rho_1^{\mathcal{A}}$ and $\rho_2^{f\mathcal{A}}$ are identical. But by Lemma 1.2.2, $\rho_2^{f\mathcal{A}}$ is equivalent to $\rho_2^{\mathcal{B}}$.

($\Leftarrow$) Let P be the matrix such that

$$\rho_2^{\mathcal{B}} = c_P \circ \rho_1^{\mathcal{A}}$$

Let

$$f : V \to W$$

be the linear map represented by the matrix P^{-1} with respect to the bases $\mathcal{A}$ and $\mathcal{B}$. Then f is an isomorphism of vector spaces, because P^{-1} is an invertible matrix. We need to show that f is also G-linear, i.e. that

$$f \circ \rho_1(g) = \rho_2(g) \circ f, \qquad \forall g \in G$$

Using our given bases we can write each of these linear maps as matrices, then this equation becomes

$$P^{-1}\rho_1^{\mathcal{A}}(g) = \rho_2^{\mathcal{B}}(g)P^{-1}, \qquad \forall g \in G$$

or equivalently

$$\rho_2^{\mathcal{B}}(g) = P^{-1}\rho_1^{\mathcal{A}}(g)P, \qquad \forall g \in G$$

and this is true by the definition of P. $\square$

Of course, not every G-linear map is an isomorphism.

Example 1.4.4. Let $G = C_2 = \langle \tau \mid \tau^2 = e \rangle$. The regular representation of G, written in the natural basis, is $\rho_{reg}(e) = I_2$ and

$$\rho_{reg}(\tau) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

(since multiplication by τ transposes the two group elements). Let ρ_1 be the 1-dimensional representation

$$\begin{aligned} \rho_1 : C_2 &\to GL_1(\mathbb{C}) \\ \tau &\mapsto -1 \end{aligned}$$

from Example 1.3.6. Now let $f : \mathbb{C}^2 \to \mathbb{C}$ be the linear map represented by the matrix $(1, -1)$ with respect to the standard bases. Then for any vector

$\mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \in \mathbb{C}^2$, we have

$$\begin{aligned} f \circ \rho_{reg}(\tau)(\mathbf{x}) &= (1, -1) \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \\ &= -(1, -1) \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \\ &= \rho_1(\tau) \circ f(\mathbf{x}) \end{aligned}$$

So f is a G-linear map from ρ_{reg} to ρ_1.

Example 1.4.5. Let G be a subgroup of S_n. Let (V, ρ_1) be the permutation representation, i.e. V is an n-dimensional vector space with a basis $\{b_1, \dots, b_n\}$, and

$$\begin{aligned} \rho_1 &: G \to GL(V) \\ \rho_1(g) &: b_k \mapsto b_{g(k)} \end{aligned}$$

Let $W = \mathbb{C}$, and let

$$\rho_2 : G \to GL(W) = GL(\mathbb{C})$$

be the (1-dimensional) trivial representation, i.e. $\rho_2(g) = 1 \, \forall g \in G$. Let $f : V \to W$ be the linear map defined by

$$f(b_k) = 1 \qquad \forall\, k$$

We claim that this is G-linear. We need to check that

$$f \circ \rho_1(g) = \rho_2(g) \circ f \quad \forall g \in G$$

It suffices to check this on the basis of V. We have:

$$f(\rho_1(g)(b_k)) = f(b_{g(k)}) = 1$$

and

$$\rho_2(g)(f(b_k)) = \rho_2(g)(1) = 1$$

for all g and k, so f is indeed G-linear.

Definition 1.4.6. A **subrepresentation** of a representation

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

is a vector subspace $W \subset V$ such that

$$\rho(g)(x) \in W \qquad \forall\, g \in G \text{ and } x \in W$$

This means that every $\rho(g)$ defines a linear map from W to W, i.e. we have a representation of G on the subspace W.

Example 1.4.7. Let $G = C_2$ and $V = \mathbb{C}^2$ with the regular representation as in Example 1.4.4. Let W be the 1-dimensional subspace spanned by the vector $\begin{pmatrix}1\\1\end{pmatrix} \in V$. Then

$$\rho_{reg}(\tau)\begin{pmatrix}1\\1\end{pmatrix} = \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}\begin{pmatrix}1\\1\end{pmatrix} = \begin{pmatrix}1\\1\end{pmatrix}$$

So $\rho_{reg}(\tau)\begin{pmatrix}\lambda\\\lambda\end{pmatrix} = \begin{pmatrix}\lambda\\\lambda\end{pmatrix}$, i.e. $\rho_{reg}(\tau)$ preserves W, so W is a subrepresentation. It's isomorphic to the trivial (1-dimensional) representation.

Example 1.4.8. We can generalise the previous example. Suppose we have a matrix representation $\rho : G \to GL_n(\mathbb{C})$. Now suppose we can find a vector $\mathbf{x} \in \mathbb{C}^n$ which is an eigenvector for every matrix $\rho(g)$, $g \in G$, i.e.

$$\rho(g)(\mathbf{x}) = \lambda_g \mathbf{x} \qquad \text{for some eigenvalues } \lambda_g \in \mathbb{C}^*$$

Then the span of $\mathbf{x}$ is a 1-dimensional subspace $\langle \mathbf{x} \rangle \subset \mathbb{C}^n$, and it's a subrepresentation. It's isomorphic to the 1-dimensional matrix representation

$$\begin{aligned}\rho &: G \to GL_1(\mathbb{C})\\ \rho &: g \mapsto \lambda_g\end{aligned}$$

Any linear map $f : V \to W$ has a kernel $\mathrm{Ker}(f) \subseteq V$ and an image $\mathrm{Im}(f) \subseteq W$ which are both vector subspaces.

Claim 1.4.9. *If f is a G-linear map between the two representations*

$$\begin{aligned}\rho_1 &: G \to GL(V)\\ \rho_2 &: G \to GL(W)\end{aligned}$$

Then $\mathrm{Ker}(f)$ *is a subrepresentation of V and* $\mathrm{Im}(f)$ *is a subrepresentation of W.*

Look back at Examples 1.4.4 and 1.4.7. The kernel of the map f is the subrepresentation W.

1.5 Maschke's theorem

Let V and W be two vector spaces. Recall the definition of the **direct sum**

$$V \oplus W$$

It's the vector space of all pairs (x, y) such that $x \in V$ and $y \in W$. Its dimension is $\dim V + \dim W$.

Suppose G is a group, and we have representations

$$\rho_V : G \to GL(V)$$
$$\rho_W : G \to GL(W)$$

Then there is a natural representation of G on $V \oplus W$ given by 'direct-summing' ρ_V and ρ_W. The definition is

$$\rho_{V\oplus W} : G \to GL(V \oplus W)$$
$$\rho_{V\oplus W}(g) : (x, y) \mapsto (\rho_V(g)(x), \rho_W(g)(y))$$

Claim 1.5.1. *For each g, $\rho_{V\oplus W}(g)$ is a linear map, and $\rho_{V\oplus W}$ is indeed a homomorphism from G to $GL(V \oplus W)$.*

Pick a basis $\{a_1, \ldots, a_n\}$ for V, and $\{b_1, \ldots, b_m\}$ for W. Suppose that in these bases, $\rho_V(g)$ is the matrix M and $\rho_W(g)$ is the matrix N. The set

$$\{(a_1, 0), \ldots, (a_n, 0), (0, b_1), \ldots, (0, b_m)\}$$

is a basis for $V \oplus W$, and in this basis the linear map $\rho_{V\oplus W}(g)$ is given by the $(n + m) \times (n + m)$ matrix

$$\begin{pmatrix} M & 0 \\ 0 & N \end{pmatrix}$$

A matrix like this is called **block-diagonal**.

Consider the linear map

$$\iota_V : V \to V \oplus W$$
$$\iota_V : x \mapsto (x, 0)$$

It's an injection, so it's an isomorphism between V and $\mathrm{Im}(\iota_V)$. So we can think of V as a subspace of $V \oplus W$. Also

$$\begin{aligned} \iota_V(\rho_V(g)(x)) &= (\rho_V(g)(x), 0) \\ &= \rho_{V \oplus W}(g)(x, 0) \end{aligned}$$

So ι_V is G-linear, and $\mathrm{Im}(\iota_V)$ is a subrepresentation which we can identify with V. Similarly, the subspace $\{(0, y),\ y \in W\} \subset V \oplus W$ is a subrepresentation, and it's isomorphic to W. The intersection of these two subrepresentations is obviously $\{0\}$.

Conversely:

Proposition 1.5.2. *Let $\rho : G \to GL(V)$ be a representation, and let $W \subset V$ and $U \subset V$ be subrepresentations such that*

i) $U \cap W = \{0\}$

ii) $\dim U + \dim W = \dim V$

Then V is isomorphic to $W \oplus U$.

Proof. You should recall that we can identify V with $W \oplus U$ as vector spaces, because every vector in V can be written uniquely as a sum $x + y$ with $x \in W$ and $y \in U$. In other words, the map

$$\begin{aligned} f &: W \oplus U \to V \\ f &: (x, y) \mapsto x + y \end{aligned}$$

is an isomorphism of vector spaces. We claim that f is also G-linear. Let's write

$$\rho_W : G \to GL(W), \qquad \rho_U : G \to GL(U)$$

for the representations of G on W and U, note that by definition we have

$$\rho_W(g)(x) = \rho_V(g)(x), \qquad \forall x \in W$$

and

$$\rho_U(g)(y) = \rho_V(g)(y), \qquad \forall y \in U$$

Then the following square commutes:

$$\begin{tikzcd}
(x, y) \arrow[r, mapsto, "\rho_{W\oplus U}(g)"] \arrow[d, mapsto, "f"] & (\rho_W(g)(x),\ \rho_U(g)(y)) \arrow[d, mapsto, "f"] \\
x + y \arrow[r, mapsto, "\rho_V(g)"] & \rho_V(g)(x+y) = \rho_V(g)(x) + \rho_V(g)(y)
\end{tikzcd}$$

So f is indeed G-linear, and hence it's an isomorphism of representations. $\square$

Now suppose $\rho : G \to GL(V)$ is a representation, and $W \subset V$ is a subrepresentation. Given the previous proposition, it is natural to ask the following:

Question 1.5.3. Can we find another subrepresentation $U \subset V$ such that $U \cap W = \{0\}$ and $\dim V = \dim W + \dim U$?

If we can, then we can split V up as a direct sum

$$V = W \oplus U$$

Such a U is called a **complementary subrepresentation** to W.

It turns out the answer to this question is always yes! This is called **Maschke's Theorem**. It's the most important theorem in the course, but fortunately the proof isn't too hard.

Example 1.5.4. Recall Examples 1.4.4 and 1.4.7. We set $G = C_2$, and V was the regular representation. We found a (1 dimensional) subrepresentation

$$W = \left\langle \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\rangle \subset \mathbb{C}^2 = V$$

Can we find a complementary subrepresentation? Let

$$U = \left\langle \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\rangle \subset \mathbb{C}^2 = V$$

Then

$$\rho_{reg}(\tau) \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = - \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

So U is a subrepresentation, and it's isomorphic to ρ_1. Furthermore, $V = W \oplus U$ because $W \cap U = 0$ and $\dim U + \dim W = 2 = \dim V$.

To prove Maschke's Theorem, we need the following:

Lemma 1.5.5. *Let V be a vector space, and let $W \subset V$ be a subspace. Suppose we have a linear map*

$$f : V \to W$$

such that $f(x) = x$ for all $x \in W$. Then $\mathrm{Ker}(f) \subset V$ is a complementary subspace to W, i.e.

$$V = W \oplus \mathrm{Ker}(f)$$

Proof. If $x \in \mathrm{Ker}(f) \cap W$ then $f(x) = x = 0$, so $\mathrm{Ker}(f) \cap W = 0$. Also, f is a surjection, so by the Rank-Nullity Theorem,

$$\dim \mathrm{Ker}(f) + \dim W = \dim V$$

□

A linear map like this is called a **projection**. For example, suppose that $V = W \oplus U$, and let π_W be the linear map

$$\begin{aligned} \pi_W : V &\to W \\ (x, y) &\mapsto x \end{aligned}$$

Then π_W is a projection, and $\mathrm{Ker}(\pi_W) = U$. The above lemma says that every projection looks like this.

Corollary 1.5.6. *Let $\rho : G \to GL(V)$ be a representation , and $W \subset V$ a subrepresentation. Suppose we have a G-linear projection*

$$f : V \to W$$

Then $\mathrm{Ker}(f)$ is a complementary subrepresentation to W.

Proof. This is immediate from the previous lemma. □

Theorem 1.5.7 (Maschke's Theorem)**.** *Let $\rho : G \to GL(V)$ be a representation, and let $W \subset V$ be a subrepresentation. Then there exists a complementary subrepresentation $U \subset V$ to W.*

Proof. By Corollary 1.5.6, it's enough to find a G-linear projection from V to W. Recall that we can always find a complementary subspace (not subrepresentation!) $\tilde{U} \subset V$ to W. For example, we can pick a basis $\{b_1, \ldots, b_m\}$ for W, then extend it to a basis $\{b_1, \ldots, b_m, b_{m+1}, \ldots, b_n\}$ for V and let $\tilde{U} = \langle b_{m+1}, ..., b_n \rangle$. Let

$$\tilde{f} : V = W \oplus \tilde{U} \to W$$

be the projection with kernel $\tilde{U}$. There is no reason why $\tilde{f}$ should be G-linear. However, we can do a clever modification. Let's define

$$f : V \to V$$

by

$$f(x) = \frac{1}{|G|} \sum_{g \in G} (\rho(g) \circ \tilde{f} \circ \rho(g^{-1}))(x)$$

Then we claim that f is a G-linear projection from V to W.

First let's check that $\operatorname{Im} f \subset W$. For any $x \in V$ and $g \in G$ we have

$$\tilde{f}(\rho(g^{-1})(x)) \in W$$

and so

$$\rho(g)(\tilde{f}(\rho(g^{-1})(x))) \in W$$

since W is a subrepresentation. Therefore $f(x) \in W$ as well.

Next we check that f is a projection. Let $y \in W$. Then for any $g \in G$, we know that $\rho(g^{-1})(y)$ is also in W, so

$$\tilde{f}(\rho(g^{-1})(y)) = \rho(g^{-1}(y))$$

Therefore

$$\begin{aligned}
f(y) &= \frac{1}{|G|}\sum_{g\in G}\rho(g)(\tilde{f}(\rho(g^{-1})(y))) \\
&= \frac{1}{|G|}\sum_{g\in G}\rho(g)(\rho(g^{-1})(y)) \\
&= \frac{1}{|G|}\sum_{g\in G}\rho(gg^{-1})(y) \\
&= \frac{1}{|G|}\sum_{g\in G}\rho(e)(y) \\
&= \frac{|G|y}{|G|} \\
&= y
\end{aligned}$$

So f is indeed a projection. Finally, we check that f is G-linear. For any $x \in V$ and any $h \in G$, we have

$$\begin{aligned}
f(\rho(h)(x)) &= \frac{1}{|G|}\sum_{g\in G}(\rho(g)\circ\tilde{f}\circ\rho(g^{-1})\circ\rho(h))(x) \\
&= \frac{1}{|G|}\sum_{g\in G}(\rho(g)\circ\tilde{f}\circ\rho(g^{-1}h))(x) \\
&= \frac{1}{|G|}\sum_{g\in G}\rho(hg)\circ\tilde{f}\circ\rho(g^{-1}))(y) \\
&= (\rho(h)\circ f)(x)
\end{aligned}$$

(the sums on the second and third lines are the same, we've just relabelled/permuted the group elements appearing in the sum, sending $g \mapsto hg$). So f is indeed G-linear. □

So if V contains a subrepresentation W, then we can split V up as a direct sum.

Definition 1.5.8. If $\rho : G \to GL(V)$ is a representation with no subrepresentations (apart from the trivial subrepresentations $0 \subset V$ and $V \subseteq V$) then we call it an **irreducible** representation.

The real power of Maschke's Theorem is the following Corollary:

Corollary 1.5.9. *Every representation can be written as a direct sum*

$$U_1 \oplus U_2 \oplus \ldots \oplus U_r$$

of subrepresentations, where each U_i is irreducible.

Proof. Let V be a representation of G, of dimension n. If V is irreducible, we're done. If not, V contains a subrepresentation $W \subset V$, and by Maschke's Theorem,

$$V = W \oplus U$$

for some other subrepresentation U. Both W and U have dimension less than n. If they're both irreducible, we're done. If not, one of them contains a subrepresentation, so it splits as a direct sum of smaller subrepresentations. Since n is finite, this process will terminate in a finite number of steps. $\square$

So every representation is built up from irreducible representations in a straight-forward way. This makes irreducible representations very important, so we abbreviate the name and call them **irreps**. They're like the 'prime numbers' of representation theory.

Obviously, any 1-dimensional representation is irreducible. Here is a 2-dimensional irrep:

Example 1.5.10. Let $G = S_3$, it's generated by

$$\sigma = (123) \qquad \tau = (12)$$

with relations

$$\sigma^3 = \tau^2 = e, \qquad \tau\sigma\tau = \sigma^{-1}$$

Let

$$\rho(\sigma) = \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix} \qquad \rho(\tau) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

where $\omega = e^{\frac{2\pi i}{3}}$. This defines a representation of G (either check the relations, or do the Problem Sheets). Let's show that ρ is irreducible. Suppose (for a contradiction) that W is a non-trivial subrepresentation. Then $\dim W = 1$.

Also, W is preserved by the action of $\rho(\sigma)$ and $\rho(\tau)$, i.e. W is an eigenspace for both matrices. The eigenvectors of $\rho(\tau)$ are

$$\begin{pmatrix}1\\1\end{pmatrix} \qquad (\lambda_1 = 1)$$
$$\begin{pmatrix}1\\-1\end{pmatrix} \qquad (\lambda_2 = -1)$$

But the eigenvectors of $\rho(\sigma)$ are

$$\begin{pmatrix}1\\0\end{pmatrix} \qquad \& \qquad \begin{pmatrix}0\\1\end{pmatrix}$$

So there is no such W.

Now let's see some examples of Maschke's Theorem in action:

Example 1.5.11. The regular representation of $C_3 = \langle \mu | \mu^3 = 3 \rangle$ is

$$\rho_{reg}(\mu) = \begin{pmatrix}0 & 0 & 1\\1 & 0 & 0\\0 & 1 & 0\end{pmatrix}$$

(c.f. Example 1.3.1). Suppose $\mathbf{x} \in \mathbb{C}^3$ is an eigenvector of $\rho_{reg}(\mu)$. Then it's also an eigenvector of $\rho_{reg}(\mu^2)$, so $\langle \mathbf{x} \rangle \subset \mathbb{C}^3$ is a 1-dimensional subrepresentation. The eigenvectors of $\rho_{reg}(\mu)$ are

$$\begin{pmatrix}1\\1\\1\end{pmatrix} (\lambda_1 = 1) \qquad \begin{pmatrix}1\\\omega^{-1}\\\omega\end{pmatrix} (\lambda_2 = \omega) \qquad \begin{pmatrix}1\\\omega\\\omega^{-1}\end{pmatrix} (\lambda_3 = \omega^{-1})$$

So ρ_{reg} is the direct sum of 3 1-dimensional irreps:

$$U_1 = \left\langle \begin{pmatrix}1\\1\\1\end{pmatrix} \right\rangle \qquad U_2 = \left\langle \begin{pmatrix}1\\\omega^{-1}\\\omega\end{pmatrix} \right\rangle \qquad U_3 = \left\langle \begin{pmatrix}1\\\omega\\\omega^{-1}\end{pmatrix} \right\rangle$$

In the eigenvector basis,

$$\rho_{reg}(\mu) = \begin{pmatrix}1 & 0 & 0\\0 & \omega & 0\\0 & 0 & \omega^{-1}\end{pmatrix}$$

Look back at Examples 1.1.1, 1.1.2 and 1.5.4. In each one we took a matrix representation and found a basis in which every matrix became diagonal, i.e. we split each representation as a direct sum of 1-dimensional irreps.

Proposition 1.5.12. *Let $\rho : G \to GL_n(\mathbb{C})$ be a matrix representation. Then there exists a basis of $\mathbb{C}^n$ in which every matrix $\rho(g)$ is diagonal iff ρ is a direct sum of 1-dimensional irreps.*

Proof. ($\Rightarrow$) Let $\{\mathbf{x}_1, \ldots, \mathbf{x}_n\}$ be such a basis. Then $\mathbf{x}_i$ is an eigenvector for every $\rho(g)$, so $\langle \mathbf{x}_i \rangle$ is a 1-dimensional subrepresentation, and

$$\mathbb{C}^n = \langle \mathbf{x}_1 \rangle \oplus \langle \mathbf{x}_2 \rangle \oplus \ldots \oplus \langle \mathbf{x}_n \rangle$$

($\Leftarrow$) Suppose $\mathbb{C}^n = U_1 \oplus \ldots \oplus U_n$ with each U_i a 1-dimensional subrepresentation. Pick a (non-zero) vector $\mathbf{x}_i$ from each U_i. Then $\{\mathbf{x}_1, \ldots, \mathbf{x}_n\}$ is a basis for $\mathbb{C}^n$. For any $g \in G$, the matrix $\rho(g)$ preserves $\langle \mathbf{x}_i \rangle = U_i$ for all i, so $\rho(g)$ is a diagonal matrix with respect to this basis. □

We will see soon that if G is abelian, every representation of G splits as a direct sum of 1-dimensional irreps. When G is not abelian, this is not true.

Example 1.5.13. Let

$$\rho : S_3 \to GL_3(\mathbb{C})$$

be the permutation representation (in the natural basis). Recall S_3 is generated by $\sigma = (123)$, $\tau = (12)$. We have

$$\rho(\sigma) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \qquad \rho(\tau) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Notice that

$$\mathbf{x}_1 = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

is an eigenvector for both $\rho(\sigma)$ and $\rho(\tau)$. Therefore, it's an eigenvector for $\rho(\sigma^2), \rho(\sigma\tau)$ and $\rho(\sigma^2\tau)$ as well, so $U_1 = \langle \mathbf{x}_1 \rangle$ is a 1-dimensional subrepresentation. It's isomorphic to the 1-dimensional trivial representation. Let

$$U_2 = \left\langle \mathbf{x}_2 = \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix}, \ \mathbf{x}_3 = \begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix} \right\rangle$$

Clearly, $\mathbb{C}^3 = U_1 \oplus U_2$ as a vector space. We claim U_2 is a subrepresentation. We check:

$$\begin{aligned}
\rho(\sigma) : \mathbf{x}_2 &\mapsto \mathbf{x}_3 \in U_2 \\
\mathbf{x}_3 &\mapsto -\mathbf{x}_2 - \mathbf{x}_3 \in U_2 \\
\rho(\tau) : \mathbf{x}_2 &\mapsto -\mathbf{x}_2 \in U_2 \\
\mathbf{x}_3 &\mapsto \mathbf{x}_2 + \mathbf{x}_3 \in U_2
\end{aligned}$$

In this basis, U_2 is the matrix representation

$$\rho_2(\sigma) = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \qquad \rho(\tau) = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}$$

So ρ is the direct sum of two subrepresentations $U_1 \oplus U_2$. In the basis $\{\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3\}$ for $\mathbb{C}^3$, ρ becomes the (block-diagonal) matrix representation

$$\rho(\sigma) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & -1 \end{pmatrix} \qquad \rho(\tau) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

The representation U_2 is irreducible. Either

(i) Check that $\rho_2(\sigma)$ and $\rho_2(\tau)$ have no common eigenvector, or

(ii) Change basis to $\begin{pmatrix} 1 \\ -\omega \end{pmatrix}$ and $\begin{pmatrix} \omega^{-1} \\ -\omega \end{pmatrix}$, then

$$\rho_2(\sigma) = \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix}, \qquad \rho_2(\tau) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

(remember that $1 + \omega + \omega^{-1} = 0$) and we proved that this was irreducible in Example 1.5.10.

