Group Representation Theory

Ed Segal

laTexed by Fatema Daya and Zach Smith

2012

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

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:

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

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.

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

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 from Example 1.1.1? The eigenvalues of M are $\pm i$, so M cannot be diagonalised over $\mathbb{R}$, but it can be diagonaized 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.

Notice, we don't assume that ρ is injective, i.e. it doesn't need to be an isomorphism onto its image. If it is an injection, we say ρ 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 representation of C_6. But $\rho(\mu^3) = 1$ also, so

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

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 dimension n). The kernel is equal to G.

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

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

given by

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

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, so we get an isomorphism $GL(V) \cong GL_n(\mathbb{C})$ (dependent on the basis). However, often we don't actually want to choose a basis.

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 defintions, 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 $\{a_1, \ldots, a_n\}$ and $\{b_1, \ldots, b_n\}$ be two bases for V. Then the two associated matrix representations*

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

are equivalent.

Proof. Since $\{a_1, \ldots, a_n\}$ and $\{b_1, \ldots, b_n\}$ are bases, $\exists$ invertible matrix P such that

$$b_i = \sum_{j=1}^{n} P_{ji} a_j$$

and hence

$$a_i = \sum_{j=1}^{n} (P^{-1})_{ji} b_j$$

Fix a $g \in G$, so we have a linear map

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

The matrix $\rho_1(g)$ is the matrix M that represents the action of $\rho(g)$ on the basis $\{a_1, \ldots, a_n\}$, i.e.

$$\rho(g) : a_i \mapsto \sum_{j=1}^{n} M_{ji} a_j$$

Similarly, $\rho_2(g)$ is the matrix N such that

$$\rho(g) : b_i \mapsto \sum_{j=1}^{n} N_{ji} b_j$$

Since $\rho(g)$ is a linear map, and

$$b_i = \sum_{j=1}^{n} P_{ji} a_j$$

$$\begin{aligned}
\rho(g) : b_i \mapsto & \sum_{j=1}^{n} P_{ji} \rho(g)(a_j) \\
&= \sum_{j=1}^{n} P_{ji} \left(\sum_{k=1}^{n} M_{kj} a_k \right) \\
&= \sum_{j,k,l} P_{ji} M_{kj} (P^{-1})_{lk} b_l \\
&= \sum_{l} (P^{-1} M P)_{li} b_l
\end{aligned}$$

so $N = P^{-1} M P$. So $\forall\, g \in G, \rho_2(g) = P^{-1} \rho_1(g) P$. Hence, $\rho_2 = c_P \circ \rho_1$. $\square$

Conversely, suppose ρ_1 and ρ_2 are equivalent matrix representations of G. Let P be the matrix such that $\rho_2 = c_P \circ \rho_1$. Let V be the vector space $\mathbb{C}^n$, equipped with the standard basis. Then we can think of ρ_1 as a representation

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

Now define a new basis of V consisting of the vectors

$$b_k = \begin{pmatrix} P_{1k} \\ \vdots \\ P_{nk} \end{pmatrix}$$

i.e. the columns of P. This is a basis, because P is invertible.

Claim 1.2.3. *When we write the representation*

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

as matrices wrt the basis $\{b_1, \ldots, b_n\}$, we get the matrix representation ρ_2.

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

1.3 Representations from combinatorics and geometry

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. $\square$

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

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

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

For some groups, we can construct representations using geometry.

Example 1.3.3. 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

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

i.e. both ways round the square

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

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 though 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 vector spaces of the same dimension, and let*

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

be two representations of G. Let $\mathcal{A} = \{a_1, \dots, a_n\}$ be a basis for V, and let $\mathcal{B} = \{b_1, \dots, b_n\}$ 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 $\iff$ $\rho_1^{\mathcal{A}}$ and $\rho_2^{\mathcal{B}}$ are equivalent.

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

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

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

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

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. 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

$$\rho_2^B = c_P \circ \rho_1^A$$

Let $f : V \to W$ be the linear map represented by the matrix P^{-1} with respect to bases $\mathcal{A}$ and $\mathcal{B}$, i.e.

$$f(a_k) = \sum_{i=1}^{n} (P^{-1})_{ik} b_i$$

Then f is an isomorphism of vector spaces (as P^{-1} is invertible), but we have to check that f is G-linear. Pick $g \in G$, and let $\rho_1^{\mathcal{A}}(g) = M$ and $\rho_2^{\mathcal{B}}(g) = N$, so $N = P^{-1}MP$. Then

$$\begin{aligned} f(\rho_1(g)(a_k)) &= f(\sum_j M_{jk} a_j) && = \sum_j M_{jk} f(a_j) = \sum_{j,l} M_{jk} P^{-1}_{lj} b_l \\ &= \sum_l (P^{-1}M)_{lk} b_l && = \sum_l (NP^{-1})_{lk} b_l = \sum_{j,l} N_{lj} P^{-1}_{jk} b_l \\ &= \rho_2(g)(f(a_k)) \end{aligned}$$

so f is indeed G-linear. $\square$

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

$$\rho_{reg}(\tau) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \text{(this transposes the two basis elements)}$$

and $\rho_{reg}(e) = I_2$. Define a 1-dimensional representation

$$\rho_1 : C_2 \to GL_1(\mathbb{C}) = \mathbb{C}^* \;\; (= \mathbb{C} \backslash \{0\})$$

by

$$\rho_1 : \tau \mapsto -1$$

(this is a representation, as $(\rho_1(\tau))^2 = (-1)^2 = 1$)).

Let $f : \mathbb{C}^2 \to \mathbb{C}$ be the linear map represented by the matrix $(1, -1)$ in the standard basis. Then for any vector $\mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \in \mathbb{C}^2$,

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

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 $\{b_1, \ldots, b_n\}$, 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.

We can generalise this. 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.

Proposition 1.4.8. *If f is a G-linear map between the two representations*

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

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

Proof. See Problem Sheet 2. □

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

$$\begin{aligned} \iota_V &: V \to V \oplus W \\ \iota_V &: x \mapsto (x, 0) \end{aligned}$$

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, suppose $\rho : G \to GL(V)$ is a representation and $W \subset V$ and $U \subset V$ are subrepresentations such that

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

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

Then 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 $y \in U$, i.e. the map

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

is an isomorphism of vector spaces. But f is also G-linear, because

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

So f is an isomorphism of representations.