1.6 Schur's lemma and abelian groups

Theorem 1.6.1 (Schur's Lemma). *Let $\rho_V : G \to GL(V)$ and $\rho_W : G \to GL(W)$ be irreps of G.*

(i) Let $f : V \to W$ be a G-linear map. Then either f is an isomorphism, or f is the zero map.

(ii) Let $f : V \to V$ be a G-linear map. Then $f = \lambda \mathbf{1}_V$ for some $\lambda \in \mathbb{C}$.

Proof. (i) Suppose f is not the zero map. $\mathrm{Ker}(f) \subset V$ is a subrepresentation of V, but V is an irrep, so either $\mathrm{Ker}(f) = 0$ or V. Since $f \neq 0$, $\mathrm{Ker}(f) = 0$, i.e. f is an injection. Also, $\mathrm{Im}(f) \subset W$ is a subrepresentation, and W is irreducible, so $\mathrm{Im}(f) = 0$ or W. Since $f \neq 0$, $\mathrm{Im}(f) = W$, i.e. f is a surjection. So f is an isomorphism.

(ii) Every linear map from V to V has at least one eigenvalue. Let λ be an eigenvalue of f and consider

$$\hat{f} = (f - \lambda \mathbf{1}_V) : V \to V$$

Then $\hat{f}$ is G-linear, because

$$\begin{aligned} \hat{f}(\rho_V(g)(x)) &= f(\rho_V(g)(x)) - \lambda \rho_V(g)(x) \\ &= \rho_V(g)(f(x)) - \rho_V(g)(\lambda x) \\ &= \rho_V(g)(\hat{f}(x)) \end{aligned}$$

for all $g \in G$ and $x \in V$. Since λ is an eigenvalue, $\mathrm{Ker}(\hat{f})$ is at least 1-dimensional. So by part 1, $\hat{f}$ is the zero map, i.e. $f = \lambda \mathbf{1}_V$. □

[Aside: (i) works over any field whereas (ii) is special to $\mathbb{C}$.]

Schur's Lemma lets us understand the representation theory of abelian groups completely.

Proposition 1.6.2. *Suppose G is abelian. Then every irrep of G is 1-dimensional.*

Proof. Let $\rho : G \to GL(V)$ be an irrep of G. Pick any $h \in G$ and consider the linear map

$$\rho(h) : V \to V$$

In fact this is G-linear, because

$$\begin{aligned}\rho(h)(\rho(g)(x)) &= \rho(hg)(x) \\ &= \rho(gh)(x) \qquad \text{as } G \text{ is abelian} \\ &= \rho(g)(\rho(h)(x))\end{aligned}$$

for all $g \in G, x \in V$. So by Schur's Lemma, $\rho(h) = \lambda_h \mathbf{1}_V$ for some $\lambda_h \in \mathbb{C}$. So every element of G is mapped by ρ to a multiple of $\mathbf{1}_V$. Now pick any $x \in V$. For any $h \in G$, we have

$$\rho(h)(x) = \lambda_h x \in \langle x \rangle$$

so $\langle x \rangle$ is a (1-dimensional) subrepresentation of V. But V is an irrep, so $\langle x \rangle = V$, i.e. V is 1-dimensional. □

Corollary 1.6.3. *Let $\rho : G \to GL(V)$ be a representation of an abelian group. Then there exists a basis of V such that every $g \in G$ is represented by a diagonal matrix $\rho(g)$.*

Proof. By Maschke's Theorem, we can split ρ as a direct sum

$$V = U_1 \oplus U_2 \oplus \ldots \oplus U_n$$

of irreps. By Proposition 1.6.2, each U_i is 1-dimensional. Now apply Proposition 1.5.12. □

As remarked before, this is not true for non-abelian groups. However, there is a weaker statement that we can prove for any group:

Corollary 1.6.4. *Let $\rho : G \to GL(V)$ of any group G, and let $g \in G$. Then there exists a basis of V such that $\rho(g)$ is diagonal.*

Notice the difference with the previous statement: with abelian groups, $\rho(g)$ becomes diagonal for every $g \in G$, here we are diagonalizing just one $\rho(g)$. This is not very impressive, because 'almost all' matrices are diagonalizable!

Proof. Consider the subgroup $\langle g \rangle \subset G$. It's isomorphic to the cyclic group of order k, where k is the order of g. In particular, it is abelian. Restricting ρ to this subgroup gives a representation

$$\rho : \langle g \rangle \to GL(V)$$

Then Corollary 1.6.3 tells us we can find a basis of V such that $\rho(g)$ is diagonal. $\square$

Let's describe all the irreps of cyclic groups (the simplest abelian groups). Let $G = C_k = \langle \mu \,|\, \mu^k = e \rangle$. We've just proved that all irreps of G are 1-dimensional. A 1-dimensional representation of G is a homomorphism

$$\rho : G \to GL_1(\mathbb{C})$$

This is determined by a single number

$$\rho(\mu) \in \mathbb{C}$$

such that $\rho(\mu)^k = 1$. So $\rho(\mu) = e^{\frac{2\pi i}{k} q}$ for some $q = [0, \ldots, k-1]$. This gives us k irreps $\rho_0, \rho_1, ..., \rho_{k-1}$ where

$$\rho_q : \mu \mapsto e^{\frac{2\pi i}{k} q}$$

Claim 1.6.5. *These k irreps are all distinct, i.e. ρ_i and ρ_j are not isomorphic if $i \neq j$.*

Example 1.6.6. Let $G = C_4 = \langle \mu \,|\, \mu^4 = e \rangle$. There are 4 distinct (1-dimensional) irreps of G. They are

$$\begin{aligned}
&\rho_0 : \mu \mapsto 1 \quad \text{(the trivial representation)} \\
&\rho_1 : \mu \mapsto e^{\frac{2\pi i}{4}} = i \\
&\rho_2 : \mu \mapsto e^{\frac{2\pi i}{4} \times 2} = -1 \\
&\rho_3 : \mu \mapsto e^{\frac{2\pi i}{4} \times 3} = -i
\end{aligned}$$

Look back at Example 1.1.1. We wrote down a representation

$$\rho : \mu \mapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

After diagonalising, this became the equivalent representation

$$\rho : \mu \mapsto \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

So ρ is the direct sum of ρ_1 and ρ_3.

More generally, let G be a direct product of cyclic groups

$$G = C_{k_1} \times C_{k_2} \times \ldots \times C_{k_r}$$

G is generated by elements $\mu_1, \ldots, \mu_r$ such that $\mu_t^{k_t} = e$ and every pair μ_s, μ_t commutes. An irrep of G must be a homomorphism

$$\rho : G \to GL_1(\mathbb{C})$$

and this is determined by r numbers

$$\rho(\mu_1), \ldots, \rho(\mu_r)$$

such that $\rho(\mu_t)^{k_t} = 1$ for all t, i.e. $\rho(\mu_t) = e^{\frac{2\pi i}{k_t} q_t}$ for some $q_t \in [0, \ldots, k_t - 1]$. This gives $k_1 \times \ldots \times k_r$ 1-dimensional irreps. We label them $\rho_{q_1,\ldots,q_r}$ where

$$\rho_{q_1,\ldots,q_r} : \mu_t \mapsto e^{\frac{2\pi i}{k_t} q_t}$$

Claim 1.6.7. *All these irreps are distinct.*

Notice that the number of irreps is equal to the size of G! We'll return to this fact later.

Example 1.6.8. Let $G = C_2 \times C_2 = \langle \sigma, \tau \,|\, \sigma^2 = \tau^2 = e, \sigma\tau = \tau\sigma \rangle$. There are 4 (1-dimensional) irreps of G. They are:

$$\begin{aligned}
&\rho_{0,0} : \sigma \mapsto 1,\ \tau \mapsto 1 \quad \text{(the trivial representation)} \\
&\rho_{0,1} : \sigma \mapsto 1,\ \tau \mapsto -1 \\
&\rho_{1,0} : \sigma \mapsto -1,\ \tau \mapsto 1 \\
&\rho_{1,1} : \sigma \mapsto -1,\ \tau \mapsto -1
\end{aligned}$$

Look back at Example 1.1.2. We found a representation of $C_2 \times C_2$

$$\rho(\sigma) = \hat{S} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$
$$\rho(\tau) = \hat{T} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

So ρ is the direct sum of $\rho_{0,1}$ and $\rho_{1,0}$.

You may have heard of the fundamental result:

Theorem (Structure theorem for finite abelian groups)**.** *Every finite abelian group is a direct product of cyclic groups.*

So now we know everything (almost!) about representations of finite abelian groups. Non-abelian groups are harder...

1.7 Vector spaces of linear maps

Let V and W be vector spaces. You should recall that the set

$$\mathrm{Hom}(V, W)$$

of all linear maps from V to W is itself a vector space. If f_1, f_2 are two linear maps $V \to W$ then their sum is defined by

$$\begin{aligned} (f_1 + f_2) : V &\to W \\ x &\mapsto f_1(x) + f_2(x) \end{aligned}$$

and for a scalar $\lambda \in \mathbb{C}$, we define

$$\begin{aligned} (\lambda f_1) : V &\to W \\ x &\mapsto \lambda f_1(x) \end{aligned}$$

If $\{a_1, \ldots, a_n\}$ is a basis for V, and $\{b_1, \ldots, b_m\}$ is a basis for W, then we can define

$$\begin{aligned} f_{ji} : V &\to W \\ a_k &\mapsto \left\{ \begin{array}{ll} b_j & \text{if } k = i \\ 0 & \text{if } k \neq i \end{array} \right. \end{aligned}$$

i.e. $a_i \mapsto b_j$ and all other basis vectors go to zero.

The set $\{f_{ji} \,|\, 1 \leq i \leq n, 1 \leq j \leq m\}$ is a basis for $\mathrm{Hom}(V, W)$. In particular,

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

Once we've chosen these bases we can identify $\mathrm{Hom}(V, W)$ with the set $\mathrm{Mat}_{n\times m}(\mathbb{C})$ of $n\times m$ matrices, and $\mathrm{Mat}_{n\times m}(\mathbb{C})$ is obviously an (nm)-dimensional vector space. The maps f_{ji} correspond to the matrices which have one of their entries equal to 1 and all other entries equal to zero.

Example 1.7.1. Let $V = W = \mathbb{C}^2$, equipped with the standard basis. Then

$$\mathrm{Hom}(V, W) = \mathrm{Mat}_{2\times 2}(\mathbb{C})$$

This is a 4-dimensional vector space. The obvious basis is

$$\begin{aligned} f_{11} &= \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} & f_{12} &= \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \\ f_{21} &= \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} & f_{22} &= \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \end{aligned}$$

Now suppose that we have representations

$$\begin{aligned} \rho_V &: G \to GL(V) \\ \rho_W &: G \to GL(W) \end{aligned}$$

There is a natural representation of G on the vector space $\mathrm{Hom}(V, W)$. For $g \in G$, we define

$$\begin{aligned} \rho_{\mathrm{Hom}(V,W)}(g) : \mathrm{Hom}(V, W) &\to \mathrm{Hom}(V, W) \\ f &\mapsto \rho_W(g) \circ f \circ \rho_V(g^{-1}) \end{aligned}$$

Clearly, $\rho_{\mathrm{Hom}(V,W)}(g)(f)$ is a linear map $V \to W$.

Claim 1.7.2. *$\rho_{\mathrm{Hom}(V,W)}(g)$ is a linear map from $\mathrm{Hom}(V, W)$ to $\mathrm{Hom}(V, W)$.*

We need to check that

(i) For all g, $\rho_{\mathrm{Hom}(V,W)}(g)$ is invertible.

(ii) The map $g \mapsto \rho_{\mathrm{Hom}(V,W)}(g)$ is a homomorphism.

Observe that

$$\begin{aligned}\rho_{\mathrm{Hom}(V,W)}(h) \circ \rho_{\mathrm{Hom}(V,W)}(g) : f \mapsto &\ \rho_W(h) \circ (\rho_W(g) \circ f \circ \rho_V(g^{-1})) \circ \rho_V(h^{-1}) \\ &= \rho_W(hg) \circ f \circ \rho_V(g^{-1}h^{-1}) \\ &= \rho_{\mathrm{Hom}(V,W)}(hg)(f)\end{aligned}$$

In particular,

$$\begin{aligned}\rho_{\mathrm{Hom}(V,W)}(g) \circ \rho_{\mathrm{Hom}(V,W)}(g^{-1}) &= \rho_{\mathrm{Hom}(V,W)}(e) \\ &= \mathbf{1}_{\mathrm{Hom}(V,W)} \\ &= \rho_{\mathrm{Hom}(V,W)}(g^{-1}) \circ \rho_{\mathrm{Hom}(V,W)}(g)\end{aligned}$$

So $\rho_{\mathrm{Hom}(V,W)}(g^{-1})$ is inverse to $\rho_{\mathrm{Hom}(V,W)}(g)$. So we have a function

$$\rho_{\mathrm{Hom}(V,W)} : G \to GL(\mathrm{Hom}(V,W))$$

and it's a homomorphism, so we indeed have a representation.

Suppose we pick bases for V and W, so ρ_V and ρ_W become matrix representations

$$\begin{aligned}\rho_V &: G \to GL_n(\mathbb{C}) \\ \rho_W &: G \to GL_m(\mathbb{C})\end{aligned}$$

Then $\mathrm{Hom}(V,W) = \mathrm{Mat}_{n\times m}(\mathbb{C})$ and

$$\rho_{\mathrm{Hom}(V,W)}(g) : \mathrm{Mat}_{n\times m}(\mathbb{C}) \to \mathrm{Mat}_{n\times m}(\mathbb{C})$$

is the linear map

$$M \mapsto \rho_W(g) M (\rho_V(g))^{-1}$$

Example 1.7.3. Let $G = C_2$, and let $V = \mathbb{C}^2$ be the regular representation, and W be the 2-dimensional trivial representation. So

$$\rho_V(\tau) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad \rho_W(\tau) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Then $\mathrm{Hom}(V,W) = \mathrm{Mat}_{2\times 2}(\mathbb{C})$, and $\rho_{\mathrm{Hom}(V,W)}(\tau)$ is the linear map

$$\begin{aligned}\rho_{\mathrm{Hom}(V,W)}(\tau) : \mathrm{Mat}_{2\times 2}(\mathbb{C}) &\to \mathrm{Mat}_{2\times 2}(\mathbb{C}) \\ M &\mapsto \rho_W(\tau) M \rho_V(\tau)^{-1} = M \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\end{aligned}$$

$\rho_{\mathrm{Hom}(V,W)}$ is a 4-dimensional representation of C_2. If we choose a basis for $\mathrm{Hom}(V,W)$, we get a 4-dimensional matrix representation

$$\rho_{\mathrm{Hom}(V,W)} : C_2 \to GL_4(\mathbb{C})$$

Let's use our standard basis for $\mathrm{Hom}(V,W)$. We have:

$$\begin{aligned}\rho_{\mathrm{Hom}(V,W)}(\tau) : \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} &\mapsto \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} &\mapsto \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \\ \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} &\mapsto \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} &\mapsto \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\end{aligned}$$

So in this basis, $\rho_{\mathrm{Hom}(V,W)}(\tau)$ is given by the matrix

$$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

When V and W have representations of G, we are particularly interested in the G-linear maps from V to W. They form a subset of $\mathrm{Hom}(V,W)$.

Claim 1.7.4. *The set of G-linear maps from V to W is a subspace of* $\mathrm{Hom}(V,W)$.

In particular, the set of G-linear maps from V to W is a vector space. We call it

$$\mathrm{Hom}_G(V,W)$$

In fact, $\mathrm{Hom}_G(V,W)$ is a subrepresentation of $\mathrm{Hom}(V,W)$.

Definition 1.7.5. Let $\rho : G \to GL(V)$ be any representation. We define the **invariant subrepresentation**

$$V^G \subset V$$

to be the set

$$\{x \in V \mid \ \rho(g)(x) = x, \quad \forall g \in G\}$$

It's easy to check that V^G is actually a subspace of V, and it's obvious that it's also a subrepresentation (this justifies the name). It's isomorphic to a trivial representation.

Proposition 1.7.6. *Let $\rho_V : G \to GL(V)$ and $\rho_W : G \to GL(W)$ be representations. Then*

$$\mathrm{Hom}_G(V, W) \subset \mathrm{Hom}(V, W)$$

is exactly the invariant subrepresentation $\mathrm{Hom}(V, W)^G$ *of* $\mathrm{Hom}(V, W)$

Proof. Let $f \in \mathrm{Hom}(V, W)$. Then f is in the invariant subrepresentation $\mathrm{Hom}(V, W)^G$ iff we have

$$\begin{aligned} & f = \rho_{\mathrm{Hom}(V,W)}(g)(f) = \rho_W(g) \circ f \circ \rho_V(g^{-1}) && \forall g \in G \\ \iff \quad & f \circ \rho_V(g) = \rho_W(g) \circ f && \forall g \in G \end{aligned}$$

which is exactly the condition that f is G-linear. □

Example 1.7.7. As in Example 1.7.3, let $G = C_2$, $V = \mathbb{C}^2$ be the regular representation and $W = \mathbb{C}^2$ be the 2-dimensional trivial representation. Then

$$M \in \mathrm{Hom}(V, W) = \mathrm{Mat}_{2\times 2}(\mathbb{C})$$

is in the invariant subrepresentation if and only if

$$\rho_{\mathrm{Hom}(V,W)}(\tau)(M) = M$$

In the standard basis $\rho_{\mathrm{Hom}(V,W)}$ is a 4×4-matrix and the invariant subrepresentation is the eigenspace of this matrix with eigenvalue 1. This is spanned by

$$\begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} \quad \& \quad \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}$$

So $\mathrm{Hom}_G(V, W) = (\mathrm{Hom}(V, W))^G$ is 2-dimensional. It's spanned by

$$\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} \quad \in \mathrm{Mat}_{2\times 2}(\mathbb{C})$$

Now we can (partially) explain the clever formula in Maschke's Theorem, when we cooked up a G-linear projection f out of a linear projection $\tilde{f}$.

Proposition 1.7.8. *Let $\rho : G \to GL(V)$ be any representation. Consider the linear map*

$$\begin{aligned} \Psi : & V \to V \\ & x \mapsto \frac{1}{|G|} \sum_{g \in G} \rho(g)(x) \end{aligned}$$

Then Ψ is a G-linear projection from V onto V^G.

Proof. First we need to check that $\Psi(x) \in V^G$ for all x. For any $h \in G$,

$$\begin{aligned} \rho(h)(\Psi(x)) &= \frac{1}{|G|} \sum_{g \in G} \rho(h)\rho(g)(x) \\ &= \frac{1}{|G|} \sum_{g} \rho(hg)(x) \\ &= \frac{1}{|G|} \sum_{g} \rho(g)(x) \qquad \text{(relabelling } g \mapsto h^{-1}g\text{)} \\ &= \Psi(x) \end{aligned}$$

So Ψ is a linear map $V \to V^G$. Next, we check it's a projection. Let $x \in V^G$. Then

$$\begin{aligned} \Psi(x) &= \frac{1}{|G|} \sum_{g} \rho(g)(x) \\ &= \frac{1}{|G|} \sum_{g} x = x \end{aligned}$$

Finally, we check that Ψ is G-linear. For $h \in G$,

$$\begin{aligned}
\Psi(\rho(h)(x)) &= \frac{1}{|G|}\sum_{g\in G}\rho(g)(h)(x) \\
&= \frac{1}{|G|}\sum_{g\in G}\rho(gh)(x) \\
&= \frac{1}{|G|}\sum_{g\in G}\rho(hg)(x) \qquad \text{(relabelling } g \mapsto hgh^{-1}) \\
&= \rho(h)\Psi(x)
\end{aligned}$$

□

As a special case, let V and W be representations of G, and consider the representation $\mathrm{Hom}(V, W)$. The above proposition gives us a G-linear projection from

$$\Psi : \mathrm{Hom}(V, W) \to \mathrm{Hom}_G(V, W)$$

In the proof of Maschke's Theorem, we applied Ψ to $\tilde{f}$ to get f. This explains why f is G-linear, but we'd still have to check that f is a projection.

1.8 More on decomposition into irreps

In Section 1.5 we proved the basic result (Corollary 1.5.9) that every representation can be decomposed into irreps. In this section, we're going to prove that this decomposition is unique. Then we're going to look at the decomposition of the regular representation, which turns out to be very powerful.

Before we can start, we need some technical lemmas.

Lemma 1.8.1. *Let U, V, W be three vector spaces. Then we have natural isomorphisms*

(i) $\mathrm{Hom}(V, U \oplus W) = \mathrm{Hom}(V, U) \oplus \mathrm{Hom}(V, W)$

(ii) $\mathrm{Hom}(U \oplus W, V) = \mathrm{Hom}(U, V) \oplus \mathrm{Hom}(W, V)$

Furthermore, if U, V, W carry representations of G, then (i) and (ii) are isomorphisms of representations.

Before we start the proof, notice that all four spaces have the same dimension, namely

$$(\dim V)(\dim W + \dim U)$$

so the statement is at least plausible!

Proof. Recall that we have inclusion and projection maps

$$U \underset{\pi_U}{\overset{\iota_U}{\rightleftarrows}} U \oplus W \underset{\iota_W}{\overset{\pi_W}{\rightleftarrows}} W$$

where

$$\iota_U : x \mapsto (x, 0)$$

$$\pi_U : (x, y) \mapsto x$$

and similarly for ι_W and π_W. From their definition, it follows immediately that

$$\iota_U \circ \pi_U + \iota_W \circ \pi_W = \mathbf{1}_{U \oplus W}$$

(i) Define

$$P : \mathrm{Hom}(V, U \oplus W) \to \mathrm{Hom}(V, U) \oplus \mathrm{Hom}(V, W)$$

by

$$P : f \mapsto (\pi_U \circ f, \pi_W \circ f)$$

In the other direction, define

$$P^{-1} : \mathrm{Hom}(V, U) \oplus \mathrm{Hom}(V, W) \to \mathrm{Hom}(V, U \oplus W)$$

by

$$P^{-1} : (f_U, f_W) \mapsto \iota_U \circ f_U + \iota_W \circ f_W$$

Claim 1.8.2. *P and P^{-1} are linear maps.*

Also, P and P^{-1} are inverse to each other (as our notation suggests!). We check that

$$\begin{aligned} P^{-1} \circ P : f \mapsto & \iota_U \circ \pi_U \circ f + \iota_W \circ \pi_W \circ f \\ &= (\iota_U \circ \pi_U + \iota_W \circ \pi_W) \circ f \\ &= f \end{aligned}$$

but both vector spaces have the same dimension, so $P \circ P^{-1}$ must also be the identity map (or you can check this directly). So P is an isomorphism of vector spaces.