This raises the following:

Question 1.5.2. Suppose $\rho : G \to GL(V)$ is a representation, and suppose $W \subset V$ is a subrepresentation. Can we find another subrepresentation $U \subset V$ such that $V = W \oplus U$?

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 1.5.3. 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 1.5.4. *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 f be the map

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

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

Corollary 1.5.5. *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 1.5.6 (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 Corollory 1.5.5, 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. $\square$

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

Definition 1.5.7. 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 1.5.8. *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 1.5.9. 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 Problem Sheet 1). 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 1.5.10. 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 1.5.3. 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 1.5.11. *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. $\square$

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 1.5.12. 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 1.5.9.

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. $f = \lambda \mathbf{1}_V$. $\square$

[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, $\rho(g) = \lambda_h \mathbf{1}_V$ 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 1.5.11. □

As remarked before, this is not true for non-abelian groups. However, there are some weaker statements that we can prove:

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 $\rho(g)$.

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 $i \neq j$.*

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 $k_1 \times \ldots \times k_r (= |G|)$ 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 1.6.6. *All these irreps are distinct.*

Example 1.6.7. 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.

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 $C_2 \times C_2$

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

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. We can get a bit of information out of our results on abelian groups.

Definition 1.6.9. The **centre** of a group is the subgroup $Z \subset G$ of all elements $z \in G$ such that

$$zg = gz \quad \forall\, g \in G$$

Clearly Z is always abelian.

Proposition 1.6.10. *Let $\rho : G \to GL(V)$ be an irrep of G, and let $z \in Z \subset G$. Then there exists $\lambda_z \in \mathbb{C}$ such that*

$$\rho(z) = \lambda_z \mathbf{1}_V$$

Proof. Consider the linear map

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

It's G-linear, because $\rho(gz) = \rho(zg)$ for all $g \in G$. So by Schur's Lemma, $\rho(z) = \lambda_z \mathbf{1}_V$ for some $\lambda_z \in \mathbb{C}$. □

If we restrict ρ to Z, we get a representation

$$\rho_Z : Z \to GL(V)$$

Every $z \in Z$ is going to $\lambda_Z \mathbf{1}_V$ for some $\lambda_Z \in \mathbb{C}$, i.e. ρ_Z is a direct sum of 1-dimensional representations ($\dim V$ of them), each of which is isomorphic to the 1-dimensional representation

$$\begin{aligned} \tilde{\rho} &: Z \to GL_1(\mathbb{C}) \\ \tilde{\rho} &: z \mapsto \lambda_z \end{aligned}$$

Since Z is abelian, $Z = C_{k_1} \times \ldots \times C_{k_r}$ and $\tilde{\rho}$ is one of the irreps $\rho_{q_1,\ldots,q_r}$.

Example 1.6.11. Let $G = D_4 = \langle \sigma, \tau \,|\, \sigma^4 = \tau^2 = e, \tau\sigma\tau = \sigma^{-1} \rangle$. The centre of G is $Z = \{e, z\}$ where $z = \sigma^2$ (rotation by π), so $Z \cong C_2$. Let $\rho : D_4 \to GL(V)$ be a representation of dimension n, then

$$\rho_Z : Z \to GL(V)$$

is a direct sum of n copies of either ρ_0 or ρ_1. So either $\rho(z) = \mathbf{1}_V$, or $\rho(z) = -\mathbf{1}_V$.

In general, if we want to list all the irreps of a group G, we can group them together according to the corresponding irrep of the centre.

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

$$\begin{aligned} f_{i,j} : V &\to W \\ a_k &\mapsto \begin{cases} b_j & \text{if } k = i \\ 0 & \text{if } k \neq i \end{cases} \end{aligned}$$

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

The set $\{f_{ij} \,|\, 1 \leq i \leq n, 1 \leq j \leq m\}$ 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_{ij} 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

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

Now suppose that we have representations

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

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 subset**

$$V^G \subset V$$

to be the set

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

Claim 1.7.6. *V^G is a subspace of V.*

It's obvious that V^G is also a subrepresentation, so we can call it the **invariant subrepresentation**. It's isomorphic to a trivial representation.

Proposition 1.7.7. *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 1.7.8. 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 1.7.9. *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 $h \in G$,

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

□

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 1.5.8) 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.

Proof. Recall that we have inclusion and projection maps

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

(i) Define

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

by

$$P(f) = (\pi_U \circ f, \pi_W \circ f)$$

Claim 1.8.2. *P is a linear map.*

Now let's show that P is an injection. Suppose $P(f) = 0$. Then for all $x \in V$,

$$P(f)(x) = (\pi_U(f(x)), \pi_W(f(x))) = (0, 0)$$

i.e.

$$\pi_U(f(x)) = \pi_W(f(x)) = 0$$

This means that $f(x) = (0, 0) \in U \oplus W$. Since this is true for all $x \in V$, f must the zero map in $\mathrm{Hom}(V, U \oplus W)$, so P is indeed an injection. But

$$\begin{aligned}
\dim(\mathrm{Hom}(V, U \oplus W)) &= (\dim V)(\dim(U \oplus W)) \\
&= (\dim V)(\dim U + \dim W) \\
&= (\dim V)(\dim U) + (\dim V)(\dim W) \\
&= \dim(\mathrm{Hom}(V, U)) + \dim(\mathrm{Hom}(V, W)) \\
&= \dim\left(\mathrm{Hom}(V, U) \oplus \mathrm{Hom}(V, W)\right)
\end{aligned}$$

So P must be 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

$$I(f) = (f \circ \iota_U, f \circ \iota_W)$$

Then use very similar arguments to those in (i). □

Claim 1.8.3. *Let $\rho_V : G \to GL(V)$ and $\rho_W : G \to GL(W)$ be representations. An isomorphism*

$$f : V \to W$$

restricts to give an isomorphism

$$f : V^G \to W^G$$

between the invariant subrepresentations.