Now assume we have representations ρ_V, ρ_W, ρ_U of G on V, W and U. We claim P is G-linear. Recall that

$$\rho_{\mathrm{Hom}(V,U\oplus W)}(g)(f) = \rho_{V\oplus W}(g) \circ f \circ \rho_V(g^{-1})$$

We have

$$\begin{aligned} \pi_U \circ (\rho_{\mathrm{Hom}(V,U\oplus W)}(g)(f)) &= \pi_U \circ \rho_{U\oplus W}(g) \circ f \circ \rho_V(g^{-1}) \\ &= \rho_U(g) \circ \pi_U \circ f \circ \rho_V(g^{-1}) \qquad \text{(since } \pi_U \text{ is } G\text{-linear)} \\ &= \rho_{\mathrm{Hom}(U,V)}(g)(f) \end{aligned}$$

and similarly for W, so

$$\begin{aligned} P(\rho_{\mathrm{Hom}(V,U\oplus W)}(g)(f)) &= (\pi_U \circ \rho_{\mathrm{Hom}(V,U\oplus W)}(g)(f), \pi_W \circ \rho_{\mathrm{Hom}(V,U\oplus W)}(g)(f)) \\ &= (\rho_{\mathrm{Hom}(V,U)}(g)(\pi_U \circ f), \rho_{\mathrm{Hom}(V,W)}(g)(\pi_W \circ f)) \\ &= \rho_{Hom(V,U)\oplus \mathrm{Hom}(V,W)}(g)(\pi_U \circ f, \pi_W \circ f) \end{aligned}$$

So P is G-linear, and we've proved (i).

(ii) Define

$$I : \mathrm{Hom}(U \oplus W, V) \to \mathrm{Hom}(U, V) \oplus \mathrm{Hom}(W, V)$$

by

$$I : f \mapsto f \circ \iota_U, f \circ \iota_W)$$

and

$$I^{-1} : \mathrm{Hom}(U, V) \oplus \mathrm{Hom}(W, V) \to \mathrm{Hom}(U \oplus W, V)$$

by

$$I^{-1} : (f_U, f_V) \mapsto f_U \circ \pi_U + f_W \circ \pi_W$$

Then use very similar arguments to those in (i). $\square$

Corollary 1.8.3. *If U, V, W are representations of G, then we have natural isomorphisms*

(i) $\mathrm{Hom}_G(V, U \oplus W) = \mathrm{Hom}_G(V, U) \oplus \mathrm{Hom}_G(V, W)$

(ii) $\mathrm{Hom}_G(U \oplus W, V) = \mathrm{Hom}_G(U, V) \oplus \mathrm{Hom}_G(W, V)$

There are two ways to prove this corollary. We'll just give the proofs for (i), the proofs for (ii) are identical.

1st proof. By Lemma 1.8.1, we have a isomorphism of representations

$$P : \mathrm{Hom}(V, U \oplus W) \to \mathrm{Hom}(V, U) \oplus \mathrm{Hom}(V, W)$$

Suppose $f \in \mathrm{Hom}(V, U \oplus W)$ is actually G-linear. Then since π_U and π_W are G-linear, we have that

$$P(f) \in \mathrm{Hom}_G(V, U) \oplus \mathrm{Hom}_G(V, W)$$

Now suppose that $f_U \in \mathrm{Hom}(V, U)$ and $f_W \in \mathrm{Hom}(V, W)$ are both G-linear. Then

$$P^{-1}(f_U, f_W) \in \mathrm{Hom}_G(V, U \oplus W)$$

because ι_U and ι_W are G-linear and the sum of two G-linear maps is G-linear. Hence P and P^{-1} define inverse linear maps between the two sides of (i). □

2nd proof. We have a G-linear isomorphism

$$P : \mathrm{Hom}(V, U \oplus W) \to \mathrm{Hom}(V, U) \oplus \mathrm{Hom}(V, W)$$

Thus P must induce an isomorphism between the invariant subrepresentations of each side. From Proposition 1.7.6, the invariant subrepresentation on the left-hand-side is

$$\mathrm{Hom}(V, U \oplus W)^G = \mathrm{Hom}_G(V, U \oplus W)$$

For the right-hand-side, we have

$$(\mathrm{Hom}(V, U) \oplus \mathrm{Hom}(V, W))^G = \mathrm{Hom}(V, U)^G \oplus \mathrm{Hom}(V, W)^G$$

(this is true for any direct sum of representations) which is the same as

$$\mathrm{Hom}_G(V, U) \oplus \mathrm{Hom}_G(V, W)$$

□

Now that we've dealt with these technicalities, we can get back to learning more about the decompostion of representations into irreps.

Let V and W be irreps of G. Recall Schur's Lemma (Theorem 1.6.1), which tells us a lot about the G-linear maps between V and W and between V and V. Here's another way to say it:

Proposition 1.8.4. *Let V and W be irreps of G. Then*

$$\dim \operatorname{Hom}_G(V, W) = \begin{cases} 0 & \text{if } V \text{ and } W \text{ aren't isomorphic} \\ 1 & \text{if } V \text{ and } W \text{ are isomorphic} \end{cases}$$

Proof. Suppose V and W aren't isomorphic. Then by Schur's Lemma, the only G-linear map from V to W is the zero map, so

$$\operatorname{Hom}_G(V, W) = \{0\}$$

Alternatively, suppose that $f_0 : V \to W$ is an isomorphism. Then for any $f \in \operatorname{Hom}_G(V, W)$:

$$f_0^{-1} \circ f \in \operatorname{Hom}_G(V, V)$$

So by Schur's Lemma, $f_0^{-1} \circ f = \lambda \mathbf{1}_V$, i.e. $f = \lambda f_0$. So f_0 spans $\operatorname{Hom}_G(V, W)$. □

Proposition 1.8.5. *Let $\rho : G \to GL(V)$ be a representation, and let*

$$V = U_1 \oplus \ldots \oplus U_s$$

be a decomposition of V into irreps. Let W be any irrep of G. Then the number of irreps in the set $\{U_1, \ldots, U_s\}$ which are isomorphic to W is equal to the dimension of $\operatorname{Hom}_G(W, V)$. It's also equal to the dimension of $\operatorname{Hom}_G(V, W)$.

Proof. By Corollary 1.8.3,

$$\operatorname{Hom}_G(W, V) = \bigoplus_{i=1}^{s} \operatorname{Hom}_G(W, U_i)$$

so

$$\dim \operatorname{Hom}_G(W, V) = \sum_{i=1}^{s} \dim \operatorname{Hom}_G(W, U_i)$$

By Proposition 1.8.4, this equals the number of irreps in $\{U_1, \ldots, U_s\}$ that are isomorphic to W. An identical argument works if we consider $\operatorname{Hom}_G(V, W)$ instead. □

Now we can prove uniqueness of irrep decomposition.

Theorem 1.8.6. *Let $\rho : G \to GL(V)$ be a representation, and let*

$$V = U_1 \oplus \ldots \oplus U_s$$
$$V = \hat{U}_1 \oplus \ldots \oplus \hat{U}_r$$

be two decompositions of V into irreducible subrepresentations. Then the two sets of irreps $\{U_1, \ldots, U_s\}$ and $\{\hat{U}_1, \ldots, \hat{U}_r\}$ are the same, i.e. $s = r$ and (possibly after reordering) U_i and $\hat{U}_i$ are isomorphic for all i.

Proof. Let W be any irrep of G. By Proposition 1.8.5, the number of irreps in the first decomposition that are isomorphic to W is equal to $\dim \mathrm{Hom}_G(W, V)$. But the number of irreps in the second decomposition that are isomorphic to W is also equal to $\dim \mathrm{Hom}_G(W, V)$. So for any irrep W, the two decompositions contain the same number of factors isomorphic to W. □

Example 1.8.7. Let $G = S_3$. So far, we've met three irreps of this group. Let

$$\rho_1 : S_3 \to GL(U_1)$$

the 1-dimensional trivial representation, let

$$\rho_2 : S_3 \to GL(U_2)$$

be the sign representation (see Example 1.3.6), which is also 1-dimensional, and let

$$\rho_3 : S_3 \to GL(U_3)$$

be the 2-dimensional irrep from Example 1.5.10. For any non-negative integers a, b, c we can form the representation

$$U_1^{\oplus a} \oplus U_2^{\oplus b} \oplus U_3^{\oplus c}$$

By the above theorem, all of these representations are distinct.

So if we know all the irreps of a group G (up to isomorphism), then we know all the representations of G: each representation can be described, uniquely, as a direct sum of some number of copies of each irrep. This is similar to the relationship between integers and prime numbers: each integer can be written uniquely as a product of prime numbers, with each prime occuring with some multiplicity. However, there are infinitely many prime numbers! As we shall see shortly, the situation for representations of G is much simpler.

In Section 1.3 we constructed the regular representation of any group G. We take a vector space V_{reg} which has a basis

$$\{b_g \mid g \in G\}$$

(so $\dim V_{reg} = |G|$), and define

$$\rho_{reg} : G \to GL(V_{reg})$$

by

$$\rho_{reg}(h) : b_g \mapsto b_{hg}$$

(and extending linearly). We claimed that this representation was very important. Here's why:

Theorem 1.8.8. *Let $V_{reg} = U_1 \oplus \ldots \oplus U_s$ be the decomposition of V_{reg} as a direct sum of irreps. Then for any irrep W of G, the number of factors in the decomposition that are isomorphic to W is equal to* $\dim W$*.*

Before we look at the proof, let's note the most important corollary of this result.

Corollary 1.8.9. *Any group G has only finitely many irreducible representations (up to isomorphism).*

Proof. Every irrep occurs in the decomposition of V_{reg} at least once, and $\dim V_{reg}$ is finite. □

So for any group G there is a finite list $U_1, ..., U_r$ of irreps of G (up to isomorphism), and every representation of G can be written uniquely as a direct sum

$$U_1^{\oplus a_1} \oplus ... \oplus U_r^{a_r}$$

for some non-negative integers $a_1, ..., a_r$. In particular, Theorem 1.8.8 says that V_{reg} decomposes as

$$V_{reg} = U_1^{\oplus d_1} \oplus ... \oplus U_r^{\oplus d_r}$$

where

$$d_i = \dim U_i$$

Example 1.8.10. Let $G = S_3$, and let U_1, U_2, U_3 be the three irreps of S_3 from Example 1.8.7. The regular representation V_{reg} of S_3 decomposes as

$$V_{reg} = U_1 \oplus U_2 \oplus U_3^{\oplus 2} \oplus ...$$

But $\dim V_{reg} = |S_3| = 6$, and

$$\dim(U_1 \oplus U_2 \oplus U_3^{\oplus 2}) = 1 + 1 + 2 \times 2 = 6$$

so there cannot be any other irreps of S_3.

The proof of Theorem 1.8.8 follows easily from the following:

Lemma 1.8.11. *For any representation W of G, we have a natural isomorphism of vector spaces*

$$\mathrm{Hom}_G(V_{reg}, W) = W$$

Proof. Recall that we have a basis vector $b_e \in V_{reg}$ corresponding to the identity element in G. Define a function

$$T : \mathrm{Hom}_G(V_{reg}, W) \to W$$

by 'evaluation at b_e', i.e.

$$T : f \to f(b_e)$$

Let's check that T is linear. We have

$$T(f_1 + f_2) = (f_1 + f_2)(b_e) = f_1(b_e) + f_2(b_e) = T(f_1) + T(f_2)$$

and

$$T(\lambda f) = (\lambda f)(b_e) = \lambda f(b_e) = \lambda T(f)$$

so it is indeed linear. Now let's check that T is an injection. Suppose that $f \in \mathrm{Hom}_G(V_{reg}, W)$, and that $T(f) = f(b_e) = 0$. Then for any basis vector $b_g \in V_{reg}$, we have

$$f(b_g) = f(\rho_{reg}(g)(b_e)) = \rho_W(g)(f(b_e)) = 0$$

So f sends every basis vector to zero, so it must be the zero map. Hence T is indeed an injection. Finally, we need to check that T is a surjection, so we need to show that for any $x \in W$ there is a G-linear map f from V_{reg} to W such that $f(b_e) = x$. Fix an $x \in W$, and define a linear map

$$f : V_{reg} \to W$$

by

$$f : b_g \mapsto \rho_W(g)(x)$$

Then in particular $f(b_e) = x$, so we just need to check that f is G-linear. But for any $h \in G$, we have

$$\begin{aligned} f \circ \rho_{reg}(h) :\ & b_g \mapsto \rho_W(hg)(x) \\ \rho_W(h) \circ f :\ & b_g \mapsto \rho_W(h)(\rho_W(g)(x)) = \rho_W(hg)(x) \end{aligned}$$

So $f \circ \rho_{reg}(h) = \rho_W(h) \circ f$, since both maps are linear and they agree on the basis. Thus f is indeed G-linear, and we have proved that T is a surjection. $\square$

Proof of Theorem 1.8.8. Let $V_{reg} = U_1 \oplus \ldots \oplus U_s$ be the decomposition of the regular representation into irreps. Let W be any irrep of G. By Proposition 1.8.5, we have that $\dim \mathrm{Hom}_G(V_{reg}, W)$ equals the number of U_i that are isomorphic to W. But by Lemma 1.8.11,

$$\dim \mathrm{Hom}_G(V_{reg}, W) = \dim W$$

$\square$

Corollary 1.8.12. *Let $U_1, \ldots, U_r$ be all the irreps of G, and let $\dim U_i = d_i$. Then*

$$\sum_{i=1}^{r} d_i^2 = |G|$$

Proof. By Theorem 1.8.8,

$$V_{reg} = U_1^{\oplus d_1} \oplus \ldots \oplus U_r^{\oplus d_r}$$

Now take dimensions of each side. $\square$

Notice this is consistent with out results on abelian groups. If G is abelian, $d_i = 1$ for all i, so this formula says that

$$r = \sum_{i=1}^{r} d_i^2 = |G|$$

i.e. the number of irreps of G is the size of G. This is what we found.

Example 1.8.13. Let $G = S_4$. Let $U_1, \ldots, U_r$ be all the irreps of G, with dimensions $d_1, \ldots, d_r$. Let U_1 be the 1-dimensional trivial representation and U_2 be the sign representation, so $d_1 = d_2 = 1$. For any symmetric group S_n these are the only possible 1-dimensional representations (see Problem Sheets), so we must have $d_i > 1$ for $i \geq 3$. We have:

$$\begin{aligned} d_1^2 + \ldots + d_r^2 &= |G| = 24 \\ \Rightarrow \quad d_3^2 + \ldots + d_r^2 &= 22 \end{aligned}$$

This has only 1 solution. Obviously $d_k \leq 4$ for all k, as $5^2 = 25$. Suppose that $d_r = 4$, then we would have

$$d_3^2 + \ldots + d_{r-1}^2 = 22 - 16 = 6$$

This is impossible, so actually $d_k \in [2,3]$ for all k. The number of k such that $d_k = 3$ must be even because 22 is even, and we can't have $d_k = 2$ for all k since $4 \nmid 22$. Therefore, the only possibility is that $d_3 = 2, d_4 = 3$ and $d_5 = 3$. So G has 5 irreps with these dimensions.

Example 1.8.14. Let $G = D_4$. Let the irreducible representations be $U_1, \ldots, U_r$ with dimensions $d_1, \ldots, d_r$. As usual, let U_1 be the 1-dimensional trivial representation. So

$$d_2^2 + \ldots + d_r^2 = |G| - 1 = 7$$

So either

(i) $r = 8$, and $d_i = 1 \;\; \forall i$

(ii) $r = 5$, and $d_2 = d_3 = d_4 = 1, d_5 = 2$

In the Problem Sheets we show that D_4 has a 2-dimensional irrep, so in fact (ii) is true. The 2-dimensional irrep U_5 is the representation we constructed in Example 1.3.7 by thinking about the action of D_4 on a square. If we present D_4 as $\langle \sigma, \tau \mid \sigma^4 = \tau^2 = e, \tau\sigma\tau = \sigma^{-1} \rangle$ then the 4 1-dimensional irreps are given by

$$\begin{aligned} \rho_{ij} : &\sigma \mapsto (-1)^i \\ &\tau \mapsto (-1)^j \end{aligned}$$

for $i, j \in \{0, 1\}$.

1.9 Duals and tensor products

Let V be a vector space. Recall the definition of the **dual vector space**:

$$V^* = \mathrm{Hom}(V, \mathbb{C})$$

This is a special case of $\mathrm{Hom}(V, W)$ where $W = \mathbb{C}$. So $\dim V^* = \dim V$, and if $\{b_1, \ldots, b_n\}$ is a basis for V, then there is a **dual basis** $\{f_1, \ldots, f_n\}$ for V defined by

$$f_i(b_j) = \begin{cases} 1 & \text{if} \quad i = j \\ 0 & \text{if} \quad i \neq j \end{cases}$$

Now let $\rho_V : G \to GL(V)$ be a representation, and let $\mathbb{C}$ carry the (1-dimensional) trivial representation of G. Then we know that V^* carries a representation of G, defined by

$$\rho_{\mathrm{Hom}(V,\mathbb{C})}(g) : f \mapsto f \circ \rho_V(g^{-1})$$

We'll denote this representation by $(\rho_V)^*$, we call it the **dual representation** to ρ_V.

Another way to say it is that we define

$$(\rho_V)^*(g) : V^* \to V^*$$

to be the dual map to

$$\rho_V(g^{-1}) : V \to V$$

If we have a basis for V, so $\rho_V(g)$ is a matrix, then $\rho_V^*(g)$ is described in the dual basis by the matrix

$$\rho_V(g)^{-T}$$

Example 1.9.1. Let $G = S_3 = \langle \sigma, \tau \mid \sigma^3 = \tau^2 = e, \tau\sigma\tau = \sigma^{-1} \rangle$ and let ρ be the 2-dimensional irrep of G. In the appropriate basis (see Problem Sheets)

$$\rho(\sigma) = \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix} \quad (\text{where } \omega = e^{\frac{2\pi i}{3}})$$
$$\rho(\tau) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

The dual representation (in the dual basis) is

$$\rho^*(\sigma) = \begin{pmatrix} \omega^{-1} & 0 \\ 0 & \omega \end{pmatrix}$$
$$\rho(\tau) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

This is equivalent to ρ under the change of basis

$$P = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

So in this case, ρ^* and ρ are isomorphic.

Example 1.9.2. Let $G = C_3 = \langle \mu \mid \mu^3 = e \rangle$ and consider the 1-dimensional representation

$$\rho_1 : \mu \mapsto \omega = e^{\frac{2\pi i}{3}}$$

The dual representation is

$$\rho_1^* : \mu \mapsto \omega^{-1} = e^{\frac{4\pi i}{3}}$$

So in this case,

$$\rho_1^* = \rho_2$$

In particular, ρ_1 and ρ_1^* are not isomorphic.

You should recall that $(V^*)^*$ is naturally isomorphic to V as a vector space. The isomorphism is given by

$$\begin{aligned} \Phi : &V \to (V^*)^* \\ &x \mapsto \Phi_x \end{aligned}$$

where

$$\begin{aligned}\Phi_x : & V^* \to \mathbb{C} \\ & f \mapsto f(x)\end{aligned}$$

We claim Φ is G-linear. Pick $x \in V$, and consider $\Phi(\rho_V(g)(x))$. This is the map

$$\begin{aligned}\Phi_{\rho_V(g)(x)} : & V^* \to \mathbb{C} \\ & f \mapsto f\left(\rho_V(g)(x)\right)\end{aligned}$$

Now consider $(\rho_{V^*})^*(g)(\Phi(x))$. By definition, this is the map

$$\begin{aligned}\Phi_x \circ \rho_{V^*}(g^{-1}) : & V^* \to \mathbb{C} \\ & f \mapsto \Phi_x\left(\rho_{V^*}(g^{-1})(f)\right) \\ & = \Phi_x\left(f \circ \rho_V(g)\right) \\ & = \left(f \circ \rho_V(g)\right)(x)\end{aligned}$$

So $\Phi\left(\rho_V(g)(x)\right)$ and $(\rho_{V^*})^*(g)\left(\Phi(x)\right)$ are the same element of $(V^*)^*$, so Φ is indeed G-linear. Therefore, $(V^*)^*$ and V are naturally isomorphic as representations.

Proposition 1.9.3. *Let V carry a representation of G. Then V is irreducible if and only if V^* is irreducible.*

Proof. Suppose V is not irreducible, i.e. it contains a non-trivial subrepresentation $U \subset V$. By Maschke's Theorem, there exists another subrepresentation $W \subset V$ such that $V = U \oplus W$. By Corollary 1.8.3, this implies $V^* = U^* \oplus W^*$, so V^* is not irreducible. By the same argument, if V^* is not irreducible then neither is $(V^*)^* = V$. □

So 'taking duals' gives an order-2 permutation of the set of irreps of G.

Next we're going to define tensor products. There are several ways to define these, of varying degrees of sophistication. We'll start with a very concrete definition.

Let V and W be two vector spaces and assume we have bases $\{a_1, \ldots, a_n\}$ for V and $\{b_1, \ldots, b_m\}$ for W.

Definition 1.9.4. The **tensor product** of V and W is the vector space which has a basis given by the set of symbols

$$\{a_i \otimes b_t \mid 1 \leq i \leq n, 1 \leq t \leq m\}$$

We write the tensor product of V and W as

$$V \otimes W$$

By definition, $\dim(V \otimes W) = (\dim V)(\dim W)$. If we have vectors $x \in V$ and $y \in W$, we can define a vector

$$x \otimes y \in V \otimes W$$

as follows. Write x and y in the given bases, so

$$\begin{aligned} x &= \lambda_1 a_1 + \ldots + \lambda_n a_n \\ y &= \mu_1 b_1 + \ldots + \mu_m b_m \end{aligned}$$

for some coefficients $\lambda_i, \mu_t \in \mathbb{C}$. Then we define

$$x \otimes y = \sum_{\substack{i \in [1,n] \\ t \in [1,m]}} \lambda_i \mu_t \, a_i \otimes b_t$$

(think of expanding out the brackets). Now let V and W carry representations of G. We can define a representation of G on $V \otimes W$, called the **tensor product representation**. We let

$$\rho_{V \otimes W}(g) : V \otimes W \to V \otimes W$$

be the linear map defined by

$$\rho_{V \otimes W}(g) : a_i \otimes b_t \mapsto \rho_V(g)(a_i) \otimes \rho_W(g)(b_t)$$

Suppose $\rho_V(g)$ is described by the matrix M (in this given basis), and $\rho_W(g)$ is described by the matrix N. Then

$$\begin{aligned} \rho_{V \otimes W}(g) : a_i \otimes b_t \mapsto & \left(\sum_{j=1}^{n} M_{ji} a_j \right) \otimes \left(\sum_{s=1}^{m} N_{st} b_s \right) \\ &= \sum_{\substack{j \in [1,n] \\ s \in [1,m]}} M_{ji} N_{st} \, a_j \otimes b_s \end{aligned}$$

So $\rho_{V\otimes W}(g)$ is described by the $nm \times nm$ matrix $M \otimes N$, whose entries are

$$[M \otimes N]_{js,it} = M_{ji} N_{st}$$

This notation can be quite confusing! This matrix has $n \times m$ rows, and to specify a row we have to give a pair of numbers (j, s), where $1 \leq j \leq n$ and $1 \leq s \leq m$. When we write js above, we mean this pair of numbers, we don't mean their product. Similiarly to specify a column we have to give another pair of numbers (i, t). Fortunately we won't have to use this notation much.

We haven't checked that $\rho_{V\otimes W}$ is a homomorphism. However, there is a more fundamental question: how do we know that this construction is independent of our choice of bases? Both questions are answered by the following:

Proposition 1.9.5. *$V \otimes W$ is isomorphic to* $\mathrm{Hom}(V^*, W)$.

We can view this proposition as an alternative definition for $V \otimes W$. It's better because it doesn't require us to choose bases for our vector spaces, but it's less explicit.

[Aside: this definition only works for finite-dimensional vector spaces. There are other basis-independent definitions that work in general, but they're even more abstract.]

Proof. Let $\{\alpha_1, \ldots, \alpha_n\}$ be the basis for V^* dual to $\{a_1, \ldots, a_n\}$. Then $\mathrm{Hom}(V^*, W)$ has a basis $\{f_{ti} \mid 1 \leq i \leq n, 1 \leq t \leq m\}$ where

$$\begin{aligned} f_{ti} : &\alpha_i \mapsto b_t \\ &\alpha_{\neq i} \mapsto 0 \end{aligned}$$

Define an isomorphism of vector spaces between $\mathrm{Hom}(V^*, W)$ and $V \otimes W$ by mapping

$$f_{ti} \mapsto a_i \otimes b_t$$

To prove the proposition it's sufficient to check that the representation $\rho_{\mathrm{Hom}(V^*,W)}$ agrees with the definition of $\rho_{V\otimes W}$ when we write it in the basis $\{f_{ti}\}$. Pick $g \in G$ and let $\rho_V(g)$ and $\rho_W(g)$ be described by matrices M and N in the given bases. By definition,

$$\rho_{\mathrm{Hom}(V^*,W)}(g) : f_{ti} \mapsto \rho_W(g) \circ f_{ti} \circ \rho_{V^*}(g^{-1})$$

Now

$$\rho_{V^*}(g^{-1}) : \alpha_k \mapsto \sum_{j=1}^{n} M_{kj}\alpha_j$$

because $\rho_{V^*}(g^{-1})$ is given by the matrix M^T in the dual basis. So

$$f_{ti} \circ \rho_{V^*}(g^{-1}) : \alpha_k \mapsto M_{ki} b_t$$

and

$$\rho_W(g) \circ f_{ti} \circ \rho_{V^*}(g^{-1}) : \alpha_k \mapsto M_{ki}\left(\sum_{j=1}^{m} N_{st} b_s\right)$$

Therefore, if we write $\rho_W(g) \circ f_{ti} \circ \rho_{V^*}(g^{-1})$ in terms of the basis $\{f_{sj}\}$, we have

$$\rho_W(g) \circ f_{ti} \circ \rho_{V^*}(g^{-1}) = \sum_{\substack{j\in[1,n]\\ s\in[1,m]}} M_{ji} N_{st} f_{sj}$$

(since both sides agree on each basis vector α_k) and this is exactly the formula for the tensor product representation $\rho_{V\otimes W}$. □

Corollary 1.9.6. $\mathrm{Hom}(V, W)$ *is isomorphic to* $V^* \otimes W$.

Proof.

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

□

In general, tensor products are hard to calculate, but there is an easy special case, namely when the vector space V is 1-dimensional. Then for any $g \in G$, $\rho_V(g)$ is just a scalar, so if $\rho_W(g)$ is described by a matrix N (in some basis), then $\rho_{V\otimes W}$ is described by the matrix $\rho_V(g)N$.

Example 1.9.7. Let $G = S_3$, and W be the 2-dimensional irrep, so

$$\rho_W(\sigma) = \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix}, \quad \rho_W(\tau) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Let V be the 1-dimensional sign representation, so

$$\rho_V(\sigma) = 1, \quad \rho_V(\tau) = -1$$

Then $V \otimes W$ is given by

$$\rho_{V\otimes W}(\sigma) = \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix}, \quad \rho_{V\otimes W}(\tau) = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$$

In general, the tensor product of two irreducible representations will not be irreducible. For example, if W is the 2-dimensional irrep of S_3 as above, then $W \otimes W$ is 4-dimensional and so cannot possibly be an irrep. However,

Claim 1.9.8. *If V is 1-dimensional, then $V \otimes W$ is irreducible iff W is irreducible.*

Therefore in the above example the 2-dimensional representation $V \otimes W$ is irreducible. We know that there's only one 2-dimensional irrep of S_3, so $V \otimes W$ must be isomorphic to W. Find the change-of-basis matrix!

2 Characters

2.1 Basic properties

Let M be an $n \times n$ matrix. Recall that the **trace** of M is

$$\mathrm{Tr}(M) = \sum_{i=1}^{n} M_{ii}$$

If N is another $n \times n$ matrix, then

$$\mathrm{Tr}(NM) = \sum_{i,j=1}^{n} N_{ij} M_{ji} = \mathrm{Tr}(MN)$$

which implies that

$$\mathrm{Tr}(P^{-1}MP) = \mathrm{Tr}(PP^{-1}M) = \mathrm{Tr}(M)$$

Definition 2.1.1. Let V be a vector space, and

$$f : V \to V$$

a linear map. Pick a basis for V and let M be the matrix describing f in this basis. We define

$$\mathrm{Tr}(f) = \mathrm{Tr}(M)$$

This definition does not depend on the choice of basis, because choosing a different basis will produce a matrix which is conjugate to M, and hence has the same trace.

Now let G be a group, and let ρ be a representation

$$\rho : V \to GL(V)$$

on a vector space V.

Definition 2.1.2. The **character** of the representation ρ is the function

$$\begin{aligned} \chi_\rho :& G \to \mathbb{C} \\ & g \mapsto \mathrm{Tr}\left(\rho(g)\right) \end{aligned}$$

Notice that χ_ρ is not a homomorphism in general, since generally

$$\mathrm{Tr}(MN) \neq \mathrm{Tr}(M)\,\mathrm{Tr}(N)$$

Example 2.1.3. Let $G = C_2 \times C_2 = \langle \sigma, \tau \mid \sigma^2 = \tau^2 = e, \sigma\tau = \tau\sigma \rangle$. Let ρ be the direct sum of $\rho_{1,0}$ and $\rho_{1,1}$, so

$$\rho(e) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \rho(\sigma) = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$
$$\rho(\tau) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \rho(\sigma\tau) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

Then

$$\begin{aligned} \chi_\rho :& \rho \mapsto 2 \\ & \sigma \mapsto -2 \\ & \tau \mapsto 0 \\ & \sigma\tau \mapsto 0 \end{aligned}$$

Proposition 2.1.4. *Isomorphic representations have the same character.*

Proof. In Proposition 1.4.3 we showed that if two representations are isomorphic, then there exist bases in which they are described by the same matrix representation. □

Later on we'll prove the converse to this statement, that if two representations have the same character, then they're isomorphic!

Proposition 2.1.5. *Let $\rho : G \to GL(V)$ be a representation of dimension d, and let χ_ρ be its character. Then*

(i) If g and h are conjugate in G then

$$\chi_\rho(g) = \chi_\rho(h)$$

(ii) For any $g \in G$

$$\chi_\rho\left(g^{-1}\right) = \overline{\chi_\rho(g)}$$

(iii) $\chi_\rho(e) = d$

(iv) For all $g \in G$,

$$|\chi_\rho(g)| \leq d$$

and $|\chi_\rho(g)| = d$ if and only if $\rho(g) = \lambda \mathbf{1}_V$ for some $\lambda \in \mathbb{C}$

Proof. (i) Suppose $g = \mu^{-1}h\mu$ for some $\mu \in G$. Then

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

So in any basis, the matrices for $\rho(g)$ and $\rho(h)$ are conjugate, so

$$\mathrm{Tr}\left(\rho(g)\right) = \mathrm{Tr}\left(\rho(h)\right)$$

This says that χ_ρ is a **class function**, more on these later.

(ii) Let $g \in G$ and let the order of g be k. By Corollary 1.6.4, there exists a basis of V such that $\rho(g)$ becomes a diagonal matrix. Let $\lambda_1, \ldots, \lambda_d$ be the diagonal entries (i.e. the eigenvalues of $\rho(g)$). Then each λ_i is a kth root of unity, so $|\lambda_i| = 1$, so $\lambda_i^{-1} = \overline{\lambda_i}$. Then

$$\chi_\rho(g^{-1}) = \mathrm{Tr}\left(\rho(g^{-1})\right) = \sum_{i=1}^{d} \lambda_i^{-1} = \sum_{i=1}^{d} \overline{\lambda_i} = \overline{\chi_\rho(g)}$$

(iii) In every basis, $\rho(e)$ is the $d \times d$ identity matrix.

(iv) Using the same notation as in (ii), we have

$$|\chi_\rho(g)| = \left|\sum_{i=1}^{d} \lambda_i\right| \leq \sum_{i=1}^{d} |\lambda_i| = d$$

by the triangle inequality. Furthermore, equality holds iff

$$\begin{aligned} &\arg(\lambda_i) = \arg(\lambda_j) \quad \text{for all } i, j \\ \iff &\lambda_i = \lambda_j \quad \text{for all } i, j \ \ (\text{since } |\lambda_i| = |\lambda_j| = 1) \\ \iff &\rho(g) = \lambda \mathbf{1}_V \ \ \text{for some } \lambda \in \mathbb{C} \end{aligned}$$

□

Property (iv) is enough to show:

Corollary 2.1.6. *Let ρ be a representation of G (of dimension d), and let χ_ρ be its character. Then for any $g \in G$*

$$\rho(g) = \mathbf{1} \quad \iff \quad \chi_\rho(g) = d$$

Proof. ($\Rightarrow$) is obvious.

($\Leftarrow$) Assume $\chi_\rho(g) = d$. Then $|\chi_\rho(g)| = d$, so by Proposition 2.1.5(iv) $\rho(g) = \lambda\mathbf{1}$ for some $\lambda \in \mathbb{C}$. But then $\chi_\rho(g) = \lambda d$, so $\lambda = 1$. □

So if you know χ_ρ, then you know the kernel of ρ. In particular you know whether or not ρ is faithful.

Let ξ, ζ be any two functions from G to $\mathbb{C}$. Then we define their sum and product in the obvious 'point-wise' way, i.e. we define

$$(\xi + \zeta)(g) = \xi(g) + \zeta(g)$$
$$(\xi\zeta)(g) = \xi(g)\zeta(g)$$

Proposition 2.1.7. *Let $\rho_V : G \to GL(V)$ and $\rho_W : G \to GL(W)$ be representations, and let χ_V and χ_W be their characters.*

(i) $\chi_{V\oplus W} = \chi_V + \chi_W$

(ii) $\chi_{V\otimes W} = \chi_V \chi_W$

(iii) $\chi_{V^*} = \overline{\chi_V}$

(iv) $\chi_{\mathrm{Hom}(V,W)} = \overline{\chi_V}\chi_W$

Proof. (i) Pick bases for V and W, and pick $g \in G$. Suppose that $\rho_V(g)$ and $\rho_W(g)$ are described by matrices M and N in these bases. Then $\rho_{V\oplus W}(g)$ is described by the block-diagonal matrix

$$\begin{pmatrix} M & 0 \\ 0 & N \end{pmatrix}$$

So

$$\mathrm{Tr}\left(\rho_{V\oplus W}(g)\right) = \mathrm{Tr}(M) + \mathrm{Tr}(N) = \mathrm{Tr}\left(\rho_V(g)\right) + Tr\left(\rho_W(g)\right)$$

(ii)$\rho_{V\otimes W}(g)$ is given by the matrix

$$[M \otimes N]_{js,it} = M_{ji}N_{st}$$

The trace of this matrix is

$$\begin{aligned}\sum_{i,t}[M \otimes N]_{it,it} &= \sum_{i,t} M_{ii}N_{tt} \\ &= \mathrm{Tr}(M)\,\mathrm{Tr}(N)\end{aligned}$$

i.e. $\chi_{V\otimes W}(g) = \chi_V(g)\chi_W(g)$. This formula is very useful, it means we can now forget the definition of the tensor product for most purposes!

(iii) $\rho_{V^*}(g)$ is described by the matrix M^{-T}, so

$$\begin{aligned}\mathrm{Tr}\left(\rho_{V^*}(g)\right) &= \mathrm{Tr}(M^{-T}) \\ &= \mathrm{Tr}(M^{-1}) \\ &= \chi_V(g^{-1}) \\ &= \overline{\chi}_V(g) \quad \text{(by Proposition 2.1.5(ii))}\end{aligned}$$

i.e. $\chi_{V^*}(g) = \overline{\chi_V(g)}$.

(iv) By Corollary 1.9.6, the representation $\mathrm{Hom}(V, W)$ is isomorphic to the representation $V^* \otimes W$, so the statement follows by parts (ii) and (iii). $\square$

If ρ is an irreducible representation, we say that χ_ρ is an **irreducible character**. We know that any group G has a finite list of irreps

$$U_1, \ldots, U_r$$

so there is a corresponding list of irreducible characters

$$\chi_1, \ldots, \chi_r$$

We also know that any representation is a direct sum of copies of these irreps, i.e. if $\rho : G \to GL(V)$ is a representation then there exist numbers $m_1, \ldots, m_r$ such that

$$V = U_1^{\oplus m_1} \oplus \ldots \oplus U_r^{\oplus m_r}$$

Then by Proposition 2.1.7(i) we have

$$\chi_\rho = m_1\chi_1 + \ldots + m_r\chi_r$$

So every character is a linear combination of the irreducible characters (with non-negative integer coefficients).

The character of the regular representation ρ_{reg} is called the **regular character**, we write it as χ_{reg}.

Proposition 2.1.8. *(i) Let $\{U_i\}$ be the irreps of G, and let d_i be their dimensions. Let $\{\chi_i\}$ be the corresponding irreducible characters. Then*

$$\chi_{reg} = d_1\chi_1 + \ldots + d_r\chi_r$$

(ii)

$$\chi_{reg}(g) = \begin{cases} |G| & \text{if } \; g = e \\ 0 & \text{if } \; g \neq e \end{cases}$$

Proof. (i) By Theorem 1.8.8

$$V_{reg} = U_1^{\oplus d_1} \oplus \ldots \oplus U_r^{\oplus d_r}$$

Taking characters of each side gives the statement.

(ii) $\chi_{reg}(e) = \dim V_{reg} = |G|$ by Proposition 2.1.5(iii). Suppose $g \neq e$. Then for all $h \in G$,

$$gh \neq h$$

The regular representation has a basis $\{b_h \mid h \in G\}$, and $\rho_{reg}(g)$ is the linear map

$$b_h \mapsto b_{gh}$$

Since $b_{gh} \neq b_h \, \forall \, h$, we have $\mathrm{Tr}\,(\rho_{reg}(g)) = 0$. $\square$

Part (ii) can be generalized to arbitrary permutation representations (see Problem Sheets).

Example 2.1.9. Let $G = C_k = \langle \mu \mid \mu^k = e \rangle$. The irreps of G are the 1-dimensional representations

$$\rho_q : \mu \mapsto e^{\frac{2\pi i}{k} q}, \quad q \in [0, k-1]$$

So the irreducible characters are the functions

$$\chi_q = \rho_q : G \to \mathbb{C}$$

(for 1-dimensional representations, the character is the same thing as the representation). Lets check the identities from the previous proposition. If

$$\chi_{reg} = \chi_0 + \ldots + \chi_{k-1}$$

then

$$\begin{aligned} \chi_{reg}(e) &= \chi_0(e) + \ldots + \chi_{k-1}(e) \\ &= 1 + \ldots + 1 = k = |G| \end{aligned}$$

and

$$\chi_{reg}(\mu) = 1 + e^{\frac{2\pi i}{k}} + \ldots + e^{\frac{2\pi i}{k}(k-1)} = 0$$

which is a familiar identity for roots of unity. In fact, for all $s \in [1, k-1]$, the (maybe less familiar) identity

$$\sum_{q=0}^{k-1} \left(e^{\frac{2\pi i}{k}}\right)^{sq} = 0$$

must hold, because both sides equal $\chi_{reg}(\mu^s)$.

2.2 Inner products of characters

Let $\mathbb{C}^G$ denote the set of all functions from G to $\mathbb{C}$. Then $\mathbb{C}^G$ is a vector space: we've already defined the sum of two functions, and similarly we can define scalar multiplication by

$$\begin{aligned} \lambda\xi : & G \to \mathbb{C} \\ & g \mapsto \lambda\xi(g) \end{aligned}$$

for $\xi \in \mathbb{C}^G$ and $\lambda \in \mathbb{C}$.

The space $\mathbb{C}^G$ has a basis given by the set of 'characteristic functions'

$$\{\delta_g \mid g \in G\}$$

defined by

$$\delta_g : h \to \begin{cases} 1 & \text{if} \quad h = g \\ 0 & \text{if} \quad h \neq g \end{cases}$$

To see that this indeed a basis, notice that we can write any function $\xi \in \mathbb{C}^G$ as a linear combination

$$\xi = \sum_{g \in G} \xi(g)\delta_g$$

This is an equality because both sides define the same function from G to $\mathbb{C}$, furthermore it should be obvious that this is the unique way to write ξ as a linear combination of the δ_g. Consequently, the dimension of $\mathbb{C}^G$ is the size of G.

We've seen this vector space before. Recall that the vector space V_{reg} on which the regular representation acts is, by definition, a $|G|$-dimensional vector space with a basis $\{b_g \mid g \in G\}$. Then the natural bijection of sets

$$\{\delta_g \mid g \in G\} \leftrightarrow \{b_g \mid g \in G\}$$

induces a natural isomorphism of vector spaces

$$\mathbb{C}^G \cong V_{reg}$$

Despite this we're going to keep two different notations, because we're going to think of these two vector spaces differently, and do different things with them. In particular when we we write $\mathbb{C}^g$ we'll generally ignore the fact that it carries a representation of G.

Viewing the vector space $\mathbb{C}^G$ as a space of functions, we can see an important extra structure, it carries a Hermitian inner product.

Definition 2.2.1. Let $\zeta, \xi \in \mathbb{C}^G$. We define their **inner product** by

$$\langle \xi | \zeta \rangle = \frac{1}{|G|} \sum_{g \in G} \xi(g) \overline{\zeta(g)}$$

It's easy to see that $\langle \xi | \zeta \rangle$ is linear in the first variable, and conjugate-linear in the second variable, i.e.

$$\langle \xi | \lambda \zeta \rangle = \overline{\lambda} \langle \xi | \zeta \rangle$$

It's also clear that

$$\langle \xi | \zeta \rangle = \overline{\langle \zeta | \xi \rangle}$$

Finally, the inner-product of any vector χ with itself is

$$\langle \xi | \xi \rangle = \sum_{g \in G} |\xi(g)|^2$$

which is a non-negative real number, and equal to zero iff $\xi = 0$. The (positive) square-root of this number is called the *norm* of ξ. This list of properties are the definition of a Hermitian inner product.

You should recall that there is a *standard inner product* on the vector space $\mathbb{C}^n$, defined by

$$\langle x | y \rangle = x_1 \bar{y_i} + ... + x_n \bar{y_n}$$

and often written as '$x.y$'. This is an example of a Hermitian inner product. If we identify $\mathbb{C}^G$ with $\mathbb{C}^n$ (where $n = |G|$) using our basis $\{\delta_g\}$, then our inner product is almost the same as the standard one, they only differ by the overall scale factor $\frac{1}{|G|}$.

The standard basis $e_1, .., e_n \in \mathbb{C}^n$ are *orthonormal* with respect to the standard inner product, which means that $e_i.e_j = 0$ if $i \neq j$ (they're *orthogonal*), and $e_i.e_i = 1$ (they each have norm 1). Notice that our basis elements $\{\delta_g\}$ for $\mathbb{C}^G$ are not quite orthonormal with respect to the inner product that we've defined, because we have

$$\langle \delta_g | \delta_h \rangle = \begin{cases} 0 & \text{if} \quad h \neq g \\ \frac{1}{|G|} & \text{if} \quad h = g \end{cases}$$

Recall that the characters of G are elements of $\mathbb{C}^G$, so we can evaluate this inner product on pairs of characters. The answer turns out to be very useful.

Theorem 2.2.2. *Let $\rho_V : G \to GL(V)$ and $\rho_W : G \to GL(W)$ be representations, and let χ_V, χ_W be their characters. Then*

$$\langle \chi_W | \chi_V \rangle = \dim \mathrm{Hom}_G(V, W)$$

In particular, the inner product of two characters is always a non-negative integer. This is a strong restriction, because the inner product of two arbitrary functions (i.e. not necessarily characters) can be any complex number.

Before we begin the proof, two quick lemmas:

Lemma 2.2.3. *Let V be a vector space (of dimension n), and let f_1, f_2 be linear maps from V to V. Then for any scalars $\lambda_1, \lambda_2 \in \mathbb{C}$, we have*

$$\mathrm{Tr}(\lambda_1 f_1 + \lambda_2 f_2) = \lambda_1 \mathrm{Tr}(f_1) + \lambda_2 \mathrm{Tr}(f_2)$$

In other words, Tr is a linear map

$$\mathrm{Tr} : \mathrm{Hom}(V, V) \to \mathbb{C}$$

Proof. Pick any basis for V, and let M_1 and M_2 be the matrices describing f_1 and f_2 in this basis. Then

$$\begin{aligned}\mathrm{Tr}(\lambda_1 f_1 + \lambda_2 f_2) = \mathrm{Tr}(\lambda_1 M_1 + \lambda_2 M_2) \qquad\qquad &= \sum_{i=1}^{n}(\lambda_1 M_1 + \lambda_2 M_2)_{ii} \\ = \lambda_1 \sum_{i=1}^{n}(M_1)_{ii} + \lambda_2 \sum_{i=1}^{n}(M_2)_{ii} \quad &= \lambda_1 \mathrm{Tr}(f_1) + \lambda_2 \mathrm{Tr}(f_2)\end{aligned}$$

□

Lemma 2.2.4. *Let V be a vector space, with subspace $U \subset V$, and let $\pi : V \to V$ a projection onto U. Then*

$$\mathrm{Tr}(\pi) = \dim U$$

Proof. Recall that $V = U \oplus \mathrm{Ker}(\pi)$. Pick bases for U and $\mathrm{Ker}(\pi)$, so together they form a basis for V. In this basis, π is given by the block-diagonal matrix

$$\begin{pmatrix} \mathbf{1} & 0 \\ 0 & 0 \end{pmatrix}$$

with $\dim U$ being the size of the top block and $\dim \mathrm{Ker}(\pi)$ being the size of the bottom block. So $\mathrm{Tr}(\pi) = \mathrm{Tr}(\mathbf{1}_U) = \dim U$. □

Now we can present the proof of the Theorem.

Proof of Theorem 2.2.2. Recall that

$$\mathrm{Hom}_G(V, W) \subset \mathrm{Hom}(V, W)$$

is the invariant subrepresentation, and that the map

$$\begin{aligned}\Psi : \mathrm{Hom}(V, W) &\to \mathrm{Hom}(V, W) \\ f &\mapsto \frac{1}{|G|}\sum_{g \in G} \rho_{\mathrm{Hom}(V,W)}(g)(f)\end{aligned}$$

is a projection onto $\mathrm{Hom}_G(V, W)$ (see Proposition 1.7.8). We claim that

$$\mathrm{Tr}(\Psi) = \langle \chi_W | \chi_V \rangle$$

By Lemma 2.2.4, this would prove the theorem.