Corollary 1.8.4. *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) $\mathrm{Hom}_G(U \oplus W, V) = \mathrm{Hom}_G(U, V) \oplus \mathrm{Hom}_G(W, V)$

Now 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 1.8.5. *Let V and W be irreps of G. Then*

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

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

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

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

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

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

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. Then

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

by Corollary 1.8.4, so

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

By Proposition 1.8.5, this equals the number of irreps in $\{U_1, \dots, U_s\}$ that are isomorphic to W. By the same argument, $\dim \operatorname{Hom}_G(W, V)$ is also the number of irreps in $\{\hat{U}_1, \dots, \hat{U}_r\}$ that are isomorphic to W. So for any irrep W, the two decompositions contain the same number of factors isomorphic to W. □

Notice we could have used $\dim \operatorname{Hom}_G(V, W)$ instead of $\dim \operatorname{Hom}_G(W, V)$, it also counts the number of copies of W occuring in the decomposition of V.

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

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

We claimed that this representation was very important. Here's why:

Theorem 1.8.7. *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 1.8.8. *Any group G has only finitely many irreducible representations (up to isomorphism).*

Proof. Every irrep occurs in the decomposition of V_{reg}, 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 Theorem 1.8.7 says that V_{reg} decomposes as

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

where

$$d_i = \dim U_i$$

The proof of Theorem 1.8.7 follows easily from the following:

Lemma 1.8.9. *For any representation W of G, we have a natural isomorphism of vector spaces*

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

Proof. Define a function

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

by $x \mapsto T_x$, where T_x is the linear map defined by

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

We need to check that T_x is G-linear. For all $h \in G$ we have

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

So $T_x \circ \rho_{reg}(h) = \rho_W(h) \circ T_x$, i.e. T_x is indeed G-linear, and T really does define a map from W to $\mathrm{Hom}_G(V_{reg}, W)$. We claim that T is in fact a linear map. Let's check:

$$\begin{aligned} T_{x+y} &: b_g \mapsto \rho_W(g)(x+y) = \rho_W(g)(x) + \rho_W(g)(y) \\ T_x + T_y &: b_g \mapsto T_x(b_g) + T_y(b_g) = \rho_W(g)(x) + \rho_W(g)(y) \end{aligned}$$

so $T_{x+y} = T_x + T_y$. Also

$$T_{\lambda x} : b_g \mapsto \rho_W(g)(\lambda x) = \lambda \rho_W(g)(x) = (\lambda T_x)(b_g)$$

so $T_{\lambda x} = \lambda T_x$. So T is indeed linear.

Now let's find an inverse to T. Let

$$\begin{aligned} T' : &\mathrm{Hom}_G(V_{reg}, W) \to W \\ &f \mapsto f(b_e) \end{aligned}$$

Then

$$(T' \circ T) : x \mapsto T'(T_x) = T_x(b_e) = \rho_W(e)(x) = x$$

so $T' \circ T = \mathbf{1}_W$. Also

$$T \circ T' : f \to T_{T'(f)} = T_{f(b_e)}$$

and

$$T_{f(b_e)} : b_g \mapsto \rho_W(g)(f(b_e)) = f(\rho_{reg}(g)(b_e)) = f(b_g)$$

So the linear maps $T_{f(b_e)}$ and f agree on a basis, so they are the same map. So

$$T \circ T' = \mathbf{1}_{\mathrm{Hom}_G(V_{reg}, W)}$$

Hence T is an isomorphism with inverse T'. □

Proof of Theorem 1.8.7. 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. Then using the same argument that we used in the proof of Theorem 1.8.6, we see that $\dim \mathrm{Hom}_G(V_{reg}, W)$ equals the number of U_i that are isomorphic to W. But by Lemma 1.8.9,

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

□

Corollary 1.8.10. *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 1.8.7,

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

Now take dimensions of each side. □

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 1.8.11. Let $G = S_3 = \langle \sigma, \tau \mid \sigma^3 = \tau^2 = e, \tau\sigma\tau = \sigma^{-1} \rangle$. Let's find all the irreps of G. Let U_1 be the 1-dimensional trivial representation. Let U_2 be the 1-dimensional representation

$$\begin{aligned} \rho_2 : &\sigma \mapsto 1 \\ &\tau \mapsto -1 \end{aligned}$$

(this is called the **sign representation**). Suppose there are r irreps of G, with dimensions $d_1, d_2, \ldots, d_r$. We know

$$d_1^2 + d_2^2 + \ldots + d_r^2 = 6$$

and we have $d_1 = d_2 = 1$, so $d_3^2 + \ldots + d_r^2 = 4$. So there are only two possibilities, either

(i) $r = 6$ and $d_3 = d_4 = d_5 = d_6 = 1$, or

(ii) $r = 3$ and $d_3 = 2$

But we know that S_3 has at least one 2-dimensional irrep (we found it in Example 1.5.9), so (ii) is true and S_3 has 3 irreps of dimensions 1, 1, and 2. The 2-dimensional irrep arises geometrically from the action of S_3 on a triangle. (See Problem Sheet 1).

The sign representation exists for any S_n (not just S_3). It's the 1-dimensional representation

$$\rho_{sgn} : S_n \to GL_1(\mathbb{C})$$

$$\rho_{sgn}(g) = \begin{cases} 1 & g \in A_n \\ -1 & g \notin A_n \end{cases}$$

(recall that A_n is the subgroup of even permutations). The sign representation and the trivial representation are the only 1-dimensional representations of S_n (see Problem Sheet 3).

Example 1.8.12. 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 $d_1 = d_2 = 1$, and $d_i > 1$ 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 1.8.13. 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 Problem Sheet 2 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 1.3.3 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 $i, j \in \{0, 1\}$.

Recall that the centre of D_4 is $\{1, \sigma^2\}$. In $U_1, \ldots, U_4$ we have σ^2 acting as 1, and in U_5 we have σ^2 acting as $-\mathbf{1}_{U_5}$. (c.f. Example 1.6.11).

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 represntation, 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 Sheet 1)

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

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 1.8.4, this implies $V^* = U^* \oplus W^*$, so V^* is not irreducible. By the same argument, if V^* is not irreducible then neither is $(V^*)^* = V$. $\square$

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

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

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 mn rows, and to specify a row we have to give a pair of numbers (j, s), where $1 \leq j \leq n$ and

$1 \leq s \leq m$. Similiarly to specify a column we also have to give another pair of numbers (i, t). Fortunately we won't have to use it 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 $\{f_{it} \mid 1 \leq i \leq n, 1 \leq t \leq m\}$ where

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

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

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

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 $\{f_{it}\}$. 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,

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

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

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

and

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

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

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

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

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 1.9.6. 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, this is obvious for dimension reasons. However if V is 1-dimensional, then $V \otimes W$ is irreducible iff V is irreducible (see Problem Sheet 5). Therefore in the above example the 2-dimensional representation $V \otimes W$ is irreducible, so is in fact 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

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

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

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

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 $g \in G$*

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

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 $\lambda = 1$. $\square$

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

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

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

i.e. $\chi_{V\otimes W}(g) = \chi_V(g)\chi_W(g)$.

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

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 1.8.7

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

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 ρ_{reg} 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 Sheet 6).

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 dimension of $\mathbb{C}^G$ is $|G|$, an obvious basis is given by the set of functions

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

defined by

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

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

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

If we view this vector space as $\mathbb{C}^G$ (i.e. 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

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

These three properties are the definition of a Hermitian inner product.

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*

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

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, a quick lemma:

Lemma 2.2.3. *Let V be a vector space, with subspace $U \subset V$, and let $\pi : V \to V$ a projection onto U. Then*

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

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 $\mathrm{Tr}(\pi) = \mathrm{Tr}(\mathbf{1}_U) = \dim U$. $\square$

The following is one of the more conceptually-difficult proofs in the course.

Proof of Theorem 2.2.2. Recall that

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

as the invariant subrepresentation, and that we have a projection

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

(see Proposition 1.7.9). We claim that

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

By Lemma 2.2.3, this would prove the theorem. Let's calculate $\mathrm{Tr}(\Psi)$. Pick bases $\{a_1, \ldots, a_n\}$ for V and $\{b_1, \ldots, b_m\}$ for W. Recall that $\mathrm{Hom}(V, W)$ has an associated basis

$$\{f_{ij} \mid 1 \le i \le n, 1 \le j \le m\}$$

where

$$\begin{aligned} f_{ij} : & a_i \mapsto b_j \\ & a_{\neq i} \mapsto 0 \end{aligned}$$

Let $\widetilde{\rho_V}, \widetilde{\rho_W}$ be the matrix representations we get by writing ρ_V and ρ_W in the given bases. From Proposition 1.9.5 we know that

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

i.e. if we write $\rho_{\mathrm{Hom}(V,W)}$ in the basis $\{f_{ij}\}$ then we get the tensor product of the matrix representations $\widetilde{\rho_{V^*}}$ and $\widetilde{\rho_W}$. So

$$\begin{aligned}
\rho_{\mathrm{Hom}(V,W)}(g)(f_{ij}) &= \rho_W(g) \circ f_{ij} \circ \rho_V(g^{-1}) \\
&= \sum_{\substack{k\in[1,n] \\ t\in[1,m]}} \widetilde{\rho_V}(g^{-1})_{ik} \widetilde{\rho_W}(g)_{tj} f_{kt}
\end{aligned}$$

Then

$$\begin{aligned}
\Psi(f_{ij}) &= \frac{1}{|G|} \sum_{g\in G} \rho_{\mathrm{Hom}(V,W)}(g)(f) \\
&= \frac{1}{|G|} \sum_{g\in G} \sum_{\substack{k\in[1,n] \\ t\in[1,m]}} \widetilde{\rho_V}(g^{-1})_{ik} \widetilde{\rho_W}(g)_{tj} f_{kt}
\end{aligned}$$

So if we wrote Ψ down as a matrix using the $\{f_{ij}\}$ basis, the diagonal entries would be

$$\frac{1}{|G|} \sum_{g\in G} \widetilde{\rho_V}(g^{-1})_{ii} \widetilde{\rho_W}(g)_{jj}$$

Therefore

$$\begin{aligned}
\mathrm{Tr}(\Psi) &= \sum_{\substack{i\in[1,n] \\ j\in[1,m]}} \frac{1}{|G|} \sum_{g\in G} \widetilde{\rho_V}(g^{-1})_{ii} \widetilde{\rho_W}(g)_{jj} \\
&= \frac{1}{|G|} \sum_{g\in G} \left(\sum_{i=1}^{n} \widetilde{\rho_V}(g^{-1})_{ii} \right) \left(\sum_{j=1}^{m} \widetilde{\rho_W}(g)_{jj} \right) \\
&= \frac{1}{|G|} \sum_{g\in G} \chi_V(g^{-1}) \chi_W(g) \\
&= \frac{1}{|G|} \sum_{g\in G} \chi_W(g) \overline{\chi_V}(g) \quad \text{(by Proposition 2.1.5(ii))} \\
&= \langle \chi_W | \chi_V \rangle
\end{aligned}$$

□

Corollary 2.2.4. *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

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

by Proposition 1.8.5. □

So the irreducible characters form a set of orthonormal vectors in $\mathbb{C}^G$. In particular, they're linearly independent. We know that any character can be written as a linear combination

$$\chi = m_1 \chi_1 + \ldots + m_r \chi_r$$

of the irreducible characters, because any representation can be decomposed into irreps. We can calculate the coefficients by calculating the inner product

$$\langle \chi | \chi_i \rangle = m_i$$

(i.e. we project the vector χ onto each of the orthonormal vectors χ_i). This is a translation of the statement that we found in Section 1, that

$$\dim \operatorname{Hom}_G(V, U_i) = \begin{matrix} \text{number of copies of the irrep } U_i \\ \text{in the decomposition of } V \end{matrix}$$

It's much easier using characters!

Example 2.2.5. 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_1 and ρ_2.