Our projection map Ψ is a linear combination of the maps

$$\rho_{\mathrm{Hom}(V,W)}(g) : \mathrm{Hom}(V, W) \to \mathrm{Hom}(V, W)$$

Therefore, by Lemma 2.2.3 we have

$$\mathrm{Tr}(\Psi) = \frac{1}{|G|} \sum_{g \in G} \mathrm{Tr}(\rho_{\mathrm{Hom}(V,W)}(g))$$

However,

$$\mathrm{Tr}(\rho_{\mathrm{Hom}(V,W)}(g)) = \chi_{\mathrm{Hom}(V,W)}(g)$$

by definition, and

$$\chi_{\mathrm{Hom}(V,W)}(g) = \overline{\chi_V(g)}\chi_W(g)$$

by Proposition 2.1.7(iv). Therefore

$$\mathrm{Tr}(\Psi) = \frac{1}{|G|} \sum_{g \in G} \overline{\chi_V(g)}\chi_W(g) = \langle \chi_W | \chi_V \rangle$$

$\square$

Corollary 2.2.5. *Let $\chi_1, \ldots, \chi_r$ be the irreducible characters of G. Then*

$$\langle \chi_i | \chi_j \rangle = \begin{cases} 1 & \text{if} \quad i = j \\ 0 & \text{if} \quad i \neq j \end{cases}$$

Proof. Let χ_i and χ_j be the characters of the irreps U_i, U_j. Then

$$\langle \chi_i | \chi_j \rangle = \dim \mathrm{Hom}_G(U_i, U_j) = \begin{cases} 1 & \text{if} \quad U_i, U_j \text{ isomorphic} \\ 0 & \text{if} \quad U_i, U_j \text{ not isomorphic} \end{cases}$$

by Proposition 1.8.4. $\square$

So the irreducible characters form a set of orthonormal vectors in $\mathbb{C}^G$. Therefore, if we take any linear combination of them

$$\xi = \lambda_1 \chi_1 + ... \lambda_r \chi_r \in \mathbb{C}^G$$

(with $\lambda_1, ..., \lambda_r \in \mathbb{C}$) then we can calculate the coefficient of χ_i in ξ as the inner product

$$\langle \xi | \chi_i \rangle = \lambda_i$$

In particular the irreducible characters must be linearly independent, because if we have some co-efficients such that

$$\lambda_1 \chi_1 + ... \lambda_r \chi_r = 0$$

then the above formula tells us that each λ_i is equal to zero.

Now take a representation $\rho : G \to GL(V)$, and look at its character χ_ρ. We know that χ_ρ can be written as a linear combination

$$\chi_\rho = m_1 \chi_1 + \ldots + m_r \chi_r$$

of the irreducible characters, because the representation V can be decomposed into irreps. The m_i are non-negative integers, they count the number of copies of the irrep U_i occuring in V. We can calculate these coefficients by calculating the inner product

$$\langle \chi_\rho | \chi_i \rangle = m_i$$

We've just proved:

Corollary 2.2.6. *Let $\rho : G \to GL(V)$ be a representation, and let χ_ρ be its character. Then the number of copies of the irrep U_i occuring in the irrep decomposition of V is given by the inner product $\langle \chi_\rho | \chi_i \rangle$.*

We can view this as a combination of Theorem 2.2.2 and Proposition 1.8.5, because

$$\langle \chi_\rho | \chi_i \rangle = \dim \operatorname{Hom}_G(U_i, V)$$

This gives us an extremely efficient way to calculate irrep decompositions!

Example 2.2.7. Let $G = C_4 = \langle \mu \mid \mu^4 = e \rangle$. Here's a 2-dimensional representation:

$$\begin{aligned} \rho : &\mu \mapsto M = \begin{pmatrix} i & 2 \\ 1 & -i \end{pmatrix} \\ &\mu^2 \mapsto M^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ &\mu^3 \mapsto M^3 = M \end{aligned}$$

The character of ρ takes values

	e	μ	μ^2	μ^3
χ_ρ	2	0	2	0

The irreducible characters of G are χ_q, $q \in [0,3]$, given by

	e	μ	μ^2	μ^3
χ_q	1	i^q	i^{2q}	i^{3q}

(these are the characters of the irreps ρ_q). So

$$\begin{aligned}\langle \chi_\rho | \chi_q \rangle &= \frac{1}{4}\left(2 \times \overline{1} + 0 \times \overline{(i^q)} + 2 \times \overline{(i^{2q})} + 0 \times \overline{(i^{3q})}\right)\\ &= \frac{1}{2}\left(1 + (-1)^q\right)\\ &= \begin{cases} 1 & \text{if} \quad q = 0, 2 \\ 0 & \text{if} \quad q = 1, 3 \end{cases}\end{aligned}$$

So ρ is the direct sum of ρ_0 and ρ_2.

Here's another Corollary of Theorem 2.2.2.

Corollary 2.2.8. *Let χ be a character of G. Then χ is irreducible if and only if*

$$\langle \chi | \chi \rangle = 1$$

Proof. Write χ as a linear combination

$$\chi = m_1\chi_1 + \ldots + m_r\chi_r$$

of the irreducible characters, for some non-negative integers $m_1, \ldots, m_r$. Then

$$\begin{aligned}\langle \chi | \chi \rangle &= \sum_{i,j \in [1,r]} m_i m_j \langle \chi_i | \chi_j \rangle\\ &= m_1^2 + \ldots + m_r^2\end{aligned}$$

by Corollary 2.2.5. So $\langle \chi | \chi \rangle = 1$ iff exactly one of the $m_i = 1$ and the rest are 0. □

Recall (Proposition 2.1.5(i)) that a character gives the same value on conjugate elements of G. For $g \in G$, we write $[g]$ for the set of elements of G that are conjugate to g, this is called the **conjugacy class** of g. If we want to calculate the inner product of two characters χ_V, χ_W, we don't need to evaluate $\chi_V(g)\overline{\chi_W}(g)$ on each group element, we just need to evaluate it once on each conjugacy class, i.e.

$$\begin{aligned}\langle \chi_V | \chi_W \rangle &= \frac{1}{|G|} \sum_{g \in G} \chi_V(g)\overline{\chi_W}(g) \\ &= \frac{1}{|G|} \sum_{[g]} |[g]| \chi_V(g)\overline{\chi_W}(g)\end{aligned}$$

Example 2.2.9. Let $G = D_4 = \langle \sigma, \tau \mid \sigma^4 = \tau^2 = e,\ \sigma\tau = \tau\sigma^{-1} \rangle$. The conjugacy classes in G are (see Problem Sheets):

$[g]$	$[e]$	$[\sigma]$	$[\tau]$	$[\sigma\tau]$	$[\sigma^2]$
$\lvert[g]\rvert$	1	2	2	2	1

Here is a two-dimensional representation of G:

$$\rho(\sigma) = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad \rho(\tau) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

(this is just the 'square' representation from Example 1.3.7 written in a particular basis). Then the character χ of this representation takes values

$[g]$	$[e]$	$[\sigma]$	$[\tau]$	$[\sigma\tau]$	$[\sigma^2]$
$\lvert[g]\rvert$	1	2	2	2	1
χ	2	0	0	0	-2

We compute

$$\langle \chi | \chi \rangle = \frac{1}{8}\left((1 \times 2^2) + 0 + 0 + 0 + (1 \times (-2)^2)\right) = 1$$

so ρ must be irreducible.

Now we can prove (as promised) that the character completely determines the representation. It's really just another corollary of Theorem 2.2.2:

Theorem 2.2.10. *Let $\rho_V : G \to GL(V)$ and $\rho_W : G \to GL(W)$ be representations, and suppose that $\chi_V = \chi_W$. Then V and W are isomorphic.*

This may look surprising at first, but it's just a consequence of the fact that there aren't very many representations of G!

Proof. Let $U_1, \ldots, U_r$ be the irreps of G, and $\chi_1, \ldots, \chi_r$ be their characters. We have

$$V = U_1^{\oplus m_1} \oplus \ldots \oplus U_r^{\oplus m_r}$$

for some numbers $m_1, \ldots, m_r$, and

$$W = U_1^{\oplus l_1} \oplus \ldots \oplus U_r^{\oplus l_r}$$

for some numbers $l_1, \ldots, l_r$. So

$$\chi_V = m_1\chi_1 + \ldots + m_r\chi_r$$

and

$$\chi_W = l_1\chi_1 + \ldots + l_r\chi_r$$

Since $\chi_V = \chi_W$, we have

$$m_i = \langle \chi_V | \chi_i \rangle = \langle \chi_W | \chi_i \rangle = l_i$$

for all i. So V and W have the same irrep decompositions, and hence they're isomorphic. $\square$

So we can understand everything about representations in terms of characters, and characters are much easier to work with.

Example 2.2.11. Let $G = D_4$. We know (Example 1.8.14) that G has 4 one-dimensional irreps U_1, U_2, U_3, U_4, and 1 two-dimensional irrep U_5 (the 'square' representation). So a complete list of the irreducible characters of D_4 is

$[g]$	$[e]$	$[\sigma]$	$[\tau]$	$[\sigma\tau]$	$[\sigma^2]$
$\lvert[g]\rvert$	1	2	2	2	1
χ_1	1	1	1	1	1
χ_2	1	-1	1	-1	1
χ_3	1	1	-1	-1	1
χ_4	1	-1	-1	1	1
χ_5	2	0	0	0	-2

This is called a **character table**. We can quickly see the following facts:

- For each i, we have $\overline{\chi_i} = \chi_i$ (since they only take real values). Therefore each U_i is isomorphic to its own dual $(U_i)^*$.
- If $1 \leq i \leq 4$, then we have $\chi_i \chi_5 = \chi_5$. Therefore $U_i \otimes U_5$ is isomorphic to U_5.
- Now let's compute $U_5 \otimes U_5$. We have

  $$\chi_5 \chi_5 = \chi_1 + \chi_2 + \chi_3 + \chi_4$$

  (in general we could find the coefficients on the right-hand-side by using the inner product, but in this case it's quicker to just spot the answer). So $U_5 \otimes U_5$ is isomorphic to $U_1 \oplus U_2 \oplus U_3 \oplus U_4$.

Example 2.2.12. Let $G = D_4$ again. Suppose we'd found all the 1-dimensional irreps of G, and we'd deduced that there must a be a 2-dimensional irrep, but we couldn't work out what it was (perhaps we were just algebraists and didn't know any geometry). Then we could write down most of the character table, but the bottom line would read

$$\begin{array}{c|ccccc} \chi_5 & 2 & a & b & c & d \end{array}$$

where a, b, c, d are unknown. Corollary 2.2.5 lets us deduce the unknown values, without finding the representation U_5. For each $1 \leq i \leq 4$, we must have $\langle \chi_i | \chi_5 \rangle = 0$. This gives the four equations

$$\begin{aligned} 2 + 2(a + b + c) + d &= 0 \\ 2 + 2(-a + b - c) + d &= 0 \\ 2 + 2(a - b - c) + d &= 0 \\ 2 + 2(-a - b + c) + d &= 0 \end{aligned}$$

Comparing the first equation with the remaining three, we get

$$a + c = b + c = a + b = 0$$

so $a = b = c = 0$, and then $d = -2$.

2.3 Class functions and character tables

Definition 2.3.1. A **class function** for a group G is a function

$$\xi\colon G \to \mathbb{C}$$

such that

$$\xi(h^{-1}gh) = \xi(g)$$

for all $g, h \in G$.

So a class function is a function in $\mathbb{C}^G$ that is constant on each conjugacy class. It's elementary to check that the class functions form a subspace of $\mathbb{C}^G$, we denote it by

$$\mathbb{C}^G_{cl} \subset \mathbb{C}^G$$

Recall that $\mathbb{C}^G$ has a basis given by the functions

$$\delta_g\colon h \mapsto \begin{cases} 1 & \text{if } h = g \\ 0 & \text{if } h \neq g \end{cases}$$

Similarly, $\mathbb{C}_{cl}$ has a basis given by the functions

$$\delta_{[g]} = \sum_{\tilde{g}\in[g]} \delta_{\tilde{g}}\colon h \mapsto \begin{cases} 1 & \text{if } h \in [g] \\ 0 & \text{if } h \notin [g] \end{cases}$$

So $\dim(\mathbb{C}^G_{cl})$ is the number of conjugacy classes in G.

The space $\mathbb{C}^G_{cl}$ carries a Hermitian inner product, it's just given by the restriction of the inner product from $\mathbb{C}^G$. Notice that if we want to calculate $\langle\xi|\zeta\rangle$ where ξ and ζ are class functions, then we only need to evaluate $\xi(g)\overline{\zeta}(g)$ once on each conjugacy class, so the formula becomes

$$\langle\xi|\zeta\rangle = \frac{1}{|G|}\sum_{[g]} |[g]|\xi(g)\overline{\zeta}(g)$$

(we already observed this for the case when ξ and ζ are characters). Also notice that the basis $\left\{\delta_{[g]}\right\}$ is orthogonal with respect to this inner product, but not orthonormal, because we have

$$\langle\delta_{[g]}|\delta_{[h]}\rangle = \begin{cases} \frac{|[g]|}{|G|} & \text{if} \quad h = g \\ 0 & \text{if} \quad h \neq g \end{cases}$$

The numbers $\frac{|[g]|}{|G|}$ have another interpretation. Recall that the **centraliser** of a group element $g \in G$ is the subgroup

$$C_g = \{h \in G \mid hgh^{-1} = g\}$$

of elements that commute with g. By the Orbit-Stabiliser theorem,

$$|C_g| = \frac{|G|}{|[g]|}$$

so the norm of $\delta_{[g]}$ is $|C_g|^{-1}$.

Now let $\chi_1, \dots, \chi_r$ be the irreducible characters of G. Then each χ_i is a class function, and they form an orthonormal set of vectors in $\mathbb{C}^G_{cl}$ (by Corollary 2.2.5), and hence they're linearly independent. The maximum size of a linearly independent set in a vector space is the dimension of the vector space, so

$$r \leq \dim \mathbb{C}^G_{cl}$$

We've just proved:

Proposition 2.3.2. *For any group G, the number of irreps of G is at most the number of conjugacy classes in G.*

In fact, a stronger result holds:

Theorem 2.3.3. *For any group G, the number of irreps of G equals the number of conjugacy classes in G.*

We're not going to prove this yet, we'll prove it in Section 3 once we've introduced the technology of **group algebras**.

Example 2.3.4. Let $G = S_4$. You should recall that two permutations are conjugate in S_n if and only if they have the same cycle type. So in S_4 we have conjugacy classes

$$[(1)], [(12)], [(123)], [(1234)], [(12)(34)]$$

So S_4 has 5 irreps. This agrees with what we found in Example 1.8.13.

Example 2.3.5. Let $G = S_5$. The conjugacy classes in G are

$$[(1)], [(12)], [(123)], [(1234)], [(12345)], [(12)(34)], [(123)(45)]$$

So S_5 has 7 irreps.

Theorem 2.3.3 is an unusual result. Since the number of irreps equals the number of conjugacy classes, it would be reasonable to guess that there's some natural way to pair up each irrep with a conjugacy class, and vice versa. But this is not true! There's no sensible way to pair them up. The correct way to think about it is expressed in the following corollary:

Corollary 2.3.6. *The irreducible characters $\chi_1, \ldots, \chi_r$ form a basis of $\mathbb{C}^G_{cl}$.*

Proof. The irreducible characters form a linearly independent set in $\mathbb{C}^G_{cl}$, and $r = \#\{\text{conjugacy classes}\} = \dim \mathbb{C}^G_{cl}$. □

So we have two sensible bases for the vector space $\mathbb{C}^G_{cl}$, we have $\{\delta_{[g_j]}\}$ which is indexed by conjugacy classes, and $\{\chi_i\}$ which is indexed by irreps. The two bases must have the same size, but there needn't be a sensible way to pair up their elements.

We've met character tables already in Section 2.2, but let's give a formal definition:

Definition 2.3.7. Let G be a group, let $\chi_1, \ldots, \chi_r$ be the irreducible characters of G, and let $[g_1], \ldots, [g_s]$ be the conjugacy classes in G. The **character table** of G is the matrix C with entries

$$C_{ij} = \chi_i(g_j)$$

From Theorem 2.3.3 we know that $r = s$, so C is a square matrix.

Example 2.3.8. Let $G = S_3$. Let

$$g_1 = (1) \quad g_2 = (12) \quad g_3 = (123)$$

and let χ_1, χ_2, χ_3 be the characters of the trivial, sign and triangular irreps. The character table of G is the matrix

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

As we observed in Corollary 2.3.6, the vector space $\mathbb{C}^G_{cl}$ has two natural bases, given by the sets $\{\delta_{[g_j]}\}$ and $\{\chi_i\}$. Suppose we had some vector written in terms of the second basis, and we want to express it in terms of the first basis. Then what we need is the change-of-basis matrix between the two bases, i.e. we need to express each vector χ_i in terms of the basis $\{\delta_{[g_j]}\}$. But this is easy, because

$$\chi_i = \chi_i(g_1)\delta_{[g_1]} + \ldots + \chi_i(g_r)\delta_{[g_r]}$$

(since both sides give the same function $G \to \mathbb{C}$). These coefficients are precisely the entries in C, i.e. C is (the transpose of) the change-of-basis matrix between our two bases of $\mathbb{C}^G_{cl}$.

Let's calculate $C\overline{C}^T$. We have

$$\begin{aligned}(C\overline{C}^T)_{ik} &= \sum_{j=1}^{r} C_{ij}\overline{C}_{kj} \\ &= \sum_{j=1}^{r} \chi_i(g_i)\overline{\chi_k}(g_j)\end{aligned}$$

This looks like the formula for $\langle \chi_i | \chi_j \rangle$ but it's missing the coefficients $\frac{|[g_j]|}{|G|}$. If we modify C by replacing it with the matrix

$$B_{ij} = \chi_i(g_j)\sqrt{\frac{|[g_j]|}{|G|}}$$

Then

$$\begin{aligned}(B\overline{B}^T)_{ik} &= \sum_{i=1}^{r} \chi_i(g_j)\bar{\chi_k}(g_j)\frac{|[g_j]|}{|G|} \\ &= \langle \chi_i | \chi_k \rangle \\ &= \begin{cases} 1 & \text{if } i = k \\ 0 & \text{if } i \neq k \end{cases}\end{aligned}$$

So $B\overline{B}^T = \mathbf{1}_r$, i.e. B is a unitary matrix.

Recall that a unitary matrix is exactly a change-of-basis matrix between two orthonormal bases of a complex vector space (it's the analogue of an orthogonal matrix for a real vector space). This explains why we have to make this modification, the problem is that the basis $\{\delta_{[g_j]}\}$ is not orthonormal. The elements are orthogonal, but they have norms $\frac{|[g_i]|}{|G|}$. However if we rescale we can get an orthonormal basis $\left\{\delta_{[g_j]}\sqrt{\frac{|G|}{|[g_j]|}}\right\}$, and B is the change-of-basis matrix between this basis and the orthonormal basis $\{\chi_i\}$. This is why B is a unitary matrix (and C is not).

Proposition 2.3.9. *Let $[g_i]$ and $[g_j]$ be two conjugacy classes in G. Then*

$$\sum_{k=1}^{r} \overline{\chi_k}(g_i)\chi_k(g_j) = \begin{cases} \frac{|G|}{|[g_i]|} & \textit{if } i = j \\ 0 & \textit{if } i \neq j \end{cases}$$

Proof. Let B be the modified character table. We have $B^{-1} = \overline{B}^T$, so $\overline{B}^T B = \mathbf{1}_r$, i.e.

$$\begin{aligned} \sum_{k=1}^{r} \overline{B_{ki}} B_{kj} &= \left(\sum_{k=1}^{r} \overline{\chi_k}(g_i)\chi_k(g_i) \right) \frac{\sqrt{|[g_i]||[g_j]|}}{|G|} \\ &= \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases} \end{aligned}$$

which implies the proposition. □

Remember that $\frac{|G|}{|[g_i]|} = |C_{g_i}|$ (the size of the centralizer of g_i), so this is always a positive integer.

Now we have two useful sets of equations on the character table C:

- **Row Orthogonality**:

$$\sum_{j=1}^{r} C_{ij}\overline{C_{kj}}|[g_j]| = \begin{cases} |G| & \text{if } i = k \\ 0 & \text{if } i \neq k \end{cases}$$

- **Column Orthogonality**:

$$\sum_{k=1}^{r} \overline{C_{ki}} C_{kj} = \begin{cases} \frac{|G|}{|[g_i]|} = |C_{g_i}| & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}$$

Both of them are really the statement that the modified character table B is unitary.

Example 2.3.10. Let's solve Example 2.2.12 again using column orthogonality. We have a partial character table

$[g]$	$[e]$	$[\sigma]$	$[\tau]$	$[\sigma\tau]$	$[\sigma^2]$
$\|[g]\|$	1	2	2	2	1
$\frac{\|G\|}{\|[g]\|}$	8	4	4	4	8
χ_1	1	1	1	1	1
χ_2	1	-1	1	-1	1
χ_3	1	1	-1	-1	1
χ_4	1	-1	-1	1	1
χ_5	2	a	b	c	d

The $[\sigma]$-column gives the equation

$$1 + 1 + 1 + 1 + |a|^2 = 4$$

so $a = 0$, and similarly $b = c = 0$. Orthogonality of the $[e]$-column and the $[\sigma^2]$-column gives the equation

$$1 + 1 + 1 + 1 + 2d = 0$$

so $d = -2$.

The column orthogonality equations carry exactly the same information as the row orthogonality equations, but sometimes it's quicker to use one rather than the other (or we can use a mixture of both).

3 Algebras and modules

3.1 Algebras

Consider the vector space $\mathrm{Mat}_{n\times n}(\mathbb{C})$ of all $n \times n$ matrices. As well as being a vector space, we have the extra structure of matrix multiplication, which is a map

$$m\colon \mathrm{Mat}_{n\times n}(\mathbb{C}) \times \mathrm{Mat}_{n\times n}(\mathbb{C}) \to \mathrm{Mat}_{n\times n}(\mathbb{C})$$
$$m\colon (M, N) \mapsto MN$$

This map has the following properties, it is:

(i) Bilinear: it's linear in each variable.

(ii) Associative:
$$m(m(L, M), N) = m(L, m(M, N)$$
i.e.
$$(LM)N = L(MN)$$

(iii) Unital: there's an element $I_n \in \mathrm{Mat}_{n\times n}(\mathbb{C})$ obeying $m(M, I) = m(I, M) = M$ for all $M \in \mathrm{Mat}_{n\times N}(\mathbb{C})$.

A structure like this is called an **algebra**.

Definition 3.1.1. An **algebra** is a vector space A equipped with a map

$$m : A \times A \to A$$

that is bilinear, associative and unital.

We'll usually write ab when we mean $m(a, b)$. Associativity means that the expression abc is well defined (without brackets). We'll generally write 1_A for the unit element.

Example 3.1.2. (i) The 1-dimensional vector space $\mathbb{C}$ is an algebra, with m the usual multiplication.

(ii) Let $A = \mathbb{C} \oplus \mathbb{C}$, with multiplication

$$m\left((x_1, y_1), (x_2, y_2)\right) = (x_1x_2, y_1y_2)$$

Then A is an algebra. The unit is $(1, 1)$.

(iii) Let $A = \mathbb{C}[x]$, the (infinite-dimensional) vector space of polynomials in x. A is an algebra under the usual multiplication of polynomials, with unit $1_A = 1$ (the constant polynomial with value 1). More generally, we have an algebra $A = \mathbb{C}[x_1, \ldots, x_n]$ of polynomials in n variables.