Corollary 2.2.6. *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 2.2.4. So $\langle \chi | \chi \rangle = 1$ iff exactly one of the $m_i = 1$ and the rest are 0. $\square$

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 2.2.7. Let $G = D_5 = \langle \sigma, \tau \mid \sigma^5 = \tau^2 = e, \sigma\tau = \tau\sigma^{-1}\rangle$. G is the symmetry group of a pentagon, it has 4 rotations $\sigma, \sigma^2, \sigma^3, \sigma^4$ and 5 reflections $\tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau, \sigma^4\tau$. We have

$$\tau\sigma\tau^{-1} = \sigma^2$$

and

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

Also all reflections are conjugate, which can be seen by repeatedly applying the relation

$$\sigma^k\tau\sigma^{-k} = \sigma^{k-2}\tau\sigma^{1-k}$$

Here is a 2-dimensional representation of G:

$$\rho_3(\sigma) = \begin{pmatrix}\alpha & 0\\ 0 & \alpha^{-1}\end{pmatrix}, \quad \rho(\tau) = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$$

where $\alpha = e^{\frac{2\pi i}{5}}$. Here's another one:

$$\rho_4(\sigma) = \begin{pmatrix}\alpha^2 & 0\\ 0 & \alpha^{-2}\end{pmatrix}, \quad \rho(\tau) = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$$

Let's write down the values of their characters on the four conjugacy classes in G.

$[g]$	$[e]$	$[\sigma]$	$[\sigma^2]$	$[\tau]$
$\|[g]\|$	1	2	2	5
χ_3	2	$\alpha+\alpha^4$	$\alpha^2+\alpha^3$	0
χ_4	2	$\alpha^2+\alpha^3$	$\alpha+\alpha^4$	0

Using $\overline{\alpha} = \alpha^4, \overline{\alpha^2} = \alpha^3$ and $1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4 = 0$, we calculate:

$$\begin{aligned}
\langle \chi_3 | \chi_3 \rangle &= \frac{1}{10}\left(2^2 + 2(\alpha + \alpha^4)(\alpha^4 + \alpha) + 2(\alpha^2 + \alpha^3)(\alpha^3 + \alpha^2) + 0\right) \\
&= \frac{1}{5}(2 + \alpha^2 + 2 + \alpha^3 + \alpha^4 + 2 + \alpha) \\
&= 1 \\
\langle \chi_4 | \chi_4 \rangle &= \frac{1}{10}\left(2^2 + 2(\alpha^2 + \alpha^3)^2 + 2(\alpha + \alpha^4)^2\right) \\
&= 1
\end{aligned}$$

So both ρ_3 and ρ_4 are irreducible. Since $\chi_3 \neq \chi_4$, ρ_3, ρ_4 aren't isomorphic. Let's check:

$$\begin{aligned}
\langle \chi_3 | \chi_4 \rangle &= \frac{1}{10}\left(2^2 + 2(\alpha + \alpha^4)(\alpha^2 + \alpha^3) + 2(\alpha^2 + \alpha^3)(\alpha + \alpha^4)\right) \\
&= \frac{1}{5}(2 + \alpha^3 + \alpha^4 + \alpha + \alpha^2 + \alpha^3 + \alpha + \alpha^4 + \alpha^2) \\
&= 0
\end{aligned}$$

These are the only two irreps of D_5 of dimension > 1 (see Problem Sheet 5).

The next result is really just another corollary of Theorem 2.2.2:

Theorem 2.2.8. *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 are isomorphic. $\square$

Example 2.2.9. Let $G = D_5$ again. Let U_3, U_4 be the 2-dimensional irreps from Example 2.2.7. Let U_1 be the 1-dimensional trivial representation, and let U_2 be the 1-dimensional representation

$$\rho_2(\sigma) = 1, \quad \rho_2(\tau) = -1$$

The characters of these irreps are:

$[g]$	$[e]$	$[\sigma]$	$[\sigma^2]$	$[\tau]$
$\|[g]\|$	1	2	2	5
χ_1	1	1	1	1
χ_2	1	1	1	-1
χ_3	2	$\alpha + \alpha^4$	$\alpha^2 + \alpha^3$	0
χ_4	2	$\alpha^2 + \alpha^3$	$\alpha + \alpha^4$	0

This is a complete list of the irreducible characters. It's called a **character table**.

Let $V = U_3 \oplus U_4$ and $W = U_3 \otimes U_4$. By Proposition 2.1.7,

$$\begin{aligned} \chi_V &= \chi_3 + \chi_4 \\ \chi_W &= \chi_3\chi_4 \end{aligned}$$

So $\chi_V(e) = 4 = \chi_W(e)$, and $\chi_V(\tau) = 0 = \chi_W(\tau)$. Also,

$$\begin{aligned} \chi_V(\sigma) &= (\alpha + \alpha^4) + (\alpha^2 + \alpha^3) \\ &= (\alpha + \alpha^4)(\alpha^2 + \alpha^3) \\ &= \chi_W(\sigma) \end{aligned}$$

and

$$\begin{aligned}\chi_V(\sigma^2) &= (\alpha^2+\alpha^3)+(\alpha+\alpha^4)\\ &= (\alpha^2+\alpha^3)(\alpha+\alpha^4)\\ &= \chi_W(\sigma^2)\end{aligned}$$

So $\chi_V = \chi_W$, and hence $V = U_3 \oplus U_4$ is isomorphic to $W = U_3 \otimes U_4$.

Now consider $U_3 \otimes U_3$. It has character

$$\begin{aligned}\chi_3^2 \colon\ & e \mapsto 4\\ & \sigma \mapsto (\alpha+\alpha^4)^2 = 2+\alpha^2+\alpha^3\\ & \sigma^2 \mapsto (\alpha^2+\alpha^3)^2 = 2+\alpha+\alpha^4\\ & \tau \mapsto 0\end{aligned}$$

Let's write this as a linear combination of the irreducible characters. In general we can find the coefficients using the inner product, but in this example it's easier to just spot the answer. It is

$$\chi_3^2 = \chi_1 + \chi_2 + \chi_4$$

Hence $U_3 \otimes U_3$ is isomorphic to $U_1 \oplus U_2 \oplus U_4$. And similarly $U_4 \otimes U_4$ is isomorphic to $U_1 \oplus U_2 \oplus U_3$.

Example 2.2.10. Let $G = D_5$ (as in the previous two examples). Suppose that we'd found the irreps U_1, U_2 and U_3, but we hadn't found U_4. We'd know the following part of the character table:

$[g]$	$[e]$	$[\sigma]$	$[\sigma^2]$	$[\tau]$
$\lvert[g]\rvert$	1	2	2	5
χ_1	1	1	1	1
χ_2	1	1	1	-1
χ_3	2	$\alpha+\alpha^4$	$\alpha^2+\alpha^3$	0
χ_4	2	?	?	?