(iv) Let A be the 2-dimensional space with basis $\{1, x\}$. Define $1^2 = 1$, $1x = x1 = x$ and $x^2 = 0$, and extend bilinearly. Then A is an algebra.

(v) Let V be a vector space, and let $A = \mathrm{Hom}(V, V)$. Multiplication is given by composition of maps. If we pick a basis for V, then A becomes isomorphic to $\mathrm{Mat}_{n\times n}(\mathbb{C})$, and composition of maps corresponds to multiplication of matrices (Proposition A.2.3). Therefore A is an algebra.

Except for example (iii), in each of these cases A is a finite-dimensional space. From now on, we'll assume our algebras are finite-dimensional. Examples (i)-(iv) are all **commutative**, i.e. $ab = ba$ for all $a, b \in A$. We will *not* assume that our algebras are commutative.

For this course, the most important algebras are given by the following construction:

Let G be a (finite) group, then we can construct an algebra from G. Suppose the elements of G are given by $\{g_1, \ldots, g_t\}$. Consider the set of formal linear combinations of elements of G:

$$\mathbb{C}[G] = \{\lambda_1 g_1 + \ldots + \lambda_t g_t \mid \lambda_1 \ldots \lambda_t \in \mathbb{C}\}$$

This set is a vector space, we define

$$(\lambda_1 g_1 + \ldots + \lambda_t g_t) + (\mu_1 g_1 + \ldots + \mu_t g_t) = (\lambda_1 + \mu_1)g_1 + \ldots + (\lambda_t + \mu_t)g_t$$

and

$$\mu(\lambda_1 g_1 + \ldots + \lambda_t g_t) = (\mu\lambda_1)g_1 + \ldots + (\mu\lambda_t)g_t$$

The set G sits inside $\mathbb{C}[G]$ as the subset where one coefficient is 1 and the rest are zero. This set forms a basis for $\mathbb{C}[G]$, in fact we could have defined $\mathbb{C}[G]$ to be the vector space with G as a basis.

$\mathbb{C}[G]$ is also an algebra, called the **group algebra** of G. To define the product of two basis elements, we just use the group product, i.e. we define

$$m(g,h) = gh \in G \subset \mathbb{C}[G]$$

Now extend this to a bilinear map.

$$m : \mathbb{C}[G] \times \mathbb{C}[G] \to \mathbb{C}[G]$$

i.e. we define

$$\begin{aligned}(\lambda_1 g_1 + \ldots + \lambda_t g_t)(\mu_1 g_1 + \ldots + \mu_t g_t) &= \lambda_1\mu_1(g_1^2) + \ldots + \lambda_t\mu_1(g_t g_1) + \ldots \\ &\quad \ldots + \lambda_1\mu_t(g_1 g_t) + \ldots + \lambda_t\mu_t(g_t^2) \\ &= \sum_k \left(\sum_{\substack{i,j \text{ such that} \\ g_i g_j = g_k}} \lambda_i \mu_j g_k \right)\end{aligned}$$

This product is associative because the product in G is, and it has unit $e \in G \subset \mathbb{C}[G]$.

Example 3.1.3. Let $G = C_2 = \langle e, g \mid g^2 = e \rangle$. Then

$$\mathbb{C}[G] = \{\lambda_1 e + \lambda_2 g \mid \lambda_1, \lambda_2 \in \mathbb{C}\}$$

is a two-dimensional vector space, with multiplication

$$\begin{aligned}(\lambda_1 e_1 + \lambda_2 g)(\mu_1 e + \mu_2 g) &= \lambda_2\mu_1 e + \lambda_1\mu_2 g + \lambda_2\mu_1 g + \lambda_2\mu_2 e \\ &= (\lambda_1\mu_1 + \lambda_2\mu_2)e + (\lambda_1\mu_2 + \lambda_2\mu_1)g\end{aligned}$$

We've met this vector space $\mathbb{C}[G]$ before. Recall that the regular representation of G acts on a vector space V_{reg} which has a basis $\{b_g \mid g \in G\}$. So V_{reg} is naturally isomorphic to $\mathbb{C}[G]$, via $b_g \leftrightarrow g$. We've also met it as the space $\mathbb{C}^G$ of $\mathbb{C}$-valued functions on G. This has a basis $\{\delta_g | g \in G\}$.

Warning: For functions $\xi, \zeta \in \mathbb{C}^G$ we defined a 'point-wise' product

$$\xi\zeta \colon g \mapsto \xi(g)\zeta(g)$$

This makes $\mathbb{C}^G$ into a algebra, but it's completely different from the group algebra $\mathbb{C}[G]$. In the pointwise product,

$$\delta_g \delta_h = \begin{cases} \delta_g & \text{if } g = h \\ 0 & \text{if } g \neq h \end{cases}$$

In particular, $\mathbb{C}^G$ is commutative, whereas $\mathbb{C}[G]$ usually isn't.

We can also define $\mathbb{C}[G]$ for infinite groups, but then we get infinite-dimensional algebras.

Definition 3.1.4. A **homomorphism** between algebras A and B is a linear map

$$f\colon A \to B$$

such that

(i) $f(1_A) = 1_B$

(ii) $f(a_1 a_2) = f(a_1) f(a_2), \ \forall a_1, a_2 \in A$

An **isomorphism** between A and B is a homomorphism that's also an isomorphism of vector spaces.

Example 3.1.5. Let $A = \langle 1, x \rangle$ where $x^2 = 0$ (from Example 3.1.2(iv)). There's a homomorphism

$$\begin{aligned} f_0\colon A &\to \mathbb{C} \\ 1_A &\mapsto 1 \\ x &\mapsto 0 \end{aligned}$$

In fact, f_0 is the only possible such homomorphism. If f is any homomorphism from A to $\mathbb{C}$ then we must have $f(1_A) = 1$, and

$$\begin{aligned} & f(x)f(x) = f(x^2) = f(0) = 0 \\ \Rightarrow \quad & f(x) = 0 \end{aligned}$$

Example 3.1.6. Let $A = \mathbb{C}[C_2]$ and let $B = \mathbb{C} \oplus \mathbb{C}$ as in Example 3.1.2(ii). Define

$$\begin{aligned} f \colon A &\to B \\ e &\mapsto (1, 1) \\ g &\mapsto (1, -1) \end{aligned}$$

Then f is an isomorphism of vector spaces, and it's also a homomorphism, because

$$f(1_A) = f(e) = (1, 1) = 1_B$$
$$f(g)^2 = ((1, -1))^2 = (1, 1) = f(g^2)$$

So $f(a_1, a_2) = f(a_1)f(a_2)$ for all $a_1, a_2 \in A$ by bilinearity. So A and B are isomorphic algebras.

Most of the rest of this chapter will be devoted to generalizing the previous example!

Now let A and B be two algebras. The vector space

$$A \oplus B$$

is naturally an algebra, it has a product

$$m\left((a_1, b_1), (a_2, b_2)\right) = (a_1 a_2, b_1 b_2)$$

The algebra axioms are easy to check, the unit is

$$1_{A \oplus B} = (1_A, 1_B)$$

We call this algebra the **direct sum** of A and B.

Example 3.1.7. If both A and B are the 1-dimensional algebra $\mathbb{C}$, then $A \oplus B = \mathbb{C} \oplus \mathbb{C}$ is the algebra we defined in Example 3.1.2(ii). If we iterate this construction we can make a k-dimensional algebra $\mathbb{C}^{\oplus k}$ for any k.

The direct sum of group algebras is not a group algebra in general, i.e. if G_1, G_2 are groups then in general there does not exist a group G_3 such that

$$\mathbb{C}[G_1] \oplus \mathbb{C}[G_2] = \mathbb{C}[G_3]$$

Definition 3.1.8. Let A be an algebra. The **opposite algebra** A^{op} is the algebra with the same underlying vector space as A, and with multiplication

$$m^{op}(a, b) = ba$$

The algebra axioms for A imply immediately that A^{op} is an algebra, with the unit 1_A. Obviously m^{op} is the same as the multiplication on A iff A is commutative. However, it's possible for a non-commutative ring to still be isomorphic to its opposite.

Proposition 3.1.9. *Let $A = \mathbb{C}[G]$. Then the linear map*

$$\begin{aligned} I\colon A &\to A^{op} \\ I(g) &= g^{-1} \end{aligned}$$

is an isomorphism of algebras.

Proof. I is an isomorphism of vector spaces (its inverse is I), and it's a homomorphism, because

$$I(gh) = h^{-1}g^{-1} = I(h)I(g)$$

□

3.2 Modules

Definition 3.2.1. Let A be an algebra. A (left) A**-module** is a vector space M, together with a homomorphism of algebras

$$\tilde{\rho} : A \to \mathrm{Hom}(M, M)$$

We'll assume all our modules are finite-dimensional (as vector spaces). Often we'll be lazy and say things like 'let M be an A-module', leaving the homomorphism $\tilde{\rho}$ implicit.

The definition of a module is a direct generalization of the definition of a representation of a group, in fact another name for an A-module is a 'representation of A'. For group algebras, the two concepts are the same:

Proposition 3.2.2. *Let G be a group. Then a $\mathbb{C}[G]$-module is the same thing as a representation of G.*

Proof. Suppose
$$\tilde{\rho} : \mathbb{C}[G] \to \mathrm{Hom}(M, M)$$
is a $\mathbb{C}[G]$-module. Restricting $\tilde{\rho}$ to the subset $G \subset \mathbb{C}[G]$ gives a function
$$\rho : G \to \mathrm{Hom}(M, M)$$
For $g, h \in G$ we have
$$\rho(gh) = \rho(g) \circ \rho(h)$$
using the fact that $\tilde{\rho}$ is an an algebra homomorphism, and the definition of the product in $\mathbb{C}[G]$. In particular,
$$\rho(g) \circ \rho(g^{-1}) = \rho(g^{-1}) \circ \rho(g) = \rho(e) = \mathbf{1}_M$$
since e is the unit in $\mathbb{C}[G]$. Thus each linear map $\rho(g)$ has an inverse $\rho(g^{-1})$, so ρ defines a function
$$\rho : G \to GL(M)$$
which we've just shown to be a homomorphism. So it's a representation of G.

Conversely, suppose that
$$\rho : G \to GL(M)$$
is a representation of G. Extending linearly, we get a linear map
$$\tilde{\rho} : \mathbb{C}[G] \to \mathrm{Hom}(M, M)$$
It follows immediately from the definition of the multiplication in $\mathbb{C}[G]$ that this map $\tilde{\rho}$ is an algebra homomorphism, and hence defines a $\mathbb{C}[G]$-module. $\square$

Example 3.2.3. Let A be the 1-dimensional algebra $\mathbb{C}$. Then an A-module is choice of vector space M and a homomorphism
$$\tilde{\rho} : \mathbb{C} \to \mathrm{Hom}(M, M)$$
However, we must have $\tilde{\rho}(1) = \mathbf{1}_M$, and by then by linearity we must have $\tilde{\rho}(\lambda) = \lambda \mathbf{1}_M$. Thus there is a unique such $\tilde{\rho}$. So a $\mathbb{C}$-module is exactly the same thing as a vector space.

Example 3.2.4. Let $A = \langle 1, x \rangle$ with $x^2 = 0$. Suppose M is a 1-dimensional A-module, i.e. a 1-dimensional vector space M and a homomorphism

$$\tilde{\rho} : A \to \mathrm{Hom}(M, M) = \mathbb{C}$$

By Example 3.1.5 there is a unique such $\tilde{\rho}$, defined by $\tilde{\rho}(x) = 0$.

Example 3.2.5. $A = \mathbb{C} \oplus \mathbb{C}$, and let M be a 1-dimensional module, i.e. a homomorphism

$$\tilde{\rho} \colon A \to \mathbb{C}$$

We must have

$$\begin{aligned}
(\tilde{\rho}(1,0))^2 &= \tilde{\rho}\left((1,0)^2\right) = \tilde{\rho}(1,0) \\
(\tilde{\rho}(0,1))^2 &= \tilde{\rho}\left((0,1)^2\right) = \tilde{\rho}(0,1) \\
\tilde{\rho}(1,0)\tilde{\rho}(0,1) &= \tilde{\rho}\left((1,0)(0,1)\right) = \tilde{\rho}(0,0) = 0 \\
\tilde{\rho}(0,1) + \tilde{\rho}(1,0) &= \tilde{\rho}\left((1,1)\right) = \tilde{\rho}(1_A) = 1
\end{aligned}$$

There are two solutions, we must set one of the two numbers $\tilde{\rho}(1,0)$ and $\tilde{\rho}(0,1)$ to be 1, and the other to be 0. So A has two 1-dimensional modules.

Recall (Example 3.1.6) that A is isomorphic to $\mathbb{C}[C_2]$, so $\mathbb{C}[C_2]$ must also have two 1-dimensional modules. But a $\mathbb{C}[C_2]$-module is the same thing a representation of C_2, and we know that there are two 1-dimensional representations of C_2. So this is consistent!

Since modules are generalizations of representations, we should be able to carry over some of the definitions and results of Section 1. Let's do this now.

We begin by generalizing the regular representation. For any algebra A, there is a canonical A-module, namely A itself. We define the module structure

$$\tilde{\rho} \colon A \to \mathrm{Hom}(A, A)$$

by

$$\begin{aligned}
\tilde{\rho}(a) : A &\to A \\
b &\mapsto ab
\end{aligned}$$

i.e. A acts on itself via left multiplication. The algebra axioms immediately imply that A is an A-module.

In the special case that $A = \mathbb{C}[G]$, we deduce that there is a canonical representation of G on the vector space $\mathbb{C}[G]$. This is exactly the regular representation V_{reg}.

Let's introduce some simpler notation. Suppose A is an algebra, and

$$\tilde{\rho} : A \to \mathrm{Hom}(M, M)$$

is an A-module. From now on, we're going to write am to mean $\tilde{\rho}(a)(m)$. Note that the expression abm is well-defined without brackets.

Definition 3.2.6. Let M and N be two A-modules. A **homomorphism** of A-modules (or an A**-linear map**) is a linear map

$$f\colon M \to N$$

such that

$$f(ax) = af(x)$$

for all $a \in A$ and $x \in M$.

The set of all A-linear maps from M to N is a subset

$$\mathrm{Hom}_A(M, N) \subset \mathrm{Hom}(M, N)$$

It's easy to check that it's a subspace. In fact it's a subalgebra, because the composition of two A-linear maps is also A-linear.

Proposition 3.2.7. *Let* $A = \mathbb{C}[G]$ *and* M *and* N *be* A*-modules. Let*

$$\rho_M\colon G \to GL(M)$$
$$\rho_N\colon G \to GL(N)$$

be the corresponding representations. Then

$$\mathrm{Hom}_A(M, N) = \mathrm{Hom}_G(M, N)$$

Proof. Suppose $f\colon M \to N$ is A-linear. Then in particular

$$f(gx) = gf(x), \quad \forall g \in G, x \in M$$

In our old representation notation, this says

$$f\left(\rho_M(g)(x)\right) = \rho_N(g)\left(f(x)\right)$$

so f is G-linear.

Conversely, if $f\colon M \to N$ is G-linear then

$$f\left((\lambda_1 g_1 + \ldots + \lambda_t g_t)(x)\right) = (\lambda_1 g_1 + \ldots + \lambda_t g_t) f(x)$$

by linearity and G-linearity of f, so f is A-linear. □

Definition 3.2.8. A **submodule** of an A-module M is a subspace $N \subseteq M$ such that

$$ax \in N, \quad \forall a \in A, x \in N$$

Claim 3.2.9. *Let $A = \mathbb{C}[G]$ be a group algebra, and let M be an A-module, i.e. a representation of G. Then a submodule of M is the same thing as a subrepresentation if M.*

Definition 3.2.10. Let A be an algebra. An A-module M is **simple** if it contains no non-trivial submodules.

Example 3.2.11. (i) Any 1-dimensional module must be simple.

(ii) If $A = \mathbb{C}[G]$, then an A-module is simple if and only if the corresponding representation of G is irreducible. Really, 'simple' is just another word for 'irreducible'.

Schur's Lemma is really a fact about simple modules:

Proposition 3.2.12. *Let M and N be simple A-modules. Then*

$$\dim \operatorname{Hom}_A(M, N) = \begin{cases} 1 & \textit{if} \quad M \textit{ and } N \textit{ are isomorphic} \\ 0 & \textit{if} \quad M \textit{ and } N \textit{ are not isomorphic} \end{cases}$$

Proof. Use the identical proof to Theorem 1.6.1 and Proposition 1.8.4. □

Definition 3.2.13. Let M and N be A-modules. The **direct sum** of M and N is the vector space $M \oplus N$ equipped with the A-module structure

$$a(x, y) = (ax, ay)$$

It's easy to check that $M \oplus N$ is an A-module, i.e. the above formula does indeed define a homorphism from A to $\mathrm{Hom}(M \oplus N, M \oplus N)$. It's also easy to check that this definition agrees with the definition of the direct sum of representations in the special case $A = \mathbb{C}[G]$.

The inclusion and projection maps

$$M \underset{\pi_M}{\overset{\iota_M}{\rightleftarrows}} M \oplus N \underset{\iota_N}{\overset{\pi_N}{\rightleftarrows}} N$$

are all A-linear, so we can view M and N as submodules of $M \oplus N$.

Lemma 3.2.14. *Let L, M, N be three A-modules. Then there are natural isomorphisms of vector spaces*

(i) $\mathrm{Hom}_A(L, M \oplus N) = \mathrm{Hom}_A(L, M) \oplus \mathrm{Hom}_A(L, N)$

(ii) $\mathrm{Hom}_A(M \oplus N, L) = \mathrm{Hom}_A(M, L) \oplus \mathrm{Hom}_A(N, L)$

Proof. This is just the same as the proof of the corresponding result for representations (Lemma 1.8.1 and Corollary 1.8.3). To prove (i) we define

$$\begin{aligned} P\colon\ \mathrm{Hom}(L, M \oplus N) &\to \mathrm{Hom}(L, M) \oplus \mathrm{Hom}(L, N) \\ f &\mapsto (\pi_M \circ f, \pi_N \circ f) \end{aligned}$$

and

$$\begin{aligned} P^{-1}\colon\ \mathrm{Hom}(L, M) \oplus \mathrm{Hom}(L, N) &\to \mathrm{Hom}(L, M \oplus N) \\ (f, g) &\mapsto \iota_M \circ f + \iota_N \circ g \end{aligned}$$

and check that both P and P^{-1} are linear, take A-linear maps to A-linear maps, and are inverse to each other. (ii) is proved similarly. $\square$

As we've seen, many constructions from the world of representations generalize to modules over an arbitrary algebra A. However, not everything generalises. For example, the space of all linear maps $\mathrm{Hom}(M, N)$ between two A-modules is *not* in general an A-module. Similarly, the dual vector space M^* and the tensor product $M \otimes N$ are not A-modules in general (see

Problem Sheets). Finally, there's no generalisation of the trivial representation. So group algebras are quite special.

To end this section, let's think about the relationship between taking the direct sum of algebras, and the direct sum of modules over the same algebra. Let $A \oplus B$ be the direct sum of two algebras A and B. If M is an A-module, then we can view M as an $A \oplus B$-module by defining

$$(a, b)(x) = ax$$

for $x \in M$, i.e. we let b act as zero on M for all $b \in B$. Similarly, every B-module N can also be viewed as an $A \oplus B$-module. So we can form the direct sum $M \oplus N$, and this is an $A \oplus B$-module. The multiplication is

$$(a, b)(x, y) = (ax, by)$$

for $x \in M$, $y \in N$.

Proposition 3.2.15. *Every module over $A \oplus B$ is isomorphic to $M \oplus N$ for some A-module M and some B-module N.*

Before we prove this Proposition, we need a very quick lemma about linear algebra. Recall that a projection is a linear map

$$f : V \to V$$

such that $f(x) = x$ whenever $x \in \mathrm{Im}(f)$.

Lemma 3.2.16. *A linear map $f : V \to V$ is a projection iff $f \circ f = f$.*

Proof. Suppose $f \circ f = f$. If $x \in \mathrm{Im}(f)$ then $x = f(y)$ for some y, so $f(x) = f(f(y)) = f(y) = x$. Hence f is a projection. Conversely, if f is a projection, then for any $y \in V$ we have that $f(y) \in \mathrm{Im}(f)$, so $f(f(y)) = f(y)$. Since this is true for all $y \in V$ we have $f \circ f = f$. □

Note that if $f : V \to V$ is a projection then the image of f is exactly the set of $x \in V$ such that $f(x) = x$.

Proof of Proposition 3.2.15. Consider the elements $(1_A, 0)$ and $(0, 1_B)$ in the algebra $A \oplus B$. Let's denote them just by 1_A and 1_B for brevity. They satisfy the following relations:

$$1_A^2 = 1_A, \quad 1_B^2 = 1_B, \quad 1_A 1_B = 1_B 1_A = 0, \quad 1_{A\oplus B} = 1_A + 1_B$$

Now let L be any $A \oplus B$-module. So we have linear maps

$$\begin{aligned} 1_A &\colon L \to L \\ 1_B &\colon L \to L \end{aligned}$$

By Lemma 3.2.16, both of these linear maps are projections. Let's define $M = \mathrm{Im}(1_A)$, and $N = \mathrm{Im}(1_B)$. Since 1_A is a projection, a vector $x \in L$ lies in M iff $1_A(x) = x$. Also, for any $x \in L$ we have

$$1_A(x) + 1_B(x) = 1_{A\oplus B}(x) = x$$

So $1_A(x) = x$ iff $1_B(x) = 0$, i.e. M is exactly the kernel of 1_B. Similarly N is exactly the kernel of 1_A. By Lemma 1.5.5, the vector space L splits as a direct sum

$$L = M \oplus N$$

We claim that both M and N are actually submodules of L. To see this, suppose $x \in M$, i.e. $1_A(x) = x$. Then for any $(a, b) \in A \oplus B$ we have

$$\begin{aligned} (a, b)(x) &= (a, b)1_A(x) \\ &= (a, 0)(x) \\ &= 1_A(a, 0)(x) \end{aligned}$$

This lies in M, since M is the image of 1_A. Therefore M is a submodule. Futhermore, the $A \oplus B$-module structure on M is really an A-module structure, since every element in B acts as zero on M. Similarly, N is a submodule, and it's really a B-module. □

Example 3.2.17. Let $A = \mathbb{C} \oplus \mathbb{C}$. Since a $\mathbb{C}$-module is nothing but a vector space, every A-module is of the form $U \oplus W$ where U and W are vector spaces. Conversely, if U and W are any two vector spaces, then $U \oplus W$ is automatically an A-module. The elements $(1, 0)$ and $(0, 1)$ in A act as the 'block-diagonal' linear maps

$$\begin{pmatrix} \mathbf{1}_U & 0 \\ 0 & 0 \end{pmatrix} \qquad \text{and} \qquad \begin{pmatrix} 0 & 0 \\ 0 & \mathbf{1}_W \end{pmatrix}$$

Now recall (Example 3.1.6) that we have an isomorphism of algebras

$$f : \mathbb{C}[C_2] \to A$$

sending

$$e \mapsto (1,1) \qquad \text{and} \qquad g \mapsto (1,-1)$$

Then the inverse isomorphism f^{-1} sends

$$(1,0) \mapsto \frac{1}{2}(e+g) \qquad \text{and} \qquad (0,1) \mapsto \frac{1}{2}(e-g)$$

So A-modules are the same thing as $\mathbb{C}[C_2]$-modules, i.e. representations of C_2. Therefore, if $\rho : C_2 \to GL(V)$ is a representation, there should be a canonical way to split up V as a direct sum $U \oplus W$ of two subrepresentations. This is true! C_2 has exactly two irreps, the trivial irrep U_1 and the sign representation U_2. Therefore any representation V of C_2 can be decomposed as $V = U \oplus W$, where U is a direct sum of copies of U_1, and W is a direct sum of copies of U_2.

The linear map $\rho(g)$ acts as $\mathbf{1}_U$ on U, since U is a trivial subrepresentation, and it acts as $-\mathbf{1}_W$ on W, by the definition of the sign representation (in other words, U and W are the eigenspaces of $\rho(g)$ with eigenvalues 1 and -1). Consequently, we have

$$\frac{1}{2}(\rho(e)+\rho(g)) = \begin{pmatrix} \mathbf{1}_U & 0 \\ 0 & 0 \end{pmatrix} \qquad \text{and} \qquad \frac{1}{2}(\rho(e)-\rho(g)) \begin{pmatrix} 0 & 0 \\ 0 & \mathbf{1}_W \end{pmatrix}$$

So now we have two points-of-view on this splitting: we can either see it from Maschke's Theorem, or from the fact that $\mathbb{C}[C_2]$ is isomorphic to $\mathbb{C} \oplus \mathbb{C}$.

3.3 Matrix algebras

Let V be a vector space. In this section, we'll study the algebra

$$A_V = \mathrm{Hom}(V,V)$$

If we pick a basis for V then A_V becomes an algebra of matrices $\mathrm{Mat}_{n\times n}(\mathbb{C})$, so we'll call any algebra of this form a **matrix algebra** (even if we haven't chosen a basis).

Since there's only one vector space (up to isomorphism) for each dimension n, there's also only one matrix algebra (up to isomorphism) for each n, and its dimension is n^2.

Lemma 3.3.1. *A_V^{op} is naturally isomorphic to* $\mathrm{Hom}(V^*, V^*)$.

Proof. Use the map

$$\begin{aligned} \mathrm{Hom}(V,V) &\to \mathrm{Hom}(V^*,V^*)^{op} \\ f &\mapsto f^* \qquad \text{(the dual map)} \end{aligned}$$

This is an isomorphism of vector spaces, and it's also a homomorphism because $(f \circ g)^* = g^* \circ f^*$. □

So A_V^{op} is also a matrix algebra, and it's isomorphic to A_V, because V^* and V have the same dimension. But there's no natural choice of isomorphism, because there's no natural isomorphism between V and V^*. However, if we pick a basis for V, then V becomes isomorphic to $\mathbb{C}^n$, and so does V^*, using the dual basis. Then both $\mathrm{Hom}(V,V)$ and $\mathrm{Hom}(V^*,V^*)$ become isomorphic to $\mathrm{Mat}_{n\times n}(\mathbb{C})$. Now the above lemma simply says that we have an isomorphism

$$\begin{aligned} \mathrm{Mat}_{n\times n}(\mathbb{C}) &\to \mathrm{Mat}_{n\times n}(\mathbb{C})^{op} \\ M &\mapsto M^T \end{aligned}$$

This is obviously an isomorphism of vector spaces, and it's an algebra homomorphism because

$$(MN)^T = N^T M^T$$

Now we're going to study the modules over a matrix algebra A_V. There's one very obvious module, which is the vector space V. This is automatically a module over A_V, because we have a canonical homomorphism

$$A_V \to \mathrm{Hom}(V,V)$$

given by the identity map! In other words, we have an action of A_V on V defined by

$$fv = f(v)$$

If we pick a basis for V this becomes the action of $\mathrm{Mat}_{n\times n}(\mathbb{C})$ on $\mathbb{C}^n$ (the space of column vectors). We'll prove shortly that in fact the only possible A_V-modules are direct sums of copies of V, this will be the main result of this section.

Lemma 3.3.2. *V is a simple A_V-module, i.e. it contains no non-trivial submodules.*

Proof. Suppose $N \subset V$ is a non-zero submodule, and pick a non-zero vector $x \in N$. For any $y \in V$, there exists a linear map $f \in A_V$ that maps x to y (for example: extend x to a basis for V and define f by mapping x to y and all other basis vectors to zero). Thus $fx = f(x) = y$ lies in N for all $y \in V$, so $N = V$. $\square$

Lemma 3.3.3. *Let V be a vector space (of dimension n) and let $A_V =$ $\mathrm{Hom}(V, V)$. Then A_V is isomorphic as an A_V-module to $V^{\oplus n}$.*

Proof. Pick a basis for V, so $A_V = \mathrm{Mat}_{n\times n}(\mathbb{C})$. Then A_V acts on itself by matrix multiplication, and it acts on $V \cong \mathbb{C}^n$ via the action of matrices on column vectors. Consider the subspace

$$(A_V)_{\bullet k} \subset A_V$$

of matrices which are zero except in the kth column, i.e. they look like

$$\begin{pmatrix} 0 & \dots & 0 & a_1 & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & a_n & 0 & \dots & 0 \end{pmatrix}$$

Then each $(A_V)_{\bullet k}$ is a submodule, and it's isomorphic to V. Also

$$A_V = \bigoplus_{k=1}^{n} (A_V)_{\bullet k}$$

$\square$

So we've shown that the A_V-module A_V is isomorphic to a direct sum of copies of V. Our goal is to prove that *every* A_V-module is isomorphic to a direct sum of copies of V. Before we can begin the proof, we need to quickly generalize one more result from Section 1.

Recall (Lemma 1.8.11) that if W is any representation of a group G, and V_{reg} is the regular representation, then there is a natural isomorphism of vector spaces

$$\mathrm{Hom}_G(V_{reg}, W) = W$$

This fact generalizes to arbitrary algebras:

Lemma 3.3.4. *For any algebra A, and A-module M, there is a natural isomorphism of vector spaces*

$$\mathrm{Hom}_A(A, M) = M$$

Proof. This is exactly the same as the proof of Lemma 1.8.11. We use the map 'evaluate at 1_A':

$$\begin{array}{rcl} T\colon \mathrm{Hom}_A(A, M) & \to & M \\ f & \mapsto & f(1_A) \end{array}$$

The inverse to T is the map

$$\begin{aligned} T^{-1} : & M \to \mathrm{Hom}_A(A, M) \\ & x \mapsto f_x \end{aligned}$$

where f_x is the A-linear map

$$f_x : a \mapsto ax$$

□

Corollary 3.3.5. *For any A_V-module M, we have*

$$\dim M = nk$$

where $k = \dim \mathrm{Hom}_A(V, M)$.

Proof. By Lemma 3.3.4 and Lemma 3.3.3 we have isomorphisms of vector spaces

$$M \cong \mathrm{Hom}_A(A, M) \cong \mathrm{Hom}_A(V^{\oplus n}, M) \cong \mathrm{Hom}_A(V, M)^{\oplus n}$$

□

Theorem 3.3.6. *Let M be any A_V-module. Then we have an isomorphism of A_V-modules*

$$M = V^{\oplus k}$$

where $k = \dim \mathrm{Hom}_{A_V}(V, M)$.

This is one of the most difficult results in this course. We're going to give two proofs, the first one is more elegant, the second one is quicker and messier.

First proof of Theorem 3.3.6. Corollary 3.3.5 says that M and $V^{\oplus k}$ have the same dimension and hence are isomorphic as vector spaces, but we need to prove that they're isomorphic as A_V-modules.

Let $\{f_1, ..., f_k\}$ be a basis for $\mathrm{Hom}_{A_V}(V, M)$, and let

$$F = (f_1, \ldots, f_k) \in \mathrm{Hom}_{A_V}(V, M)^{\oplus k} = \mathrm{Hom}_{A_V}(V^{\oplus k}, M)$$

So F is a homomorphism of A_V-modules from $V^{\oplus k}$ to M. We want to prove that F is an isomorphism, and in fact it's sufficient to prove that it's an injection, because both modules have the same dimension.

Consider the maps

$$F_{\leq l} = (f_1, ..., f_l) : V^{\oplus l} \to M$$

where $1 \leq l \leq k$. We're going to prove, by induction, that each map $F_{\leq l}$ is an injection. Since $F = F_{\leq k}$, this will prove the theorem.

(i) First we need to show that $F_{\leq 1} = f_1 : V \to M$ is an injection. The kernel of f_1 is a submodule of V, but V is a simple module (Lemma 3.3.2) and f_1 is not the zero map, so we must have $\mathrm{Ker}(f_1) = \{0\}$. So $F_{\leq 1}$ is indeed an injection. Note that the same argument shows that each map $f_i : V \to M$ must be an injection.

(ii) Take $1 \leq l < k$, and assume (for the inductive step) that

$$F_{\leq l} : V^{\oplus l} \to M$$

is an injection. Let $N_{\leq l} \subset M$ be the image of this map, it's a submodule of M which is isomorphic to $V^{\oplus l}$. Now let $N_{l+1} \subset M$ be the image of the map $f_{l+1} : V \to M$. By part (i), N_{l+1} is a submodule which is isomorphic to V. Suppose that

$$N_{\leq l} \cap N_{l+1} \neq \{0\} \tag{1}$$

The intersection of any two submodules is a submodule (this follows immediately from the definition of a submodule), so $N_{\leq l} \cap N_{l+1}$ is a submodule of N_{l+1}. But $N_{l+1} \cong V$ is a simple A_V-module, so we must have

$$N_{\leq l} \cap N_{l+1} = N_{l+1}$$

i.e. N_{l+1} is contained in $N_{\leq l}$. This implies that f_{l+1} defines an A_V-linear map

$$f_{l+1} : V \to N_{\leq l}$$

Each of the maps $f_1, ..., f_l$ also defines an A_V-linear map from V to $F_{\leq l}$, so we have a subset

$$\{f_1, ..., f_{l+1}\} \subset \mathrm{Hom}_{A_V}(V, N_{\leq l})$$

of size $l + 1$. However, the dimension of this space is

$$\begin{aligned} \dim \mathrm{Hom}_{A_V}(V, N_{\leq l}) &= \dim \mathrm{Hom}_{A_V}(V, V^{\oplus l}) \quad \text{(by the inductive hypothesis)} \\ &= \dim \mathrm{Hom}_{A_V}(V, V)^{\oplus l} \ = \ l \end{aligned}$$

by Schur's Lemma (Proposition 3.2.12). Therefore the maps $f_1, ..., f_{l+1}$ cannot be linearly independent, which contradicts the fact that $\{f_1, ..., f_k\}$ is a basis for $\mathrm{Hom}_{A_V}(V, M)$. We conclude that (1) is impossible, and actually $N_{\leq l} \cap N_{l+1} = \{0\}$.

The image of the map

$$F_{\leq l+1} : V^{\oplus l+1} \to M$$

is a submodule of M, and it's spanned by the two submodules $N_{\leq l}$ and N_{l+1}. Since these have trivial intersection, it follows that

$$\mathrm{Im}(F_{\leq l+1}) \cong N_{\leq l} \oplus N_{l+1} \cong V^{\oplus l} \oplus V$$

So $F_{\leq l+1}$ is an isomorphism onto its image, i.e. it's an injection. This proves the inductive step and completes the proof of theorem.

□

Second proof of Theorem 3.3.6. We use the same A_V-linear map

$$F : V^{\oplus k} \to M$$

as in the first proof above. This time, we're going to prove that F is a surjection.

Pick any $x \in M$. We need to show that x is in the image of F. Under the isomorphism between M and $\mathrm{Hom}_{A_V}(A_V, M)$, the vector x corresponds to the A_V-linear map

$$\begin{aligned} T_x \colon A_V &\to M \\ a &\mapsto ax \end{aligned}$$

In particular, $T_x(1_A) = x$. Now pick a basis for V, so we can identify $V \cong \mathbb{C}^n$ (the space of column vectors). We can also identify $A_V = \mathrm{Mat}_{n\times n}(\mathbb{C})$, and we have A_V-linear injections

$$\iota_t \colon V \to A_V$$

given by mapping $\mathbb{C}^n$ to the space $(A_V)_{\bullet t}$ of matrices which are zero outside the tth column. Let $e_1, ..., e_n$ be the standard basis for $\mathbb{C}^n$, then

$$\sum_{t=1}^{n} \iota_t(e_t) = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix} = I_n = 1_{A_V}$$

So

$$T_x\left(\sum_{t=1}^{n} \iota_t(e_t)\right) = \sum_{t=1}^{n} (T_x \circ \iota_t)(e_t) = x \in M$$

Now each map $T_x \circ \iota_t$ is in $\mathrm{Hom}_{A_V}(V, M)$, so it can be written as a linear combination of the basis vectors

$$T_x \circ \iota_t = \lambda_t^1 f_1 + \ldots + \lambda_t^k f_k$$

for some coefficients $\lambda_t^i \in \mathbb{C}$. Therefore

$$\begin{aligned} x &= \sum_{t=1}^{n} (T_x \circ \iota_t)(e_t) & &= \sum_{t=1}^{n} \sum_{i=1}^{k} \lambda_t^i f_i(e_t) \\ &= \sum_{i=1}^{k} f_i\left(\sum_{t=1}^{n} \lambda_t^i e_t\right) & &= F\left(\sum_{t=1}^{n} \lambda_t^1 e_t, \ldots, \sum_{t=1}^{n} \lambda_t^k e_t\right) \end{aligned}$$

So F is indeed surjective. □

[Aside: What we've actually proved is that M is isomorphic as an A_V-module to

$$V \otimes \mathrm{Hom}_{A_V}(V, M)$$

where we give the latter an A_V-module structure by letting A_V act only on the V factor.]

So up to isomorphism, there is one A_V-module

$$V,\ V^{\oplus 2},\ \ldots,\ V^{\oplus k},\ \ldots$$

for each positive integer k. This is similar to the situation for vector spaces (= $\mathbb{C}$-modules), up to isomorphism there's one vector space

$$\mathbb{C},\ \mathbb{C}^2,\ \ldots,\ \mathbb{C}^k,\ \ldots$$

for each k. This similarity goes further. Since V is simple (Lemma 3.3.2), we have

$$\mathrm{Hom}_{A_V}(V, V) = \mathbb{C} = \mathrm{Hom}(\mathbb{C}, \mathbb{C})$$

by Schur's Lemma (Proposition 3.2.12). How about $\mathrm{Hom}_{A_V}(V^{\oplus 2}, V^{\oplus 2})$? We have

$$\mathrm{Hom}_{A_V}(V^{\oplus 2}, V^{\oplus 2}) = \mathrm{Hom}_{A_V}(V, V)^{\oplus 4}$$

i.e. to specify an A_V-linear map $f\colon V^{\oplus 2} \to V^{\oplus 2}$ we have to give four maps $f_{11}, f_{12}, f_{21}, f_{22} \in \mathrm{Hom}_{A_V}(V, V)$. Then

$$f(x_1, x_2) = (f_{11}(x_1) + f_{12}(x_2), f_{21}(x_1) + f_{22}(x_2))$$

But each $f_{ji} \in \mathrm{Hom}_{A_V}(V, V)$ is just a complex number, so we can write the above formula as

$$f(x_1, x_2) = \begin{pmatrix} f_{11} & f_{12} \\ f_{21} & f_{22} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$$

Writing it this way, it should be clear that the composition of two A_V-linear maps from $V^{\oplus 2}$ to $V^{\oplus 2}$ is given by multiplying together the two corresponding 2×2-matrices. So we have an isomorphism of algebras

$$\mathrm{Hom}_{A_V}(V^{\oplus 2}, V^{\oplus 2}) \cong \mathrm{Mat}_{2\times 2}(\mathbb{C}) = \mathrm{Hom}(\mathbb{C}^2, \mathbb{C}^2)$$

(we'll prove this more carefully in the next section). More generally:

$$\begin{aligned} \mathrm{Hom}_{A_V}(V^{\oplus k}, V^{\oplus l}) &= \mathrm{Mat}_{l\times k}(\mathbb{C}) \\ &= \mathrm{Hom}(\mathbb{C}^k, \mathbb{C}^l) \end{aligned}$$

and composition of maps corresponds to matrix multiplication.

So A_V-modules match up with $\mathbb{C}$-modules, and A_V-linear maps match up with $\mathbb{C}$-linear maps. Technically, this is called an **equivalence of categories**. We say that A_V and $\mathbb{C}$ are **Morita equivalent**.

3.4 Semi-simple algebras

Definition 3.4.1. An A-module M is **semi-simple** if it's isomorphic to a direct sum of simple A-modules.

This was not an important concept for representations of groups. This is because, thanks to Maschke's Theorem, every representation of a group is semi-simple. But for general algebras, this is not true.

Example 3.4.2. Let $A = \langle 1, x \rangle$ with $x^2 = 0$. Let M be the A-module given by A itself. Let's look for 1-dimensional submodules of M, i.e. subspaces

$$\langle \lambda + \mu x \rangle \subset A$$

that are preserved under left-multiplication by all elements of A. We must have

$$x(\lambda + \mu x) = \lambda x \in \langle \lambda + \mu x \rangle$$

So $\lambda = 0$, and hence the subspace $\langle x \rangle$ is the only 1-dimensional submodule. So M is not simple (it contains a 1-dimensional submodule), but also it doesn't split up as a sum of a direct sum of simples, so M is not semi-simple either.

Proposition 3.4.3. *If M is a semi-simple module, then its decomposition into simple A-modules is unique, up to isomorphism and re-ordering of the summands.*

Proof. This is a generalisation of Theorem 1.8.6, and the proof is exactly the same. If N is any simple module, then $\dim \mathrm{Hom}_A(N, M)$ is the multiplicity with which N occurs in M. $\square$

Definition 3.4.4. An algebra A is **semi-simple** if every A module is semi-simple.

So $\mathbb{C}[G]$ is semi-simple for any finite group, but Example 3.4.2 shows that the algebra $\langle 1, x\rangle$ is not semi-simple.

By Theorem 3.3.6, the matrix algebra $A_V = \mathrm{Hom}(V, V)$ is semi-simple, because every A_V-module is a direct sum of copies of the simple A_V-module V.

Theorem 3.4.5 (Classification of semi-simple algebras)**.** *Let A be an algebra. The following are equivalent:*

(i) A is semi-simple.

(ii) The A-module A is a semi-simple module.

(iii) A is isomorphic to a direct sum of matrix algebras.

[Aside: This is over $\mathbb{C}$. It can be generalised to other fields but the statement becomes more complicated.]

Notice that (i) $\Rightarrow$ (ii) by definition. The fact that (iii) $\Rightarrow$ (i) folllows immediately from the following:

Lemma 3.4.6. *If A and B are semi-simple algebras then so is $A \oplus B$.*

Proof. By Lemma 3.2.15 every module over $A \oplus B$ is a direct sum $M \oplus N$ for an A-module M and a B-module N. If A and B are semi-simple, we have further splittings

$$\begin{aligned} M &= M_1 \oplus \ldots \oplus M_k \\ N &= N_1 \oplus \ldots \oplus N_l \end{aligned}$$

where the M_i are simple A-modules and the N_j are simple B-modules. But then each M_i and N_j is a simple $A \oplus B$ module, so $M \oplus N$ is semi-simple. So every $(A \oplus B)$-module is semi-simple. $\square$

Every matrix algebra is semi-simple, so this proves that (iii)$\Rightarrow$(i) in Theorem 3.4.5. The hardest part of the theorem is the fact that (ii)$\Rightarrow$ (iii). We'll prove it in stages.

Lemma 3.4.7. *For any algebra A, there is a natural isomorphism of algebras*

$$A^{op} = \mathrm{Hom}_A(A, A)$$

Proof. We know (Lemma 3.3.4) that for any A-module M there is a natural isomorphism of vector spaces

$$\begin{aligned} T : \mathrm{Hom}_A(A, M) &\to M \\ f &\mapsto f(1_A) \end{aligned}$$

Setting $M = A$, we get an isomorphism of vector spaces

$$T\colon\ \mathrm{Hom}_A(A, A) \to A$$

We have

$$T(f) = f(1_A) = f(1_A)1_A$$

and therefore

$$T(g \circ f) = (g \circ f)(1_A) = g(f(1_A)) = f(1_A)g(1_A)$$

since g is A-linear. This says that T is a homomorphism from $\mathrm{Hom}_A(A, A)$ to A^{op}. $\square$

Lemma 3.4.8. *For any algebra A, and any simple A-module M, we have an isomorphism of algebras*

$$\mathrm{Hom}_A(M^{\oplus k}, M^{\oplus k}) \cong \mathrm{Mat}_{k\times k}(\mathbb{C})$$

We saw a rough argument for this in the previous section, in the case that $A = A_V$ and $M = V$.

Proof. Let e_{ji} be the matrix that maps e_i to e_j, i.e. the (ij)-th entry is 1 and all other entries are zero. These matrices form a basis for $\mathrm{Mat}_{k\times k}(\mathbb{C})$ (in fact they're the standard basis), and they obey the relations

$$e_{ji}e_{pq} = \begin{cases} e_{jq} & \text{if } i = p \\ 0 & \text{if } i \neq p \end{cases}$$

Now let

$$\pi_i : M^{\oplus k} \to M$$
$$\iota_j : M \to M^{\oplus k}$$

be projection onto on the ith factor and inclusion of the jth factor respectively, and define

$$f_{ji} = \iota_j \circ \pi_i : M^{\oplus k} \to M^{\oplus k}$$

These maps are evidently linearly independent, and obey the same relations as the e_{ji}.

We define a linear map from $\mathrm{Mat}_{k\times k}(\mathbb{C})$ to $\mathrm{Hom}_A(M^{\oplus k}, M^{\oplus k})$ by sending e_{ji} to f_{ji}. This map is injective because the f_{ji} are linearly-independent, and it's an algebra homomorphism because it respects the relations between the e_{ji}. So it must be an isomorphism, because

$$\dim \mathrm{Hom}_A(M^{\oplus k}, M^{\oplus k}) = \dim \mathrm{Hom}_A(M, M)^{\oplus k^2} = k^2 = \dim \mathrm{Mat}_{k\times k}(\mathbb{C})$$

by Schur's Lemma. □

Now we can finish the proof of the theorem.

Proof of Theorem 3.4.5(ii)⇒(iii). Assume A is a semi-simple A-module. So we have an isomorphism of A-modules

$$A = M_1^{\oplus m_1} \oplus \ldots \oplus M_k^{\oplus m_k}$$

for some numbers $m_1, \ldots, m_k$ where each M_i is a simple module, and M_i is not isomorphic to M_j for $i \neq j$. Then by Lemma 3.4.7,

$$\begin{aligned} A^{op} &= \mathrm{Hom}_A(A, A) \\ &= \bigoplus_{i,j} \mathrm{Hom}_A(M_i^{\oplus m_i}, M_j^{\oplus m_j}) \\ &= \mathrm{Hom}_A(M_1^{\oplus m_1}, M_1^{\oplus m_1}) \oplus \ldots \oplus \mathrm{Hom}_A(M_k^{\oplus m_k}, M_k^{\oplus m_k}) \end{aligned}$$

by Schur's Lemma. By Lemma 3.4.8 we have

$$\mathrm{Hom}_A(M_i^{\oplus m_i}, M_i^{\oplus m_i}) = \mathrm{Mat}_{m_i\times m_i}(\mathbb{C})$$

So

$$A^{op} = \mathrm{Mat}_{m_1 \times m_1}(\mathbb{C}) \oplus \ldots \oplus \mathrm{Mat}_{m_k \times m_k}(\mathbb{C})$$

and thus

$$A = \mathrm{Mat}_{m_1 \times m_1}(\mathbb{C})^{op} \oplus \ldots \oplus \mathrm{Mat}_{m_k \times m_k}(\mathbb{C})^{op}$$

But each $\mathrm{Mat}_{m_i \times m_i}(\mathbb{C})^{op}$ is a matrix algebra by Lemma 3.3.1. □

This completes the proof of Theorem 3.4.5.