(where α is a primitive 5th root of unity). Corollary 2.2.4 lets us deduce the unknown values, without finding the representation U_4. Let the unknown values be

$$\begin{array}{c|cccc} \chi_4 & 2 & x & y & z \end{array}$$

Then

$$\begin{aligned}
\langle \chi_4 | \chi_1 \rangle &= 0 = \frac{1}{10}(1 \times 2 \times 1 + 2x + 2y + 5z) \\
\langle \chi_4 | \chi_2 \rangle &= 0 = \frac{1}{10}(2 + 2x + 2y - 5z) \\
\langle \chi_4 | \chi_3 \rangle &= 0 = \frac{1}{10}(4 + 2x(\alpha + \alpha^4) + 2y(\alpha^2 + \alpha^3)) \\
\langle \chi_4 | \chi_4 \rangle &= 1 = \frac{1}{10}(4 + 2|x|^2 + 2|y|^2 + 5|z|^2)
\end{aligned}$$

The first two equations tell us that $z = 0$ and $y = -1 - x$. The third equation tells us

$$\begin{aligned}
2 + x(\alpha + \alpha^4) - (1 + x)(\alpha^2 + \alpha^3) = 0 \\
\Rightarrow \quad x = \frac{\alpha^2 + \alpha^3 - 2}{\alpha + \alpha^4 - \alpha^2 - \alpha^3}
\end{aligned}$$

and this is equal to $\alpha^2 + \alpha^3$ (check by substitution). Then

$$y = -1 - \alpha^2 - \alpha^3 = \alpha + \alpha^4$$

2.3 Class functions

Definition 2.3.1. A **class function** for a group G is a function

$$\xi \colon G \to \mathbb{C}$$

such that

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

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 $\dim(\mathbb{C}_{cl}^G)$ is the number of conjugacy classes in G.

Let $\chi_1, \ldots, \chi_r$ be the irreducible characters of G. Then each χ_i is a class function, and they are linearly independent (by Corollary 2.2.4). The maximum size of a linearly independent set in a vector space is the dimension of the vector space, so

$$r \leq \dim \mathbb{C}_{cl}^G$$

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've shown the inequality in one direction, the harder part is to show that

$$\#\{\text{irreps}\} \geq \#\{\text{conjugacy classes}\}$$

Before we start the proof, we need a lemma:

Lemma 2.3.4. *Let $\rho_i \colon G \to GL(U_i)$ be an irrep of G. Fix a conjugacy class $[g]$ in G. Consider the linear map*

$$D_i^{[g]} \colon U_i \to U_i$$
$$D_i^{[g]} = \sum_{h \in [g]} \rho_i(h)$$

Then

$$D_i^{[g]} = \lambda_i^{[g]} \mathbf{1}_{U_i}$$

for some $\lambda_i^{[g]} \in \mathbb{C}$.

Proof. We claim that $D_i^{[g]}$ is actually G-linear. If we can show this, then since U_i is an irrep, it follows from Schur's Lemma that $D_i^{[g]}$ must be a scalar multiple of $\mathbf{1}_{U_i}$. So fix $\hat{g} \in G$ and check

$$\begin{aligned} D_i^{[g]} \circ \rho_i(\hat{g}) &= \sum_{h \in [g]} \rho_i(h) \circ \rho_i(\hat{g}) \\ &= \sum_{h \in [g]} \rho_i(h\hat{g}) \\ &= \sum_{h \in [g]} \rho_i(\hat{g}h) \quad \text{(relabelling } h \mapsto \hat{g}g\hat{g}^{-1}\text{, which is a permutation of } [g]) \\ &= \rho_i(\hat{g}) \circ D_i^{[g]} \end{aligned}$$

□

We can say more: if we take traces of the equation

$$D_i^{[g]} = \lambda_i^{[g]} \mathbf{1}_{U_i}$$

we get

$$\sum_{h \in [g]} \chi_i(h) = |[g]| \chi_i(g) = \lambda_i^{[g]} d_i$$

where χ_i is the character of U_i, and d_i is its dimension. So

$$\lambda_i^{[g]} = \chi_i(g) \frac{|[g]|}{d_i}$$

Proof of Theorem 2.3.3. Recall that we can identify $\mathbb{C}^G \cong V_{reg}$ by identifying each δ_g with a basis vector $b_g \in V_{reg}$. So we can view $\mathbb{C}^G_{cl}$ as a subspace of V_{reg}. Also recall (Lemma 1.8.9) that for any representation W of G we have an isomorphism of vector spaces

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

defined by $T \colon x \mapsto T_x$, where

$$T_x \colon b_g \mapsto \rho_W(g)(x)$$

If we set $W = V_{reg}$, we get an isomorphism

$$\begin{aligned} T\colon V_{reg} &\to \mathrm{Hom}_G(V_{reg}, V_{reg}) \\ b_h &\mapsto T_h (:= T_{b_h}) \end{aligned}$$

where

$$T_h\colon b_g \mapsto \rho_{reg}(g)(b_h) = b_{gh}$$

i.e. T_h is the linear map from $V_{reg} \to V_{reg}$ induced by letting h act on G by right multiplication. So now we have two isomorphisms

$$\mathbb{C}^G \cong V_{reg} \overset{T}{\cong} \mathrm{Hom}_G(V_{reg}, V_{reg})$$

and hence we can view $\mathbb{C}^G_{cl}$ as a subspace of $\mathrm{Hom}_G(V_{reg}, V_{reg})$. Consider the basis element

$$\delta_g = \sum_{h \in [g]} \delta_h \in \mathbb{C}^G_{cl}$$

We identify this with the vector $\sum_{h\in[g]} b_h \in V_{reg}$. So under T this maps to the G-linear map

$$T_{[g]} = \sum_{g \in [g]} T_h \in \mathrm{Hom}_G(V_{reg}, V_{reg})$$

The effect of this G-linear map is

$$\begin{aligned} T_{[g]}\colon b_{\tilde{g}} \mapsto & \sum_{h\in[g]} T_h(b_{\tilde{g}}) \\ &= \sum_{h\in[g]} b_{\tilde{g}h} \\ &= \sum_{h\in[g]} b_{h\tilde{g}} \quad (\text{by relabelling } h \mapsto \tilde{g}^{-1}h\tilde{g}) \\ &= \sum_{h\in[g]} \rho_{reg}(h)(b_{\tilde{g}}) \end{aligned}$$