If we look at the proof of the theorem again, we see we can actually make some more precise statements, which we list as the following corollaries.

Corollary 3.4.9. *Let A be a semi-simple algebra. Then A has only finitely-many simple modules up to isomorphism.*

Proof. We know A is isomorphic to

$$\mathrm{Hom}(V_1, V_1) \oplus \ldots \oplus \mathrm{Hom}(V_r, V_r)$$

for some vector spaces $V_1, \ldots, V_r$. Each V_i is a simple $\mathrm{Hom}(V_i, V_i)$-module, and hence is also a simple A-module. By Lemma 3.2.15 and Theorem 3.3.6, every A-module is a direct sum of copies of these r simple modules. In particular, $V_1, \ldots, V_r$ are the only simple A-modules. □

Corollary 3.4.10. *Let A be a semi-simple algebra and let the simple A-modules be $M_1, \ldots, M_r$, where M_i has dimension d_i. Then*

(i) A is isomorphic as an A-module to

$$M_1^{\oplus d_1} \oplus \ldots \oplus M_r^{\oplus d_r}$$

(ii) A is isomorphic as an algebra to

$$\mathrm{Mat}_{d_1 \times d_1}(\mathbb{C}) \oplus \ldots \oplus \mathrm{Mat}_{d_r \times d_r}(\mathbb{C})$$

Proof. Since A is semi-simple, A is isomorphic as an A-module to

$$\bigoplus_{i=1}^{r} M_i^{\oplus m_i}$$

for some numbers $m_1, \ldots, m_r$. We observed in the proof of Theorem 3.4.5 ((ii)⇒(iii)) that this implies that A is isomorphic as an algebra to

$$\bigoplus_{i=1}^{r} \mathrm{Mat}_{m_i \times m_i}(\mathbb{C})$$

But then there are r simple A-modules with dimensions $m_1, \ldots, m_r$, i.e. we must have $d_i = m_i$ for all i. This proves (i) and (ii). □

Corollary 3.4.11. *Let A be semi-simple, and let the dimensions of the simple A-modules be $d_1, \ldots, d_r$. Then*

$$\dim A = \sum_{i=1}^{r} d_i^2$$

Proof. Immediate from Corollary 3.4.10(ii). □

Our favourite example of a semi-simple algebra is a group algebra. Setting $A = \mathbb{C}[G]$ in the above results, we recover Theorem 1.8.8, Corollary 1.8.9 and Corollary 1.8.12 as special cases. But we also have a new result, which is a special case of Corollary 3.4.10(ii):

Corollary 3.4.12. *Let G be a group, and let $d_1, \ldots, d_r$ be the dimensions of the irreps of G. Then $\mathbb{C}[G]$ is isomorphic as an algebra to*

$$\mathrm{Mat}_{d_1 \times d_1}(\mathbb{C}) \oplus \ldots \oplus \mathrm{Mat}_{d_r \times d_r}(\mathbb{C})$$

As we've stated it, this result only tells us that such an isomorphism exists, it doesn't tell us how to write one down. In the case $G = C_2$, we actually found an isomorphism

$$\mathbb{C}[C_2] \xrightarrow{\sim} \mathbb{C} \oplus \mathbb{C}$$

explicitly (and the case $G = C_3$ is in the Problem Sheets). In fact with just a little more work we can see how to find this isomorphism more explicitly for a general G.

Proposition 3.4.13. *Let A be semi-simple, and let $M_1, ..., M_r$ be the simple A-modules. Let*

$$\tilde{\rho}_i : A \to \mathrm{Hom}(M_i, M_i)$$

be the module structure maps for each simple module, and let

$$\tilde{\rho} = (\tilde{\rho}_1, ..., \tilde{\rho}_r) : A \to \mathrm{Hom}(M_1, M_1) \oplus ... \oplus \mathrm{Hom}(M_r, M_r)$$

Then $\tilde{\rho}$ is an isomorphism of algebras.

This proposition is a more precise version of Corollary 3.4.10(ii).

Proof. Firstly, suppose A is a matrix algebra A_V. There is only simple A_V-module, namely the vector space V (with its canonical A_V-module structure). Then the proposition claims that the map

$$\tilde{\rho} : A_V \to \mathrm{Hom}(V, V)$$

is an isomorphism, which is certainly true, since this map is actually the identity! More generally, suppose that A is a direct sum of matrix algebras, $A = A_{V_1} \oplus ... \oplus A_{V_r}$. Then A has r simple modules, given by the vector spaces $V_1, ..., V_r$. So the map $\tilde{\rho}$ is again the identity map

$$\tilde{\rho} : A \to \mathrm{Hom}(V_1, V_1) \oplus ... \oplus \mathrm{Hom}(V_r, V_r)$$

so it's an isomorphism. But every semi-simple algebra is isomorphic to a direct sum of matrix algebras, so the proposition is true. □

Corollary 3.4.14. *Let G be a group, and let*

$$\rho_i \colon G \to \mathrm{Hom}(U_i, U_i)$$

be the irreps of G. Let

$$\tilde{\rho}_i : \mathbb{C}[G] \to \mathrm{Hom}(U_i, U_i)$$

be the linear extension of ρ_i, and let

$$\tilde{\rho} = (\tilde{\rho}_1, \ldots, \tilde{\rho}_r) \colon \mathbb{C}[G] \to \bigoplus_{i=1}^{r} \mathrm{Hom}(U_i, U_i)$$

Then $\tilde{\rho}$ is an isomorphism of algebras.

Example 3.4.15. Let $G = S_3 = \langle \sigma, \tau \mid \sigma^3 = \tau^2 = e, \sigma\tau = \tau\sigma^2 \rangle$. G has three irreps of dimensions 1, 1 and 2, so we have an isomorphism

$$\mathbb{C}[G] \xrightarrow{\sim} \mathbb{C} \oplus \mathbb{C} \oplus \mathrm{Mat}_{2\times 2}(\mathbb{C})$$
$$\sigma \mapsto \left(1, 1, \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix}\right)$$
$$\tau \mapsto \left(1, -1, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right)$$

(where $\omega = e^{\frac{2\pi i}{3}}$).

There's a nicer way to write this. We can view $\mathrm{Mat}_{n\times n}(\mathbb{C}) \oplus \mathrm{Mat}_{m\times m}(\mathbb{C})$ as a subalgebra of $\mathrm{Mat}_{(n+m)\times(n+m)}(\mathbb{C})$ consisting of block-diagonal matrices

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

So in the above example, we have a homomorphism

$$\mathbb{C}[G] \to \mathrm{Mat}_{4\times 4}(\mathbb{C})$$
$$\sigma \mapsto \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \omega & 0 \\ 0 & 0 & 0 & \omega^{-1} \end{pmatrix}$$
$$\tau \mapsto \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

which is an isomorphism onto the subalgebra of block-diagonal matrices (with blocks of sizes 1, 1, and 2). Of course, this is just the matrix representation corresponding to $U_1 \oplus U_2 \oplus U_3$.

3.5 Centres of algebras

Definition 3.5.1. Let A be an algebra. The **centre** of A is the subspace

$$Z_A = \{z \in A \mid za = az, \ \ \forall a \in A\}$$

Z_A is a subalgebra of A, and it's commutative. Obviously $Z_A = A$ iff A is commutative.

Proposition 3.5.2. *Let V be a vector space, and $A_V = \mathrm{Hom}(V, V)$. Then*

$$Z_A = \{\lambda \mathbf{1}_V \mid \lambda \in \mathbb{C}\}$$

so Z_A is the 1-dimensional algebra.

Proof. Pick a basis for V, so $A_V = \mathrm{Mat}_{n\times n}(\mathbb{C})$. Then the statement is that the only matrices that commute with all other matrices are λI_n for $\lambda \in \mathbb{C}$. This is easy to check. □

Corollary 3.5.3. *Let A be a semi-simple algebra. Then Z_A is isomorphic (as an algebra) to $\mathbb{C}^{\oplus r}$, where r is the number of simple A-modules.*

Proof. By Proposition 3.4.13, A is isomorphic to a direct sum of matrix algebras $A_{M_1} \oplus ... \oplus A_{M_r}$, where $M_1, ..., M_r$ are the simple A-modules. It's elementary to check that $Z_{A_1 \oplus A_2} = Z_{A_1} \oplus Z_{A_2}$ for any two algebras A_1 and A_2, and the result follows. □

Now let $A = \mathbb{C}[G]$ for a group G. If $g \in G$ is in the centre of G (i.e. it commutes with all other group elements), then clearly $\lambda g \in A$ lies in Z_A for any $\lambda \in \mathbb{C}$. However, Z_A is usually larger than this.

Proposition 3.5.4. *Let $A = \mathbb{C}[G]$. Then $Z_A \subset A$ is spanned by the elements*

$$z_{[g]} = \sum_{h\in[g]} h \in A$$

for each conjugacy class $[g]$ in G.

Proof. Let $G = \{g_1, \ldots, g_k\}$, so a general element of $\mathbb{C}[G]$ looks like

$$a = \lambda_{g_1} g_1 + \ldots \lambda_{g_k} g_k$$

for some $\lambda_{g_1}, \ldots, \lambda_{g_k} \in \mathbb{C}$. Then a is in Z_A iff

$$ag = ga \quad \Longleftrightarrow \quad g^{-1}ag = a$$

for all $g \in G$. This holds iff

$$\lambda_{gg_ig^{-1}} = \lambda_{g_i}$$

for all g and g_i in G, i.e. iff

$$a = \sum_{\substack{\text{conjugacy classes} \\ [g] \text{ in } G}} \lambda_{[g]} z_{[g]}$$

for some scalars $\lambda_{[g]} \in \mathbb{C}$.

$\square$

The elements $z_{[g]}$ are obviously linearly independent, so $\dim Z_{\mathbb{C}[G]}$ is the number of conjugacy classes in G. If we identify $\mathbb{C}[G]$ with $\mathbb{C}^G$ by sending

$$g \leftrightarrow \delta_g$$

then the element $z_{[g]}$ maps to $\delta_{[g]}$, and $Z_{\mathbb{C}[G]}$ corresponds exactly to the space of class functions

$$\mathbb{C}^G_{cl} \subset \mathbb{C}^G$$

We are finally in a position to explain the proof of Theorem 2.3.3, that for any group G

$$\#\{\text{conjugacy classes in } G\} = \#\{\text{irreps of } G\}$$

Proof of Theorem 2.3.3. Let $U_1, \dots, U_r$ be the irreps of G. Then we know from Corollary 3.4.14 that we have an isomorphism of algebras

$$\tilde{\rho} : \mathbb{C}[G] \to A_{U_1} \oplus ... \oplus A_{U_r}$$

By Corollary 3.5.3 this means that $Z_{\mathbb{C}[G]}$ is isomorphic to $\mathbb{C}^{\oplus r}$, and in particular that $\dim Z_{\mathbb{C}[G]} = r$. Since $\dim Z_{\mathbb{C}[G]}$ is also the number of conjugacy classes in G, this proves the theorem. $\square$

A Revision on linear maps and matrices

This appendix contains some brief revision material on the relationship between matrices and linear maps.

A.1 Vector spaces and bases

We let $\mathbb{C}^n$ be the set of column vectors

$$\begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_n \end{pmatrix}, \quad \lambda_i \in \mathbb{C}$$

This is a vector space of dimension n (over $\mathbb{C}$). It comes with its *standard basis* $e_1, e_2, ..., e_n$, where e_i is the column vector in which $\lambda_i = 1$ and all the other λ_j are zero. We can write the column vector above as $\sum_{i=1}^{n} \lambda_i e_i$.

Now let V be an abstract n-dimensional vector space (over $\mathbb{C}$).

Proposition A.1.1. *Choosing a basis for V is the same thing as choosing an isomorphism*

$$f : \mathbb{C}^n \xrightarrow{\sim} V$$

Proof. Suppose we've chosen such an isomorphism f. Then the images of the standard basis vectors under f give us a basis for V. Conversely, suppose $a_1, ..., a_n \in V$ is a basis. Define a linear map $f : \mathbb{C}^n \to V$ by mapping e_i to a_i, and then extending linearly. Then f is an isomorphism, because every vector $v \in V$ can be uniquely expressed as a linear combination

$$v = \lambda_1 a_1 + \lambda_2 a_2 + ... + \lambda_n a_n$$

□

A.2 Linear maps and matrices

Proposition A.2.1. *Linear maps from $\mathbb{C}^n$ to $\mathbb{C}^m$ are the same thing as $m \times n$ matrices (with complex coefficients).*

Proof. Each matrix $M \in \mathrm{Mat}_{m\times n}(\mathbb{C})$ defines a linear map

$$\phi : \mathbb{C}^n \to \mathbb{C}^m$$

by multiplying column vectors by M (on the left). Notice that the image $\phi(e_i)$ of the ith standard basis vector is the column vector which forms the ith column of M.

Conversely, suppose $\phi : \mathbb{C}^n \to \mathbb{C}^m$ is any linear map. Let $M \in \mathrm{Mat}_{m\times n}(\mathbb{C})$ be the matrix whose columns are the vectors $\phi(e_1), \phi(e_2), ..., \phi(e_n)$, i.e.

$$\phi(e_i) = \sum_{j=1}^{m} M_{ji}\tilde{e}_j$$

where $\tilde{e}_1, ..., \tilde{e}_m$ is the standard basis for $\mathbb{C}^m$. Then for any column vector

$$v = \sum_{i=1}^{n} \lambda_i e_i \in \mathbb{C}^n$$

we have

$$\phi(v) = \sum_{i=1}^{n} \lambda_i \phi(e_i) \qquad = \sum_{i=1}^{n} \lambda_i \left(\sum_{j=1}^{m} M_{ji}\tilde{e}_j \right) \qquad = \sum_{j=1}^{m} \left(\sum_{i=1}^{n} M_{ji}\lambda_i \right) \tilde{e}_j$$

so the linear map ϕ is exactly multiplication by the matrix M. □

Corollary A.2.2. *Let V and W be abstract vector space of dimensions n and m respectively. Choose a basis $\mathcal{A} = \{a_1, ..., a_n\}$ for V, and a basis $\mathcal{B} = \{b_1, ..., b_m\}$ for W. Then we have a bijection between the set of linear maps from V to W and the set of $m \times n$ matrices.*

Proof. Because we've chosen bases for V and W, we have corresponding isomorphims

$$f_{\mathcal{A}} : \mathbb{C}^n \xrightarrow{\sim} V, \qquad\qquad f_{\mathcal{B}} : \mathbb{C}^m \xrightarrow{\sim} W$$

by Proposition A.1.1. Let

$$\varphi : V \to W$$

be a linear map. Then the composition

$$\phi = f_{\mathcal{B}}^{-1} \circ \varphi \circ f_{\mathcal{A}}$$

is a linear map from $\mathbb{C}^n$ to $\mathbb{C}^m$, so it has a corresponding matrix M. Conversely, any matrix $M \in \mathrm{Mat}_{m\times n}$ defines a linear map $\phi : \mathbb{C}^n \to \mathbb{C}^m$, and hence a linear map

$$\varphi = f_{\mathcal{B}} \circ \phi \circ f_{\mathcal{A}}^{-1} : V \to W$$

Clearly this gives a bijection between linear maps and matrices. □

Let's make this bijection between linear maps and matrices more explicit. Consider the diagram:

$$\begin{tikzcd} V \arrow[r, "\varphi"] & W \\ \mathbb{C}^n \arrow[u, "f_{\mathcal{A}}"] \arrow[r, "\phi"] & \mathbb{C}^m \arrow[u, "f_{\mathcal{B}}"'] \end{tikzcd}$$

By the definition of the matrix M, we have

$$\phi(e_i) = \sum_{j=1}^{m} M_{ji}\tilde{e}_j$$

Thus

$$\begin{aligned} \varphi(a_i) &= \varphi(f_{\mathcal{A}}(e_i)) = f_{\mathcal{B}}(\phi(e_i)) \\ &= f_{\mathcal{B}}\left(\sum_{j=1}^{m} M_{ji}\tilde{e}_j\right) = \sum_{j=1}^{m} M_{ji} f_{\mathcal{B}}(\tilde{e}_j) \\ &= \sum_{j=1}^{m} M_{ji} b_j \end{aligned}$$

So the ith column of M is the image of the basis vector a_i, expressed as a column vector using the basis $\mathcal{B}$.

Proposition A.2.3. *Let $\phi : \mathbb{C}^n \to \mathbb{C}^m$ be a linear map with corresponding matrix M, and let $\psi : \mathbb{C}^m \to \mathbb{C}^p$ be a linear map with corresponding matrix N. Then the composition $\psi \circ \phi$ corresponds to the matrix product NM.*

Proof. We have

$$\phi(e_i) = \sum_{j=1}^{m} M_{ji}\tilde{e}_j, \qquad \psi(\tilde{e}_j) = \sum_{k=1}^{p} N_{kj}\hat{e}_k$$

where $\hat{e}_1, ..., \hat{e}_p$ is the standard basis for $\mathbb{C}^p$. Therefore

$$\begin{aligned}
(\psi \circ \phi)(e_i) &= \psi\left(\sum_{j=1}^{m} M_{ji}\tilde{e}_j\right) && = \sum_{j=1}^{m} M_{ji}\psi(\tilde{e}_j) \\
&= \sum_{j=1}^{m} M_{ji}\left(\sum_{k=1}^{p} N_{kj}\hat{e}_k\right) && = \sum_{k=1}^{p}\left(\sum_{j=1}^{m} N_{kj}M_{ji}\right)\hat{e}_k \\
&= \sum_{k=1}^{p}(NM)_{ki}\hat{e}_k
\end{aligned}$$

So the matrix NM corresponds to $\psi \circ \phi$. $\square$

A.3 Changing basis

Let V be an n-dimensional vector space, and let $\mathcal{A} = \{a_1, ..., a_n\} \subset V$ and $\mathcal{C} = \{c_1, ..., c_n\} \subset V$ be two different possible bases for V. Then by Proposition A.1.1 we have isomorphisms

$$\begin{tikzcd}
& V & \\
\mathbb{C}^n \arrow[ur, "f_{\mathcal{A}}"] & & \mathbb{C}^n \arrow[ul, "f_{\mathcal{C}}"'] \arrow[ll, "f_{\mathcal{A}}^{-1} \circ f_{\mathcal{C}}"]
\end{tikzcd}$$

The composition $f_{\mathcal{A}}^{-1} \circ f_{\mathcal{C}}$ is an isomorphism from $\mathbb{C}^n$ to $\mathbb{C}^n$, so it correponds to some invertible $n \times n$ matrix P. We'll call P the *change-of-basis matrix* between $\mathcal{A}$ and $\mathcal{C}$. Note that

$$\begin{aligned}
c_i = f_{\mathcal{C}}(e_i) &= f_{\mathcal{A}}(f_{\mathcal{A}}^{-1} \circ f_{\mathcal{C}}(e_i)) && = f_{\mathcal{A}}\left(\sum_{j=1}^{n} P_{ji}e_j\right) \\
= \sum_{j=1}^{n} P_{ji}f_{\mathcal{A}}(e_j) &= P_{1i}a_1 + P_{2i}a_2 + ... + P_{ni}a_n
\end{aligned}$$

i.e. the entries of P tell you the coefficients of the vectors in the second basis $\mathcal{C}$, expressed using the first basis $\mathcal{A}$.

In particular, suppose that V is actually $\mathbb{C}^n$, and that $\mathcal{A} = \{e_1, ..., e_n\}$ is the standard basis (so $f_\mathcal{A}$ is the identity map). Then the columns of P are the vectors that form the second basis $\mathcal{C}$. This gives a bijection between the set of possible bases for $\mathbb{C}^n$ and the set of invertible $n \times n$ matrices.

Now let V and W be two vector spaces, of dimensions n and m respectively. In Corollary A.2.2 we saw that linear maps from V and W corresponded to $n \times m$ matrices, *after* we'd chosen bases for V and W. For a given linear map φ, the matrix that we write down depends on our choice of bases, and if we change our choice of bases then the matrix that represents φ will also change.

Proposition A.3.1. *Let V and W be two vector spaces of dimensions n and m respectively, and let*

$$\varphi : V \to W$$

be a linear map. Let $\mathcal{A}$ be a basis for V and $\mathcal{B}$ be a basis for W, and let

$$M \in \mathrm{Mat}_{n\times n}(\mathbb{C})$$

be the matrix representing φ with respect to the bases $\mathcal{A}$ and $\mathcal{B}$. Now let $\mathcal{C}$ be a second choice of basis for V, and let N be the matrix representing φ with respect to the bases $\mathcal{C}$ and $\mathcal{B}$. Then

$$N = MP$$

where P is the change-of-basis matrix between $\mathcal{A}$ and $\mathcal{C}$.

Proof. Examine the following diagram:

$$\begin{tikzcd}
\mathbb{C}^n \arrow[dr, "f_\mathcal{C}"] \arrow[dd, "f_\mathcal{A}^{-1}\circ f_\mathcal{C}"'] \arrow[drrr, bend left, "f_\mathcal{B}^{-1}\circ\varphi\circ f_\mathcal{C}"] & & & \\
& V \arrow[r, "\varphi"] & W & \mathbb{C}^m \arrow[l, "f_\mathcal{B}"'] \\
\mathbb{C}^n \arrow[ur, "f_\mathcal{A}"'] \arrow[urrr, bend right, "f_\mathcal{B}^{-1}\circ\varphi\circ f_\mathcal{A}"'] & & &
\end{tikzcd}$$

We have

$$(f_\mathcal{B}^{-1} \circ \varphi \circ f_\mathcal{C}) = (f_\mathcal{B}^{-1} \circ \varphi \circ f_\mathcal{A}) \circ (f_\mathcal{A}^{-1} \circ f_\mathcal{C})$$

These three linear maps correspond to the matrices N, M and P respectively, so

$$N = MP$$

by Proposition A.2.3. $\square$

Now suppose that $\mathcal{D}$ is a second choice of basis for W, and let Q be the change-of-basis matrix between $\mathcal{B}$ and $\mathcal{D}$. A very similar proof shows that the matrix representing φ with respect to the bases $\mathcal{A}$ and $\mathcal{D}$ is

$$Q^{-1}M$$

and that the matrix representing φ with respect to $\mathcal{C}$ and $\mathcal{D}$ is

$$Q^{-1}MP$$

Now let's specialize to the case that W and V are actually the same vector space:

Corollary A.3.2. *Let V be an n-dimensional vector space.*

i) If we choose a basis $\mathcal{A}$ for V, then we get a bijection between $\mathrm{Mat}_{n\times n}(\mathbb{C})$ and the set of linear maps from V to V.

ii) Let

$$\varphi : V \to V$$

be a linear map, and let M be the matrix representing φ with respect to the basis $\mathcal{A}$. Now let $\mathcal{C}$ be another basis for V, and let P be the change-of-basis matrix between $\mathcal{A}$ and $\mathcal{C}$. Then the matrix representing φ with respect to the basis $\mathcal{C}$ is

$$P^{-1}MP$$