So we have a linear injection

$$\mathbb{C}^G_{cl} \hookrightarrow \mathrm{Hom}_G(V_{reg}, V_{reg})$$

which on the basis elements is given by

$$\delta_{[g]} \mapsto \sum_{h\in[g]} \rho_{reg}(h)$$

Now recall that V_{reg} decomposes into irreps

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

where $\{U_i\}$ are all the irreps of G and d_i are their dimensions. For each $i \in [1, r]$, define $\theta_i \in \mathrm{Hom}_G(V_{reg}, V_{reg})$ to be the composition

$$V_{reg} \xrightarrow{\pi} U_i^{\oplus d_i} \xrightarrow{\iota} V_{reg}$$

Define $\Theta \subset \mathrm{Hom}_G(V_{reg}, V_{reg})$ to be the subspace spanned by $\theta_1, \ldots, \theta_r$. Since the θ_i are obviously linearly independent, they form a basis for Θ, so $\dim \Theta = r$, the number of irreps. We claim that when we map $\mathbb{C}_{cl}^G$ into $\mathrm{Hom}_G(V_{reg}, V_{reg})$ (using T) the image actually lies inside the subspace Θ. This would prove the theorem, because it implies that

$$\#\{\text{conjugacy classes}\} = \dim \mathbb{C}_{cl}^G \leq \dim \Theta = \#\{\text{irreps}\}$$

It's sufficient to check the claim on the basis $\{\delta_{[g]}\}$ for $\mathbb{C}_{cl}^G$. We know that

$$\delta_{[g]} \mapsto \sum_{h\in[g]} \rho_{reg}(h) \in \mathrm{Hom}_G(V_{reg}, V_{reg})$$

We also know that $V_{reg} \cong U_1^{\oplus d_1} \oplus \ldots \oplus U_r^{\oplus d_r}$. The map $\rho_{reg}(h)$ acts on this decomposition as a 'block-diagonal' map, i.e. it acts as the direct sum of the maps

$$\rho_i(h) \colon U_i \to U_i$$

Therefore, $\delta_{[g]}$ acts as the direct sum of the maps

$$\sum_{h\in[g]} \rho_i(h) = D_i^{[g]} \colon U_i \to U_i$$

But by Lemma 2.3.4,

$$D_i^{[g]} = \lambda_i^{[g]} \mathbf{1}_{U_i}$$

So $\delta_{[g]}$ acts on $U_i^{\oplus d_i}$ as $\lambda_i^{[g]} \mathbf{1}_{U_i^{\oplus d_i}}$ and it acts on the whole of V_{reg} as the map

$$\sum_{i=1}^{r} \lambda_i^{[g]} \theta_i$$

So $\delta_{[g]}$ lands in the span of the θ_i, as claimed. $\square$

This was probably the hardest proof in the course. In Section 3 we'll introduce the technology of **group algebras**, which will allow us to present this proof much more concisely.

Example 2.3.5. 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 1.8.12.

Example 2.3.6. 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. Normally in mathematics when we show that two sets are the same size we do it by constructing a natural bijection between them. But in this case there is no natural bijection! I.e. there is no (sensible) way to pair up irreps with conjugacy classes, even though there's the same number of each.

Corollary 2.3.7. *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 $r = \#\{\text{conjugacy classes}\} = \dim \mathbb{C}^G_{cl}$. □

2.4 More on character tables

We've met character tables already in Section 2.2, but let's give a formal definition:

Definition 2.4.1. 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 2.4.2. 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

In Corollary 2.3.7 we observed that the vector space $\mathbb{C}^G_{cl}$ has two natural bases, we have $\{\delta_{[g_j]}\}$ which is indexed by conjugacy classes, and $\{\chi_i\}$ which is indexed by irreps. To switch between these two bases we must express each χ_i in the basis $\{\delta_{[g_j]}\}$. This is easy, we have

$$\chi_i = \chi_i(g_1)\delta_{[g_1]} + \ldots + \chi_i(g_r)\delta_{[g_r]}$$

(since both sides give the same function $G \to \mathbb{C}$). These coefficients are the entries in C, i.e. C is the (transpose of the) change-of-basis matrix between the 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 to 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

$$
\langle \delta_{[g_i]} | \delta_{[g_i]} \rangle = \frac{|[g_i]|}{|G|}
$$

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 2.4.3. *Let $[g_i]$ and $[g_j]$ be two conjugacy classes in G. Then*

$$
\sum_{k=1}^{r} \overline{\chi_k}(g_i)\chi_k(g_j) = \begin{cases} \frac{|G|}{|[g_i]|} & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}
$$

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. $\square$

So 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:

$$\sum_{k=1}^{r} \overline{C_{ki}}C_{kj} = \begin{cases} \frac{|G|}{|[g_i]|} & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}$$

Both of them are really the statement that the modified character table B is unitary.

Example 2.4.4. Let's solve Example 2.2.10 again using column orthogonality. We have G such that $|G| = 10$ and a character table

	$[g_1]$	$[g_2]$	$[g_3]$	$[g_4]$
$\|[g]\|$	1	2	2	5
χ_1	1	1	1	1
χ_3	1	1	1	-1
χ_4	2	$\alpha + \alpha^4$	$\alpha^2 + \alpha^3$	0
χ_4	2	x	y	z

where $\alpha = e^{\frac{2\pi i}{5}}$, and we want to know x, y, z. The norm of the last column is $\frac{10}{5} = 2$ so $z = 0$. The inner product of the first two columns is

$$1 + 1 + 2(\alpha + \alpha^4) + 2x = 0$$

so $x = 1 - \alpha - \alpha^4 = \alpha^2 + \alpha^3$. The inner product of the first and third columns is

$$1 + 1 + 2(\alpha^2 + \alpha^3) + 2y = 0$$

so $y = \alpha + \alpha^4$.

The column orthogonality equations carry exactly the same information as the row orthogonality equations, but as this example shows, sometimes it's quicker to use one rather than the other (or we can use a mixture of both).

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 in the column orthogonality equations, the norm of the ith column is $|C_{g_i}|$. In particular this is always a positive integer.

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

$$\begin{aligned} m\colon \mathrm{Mat}_{n\times n}(\mathbb{C}) \times \mathrm{Mat}_{n\times n}(\mathbb{C}) &\to \mathrm{Mat}_{n\times n}(\mathbb{C}) \\ m\colon (M, N) &\mapsto MN \end{aligned}$$

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 $x^2 = 0$. Then A is an algebra.

(v) Let A be the 5-dimensional space with basis $\{1, x, y, xy, yx\}$. Define multiplication in the obvious way, and with

$$x^2 = y^2 = xyx = yxy = 0$$

Then A is an algebra.

(vi) Let V be a vector space, and let $A = \mathrm{Hom}(V, V)$. Multiplication is given by composition of maps. Then A is an algebra: associativity and unitality are obvious, and for bilinearity see Problem Sheet 4. If we pick a basis for V, then A becomes the algebra $\mathrm{Mat}_{n\times n}(\mathbb{C})$. In particular composition of maps corresponds to multiplication of matrices.

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

$$(\lambda_1 g_1 + \ldots + \lambda_t g_t)(\mu_1 g_1 + \ldots + \mu_t g_t) = \lambda_1\mu_1(g_1^2) + \ldots + \lambda_t\mu_1(g_t g_1) + \ldots$$
$$\ldots + \lambda_1\mu_t(g_1 g_t) + \ldots + \lambda_t\mu_t(g_t^2)$$
$$= \sum_k \left(\sum_{\substack{i,j \text{ such that} \\ g_i g_j = g_k}} \lambda_i \mu_j g_k \right)$$

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 $A = \mathbb{C}[C_2]$ 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

$$\begin{aligned} f(1_A) = f(e) = (1,1) &= 1_B \\ f(g)^2 = ((1,-1))^2 = (1,1) &= f(g^2) \end{aligned}$$

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!

Example 3.1.6. 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

$$\begin{aligned} & f(x)f(x) = f(x^2) = f(0) = 0 \\ \Rightarrow \quad & f(x) = 0 \end{aligned}$$

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

$$\mathbb{C}[G_1] \oplus \mathbb{C}[G_2] = \mathbb{C}[G_3]$$

So

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 with a bilinear map

$$\tilde{m}\colon A \times M \to M$$

such that

(i) $\tilde{m}(1_A, x) = x, \ \ \forall x \in M$

(ii) $\tilde{m}\left(a, \tilde{m}(b, x)\right) = \tilde{m}(ab, x), \ \ \forall a, b \in A, x \in M.$

We'll assume all our modules are finite-dimensional (as vector spaces) and we'll generally write ax when we mean $\tilde{m}(a, x)$. Then axiom (ii) says that

$$a(bx) = (ab)x$$

Modules can be viewed as generalisations of representations.

Proposition 3.2.2. *Let G be a group, and $A = \mathbb{C}[G]$ be the group algebra. Then an A-module is the same thing as a representation of G.*

Proof. Let M be an A-module. Then since $G \subset \mathbb{C}[G]$, we have for each $g \in G$ a linear map

$$\begin{aligned} \tilde{m}(g,-)\colon M &\to M \\ x &\mapsto gx \end{aligned}$$

If g and h are two elements of G, then

$$\begin{aligned} \tilde{m}(g,-) \circ \tilde{m}(h,-)\colon M &\to M \\ x &\mapsto g(hx) = (gh)x \end{aligned}$$

So $\tilde{m}(g,-) \circ \tilde{m}(h,-) = \tilde{m}(gh,-)$. In particular

$$\begin{aligned} \tilde{m}(g,-) \circ \tilde{m}(g^{-1},-) &= \tilde{m}(e,-) \\ &= \tilde{m}(1_A,-) \\ &= \mathbf{1}_M \end{aligned}$$

and similarly, $\tilde{m}(g^{-1},-) \circ \tilde{m}(g,-) = \mathbf{1}_M$. So each linear map $\tilde{m}(g,-)$ is invertible, so we can define

$$\begin{aligned} \rho\colon G &\to GL(M) \\ g &\mapsto \tilde{m}(g,-) \end{aligned}$$

and this is a representation.

Conversely, suppose we have a representation

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

So we have a map

$$\begin{aligned} \tilde{m}\colon G \times M &\to M \\ (g,x) &\mapsto \rho(g)(x) \end{aligned}$$

Extend this to a bilinear map

$$\tilde{m}\colon \mathbb{C}[G] \times M \to M$$

Then

$$\tilde{m}(1_{\mathbb{C}[G]}, x) = \tilde{m}(e,x) = \rho(e)(x) = x$$

for all $x \in M$. Also

$$\tilde{m}\left(g, \tilde{m}(h,x)\right) = \rho(g)\rho(h)(x) = \rho(gh)(x) = \tilde{m}(gh,x)$$

So by linearity,

$$\tilde{m}\left(a, \tilde{m}(b,x)\right) = \tilde{m}(ab,x)$$

for all $a, b \in \mathbb{C}[G]$. So M is a $\mathbb{C}[G]$-module. □

Also:

Claim 3.2.3. *An A-module structure on a vector space M is the same thing as an algebra homomorphism from A to* $\mathrm{Hom}(M,M)$*.*

So an A-module really is a 'representation' of an algebra.

Example 3.2.4. Let $A = \langle 1, x\rangle$ with $x^2 = 0$. Let M be a 1-dimensional A-module, this is the same thing as a homomorphism

$$A \to \mathrm{Hom}(M,M) = \mathbb{C}$$

So by Example 3.1.6, there is a unique such M, defined by $xy = 0$ for all $y \in M$.

Example 3.2.5. $A = \mathbb{C} \oplus \mathbb{C}$, and let M be a 1-dimensional module, i.e. a homomorphism

$$f\colon A \to \mathbb{C}$$

We must have

$$\begin{aligned}
\left(f(1,0)\right)^2 &= f\left((1,0)^2\right) = f(1,0) \\
\left(f(0,1)\right)^2 &= f\left((0,1)^2\right) = f(0,1) \\
f(1,0)f(0,1) &= f\left((1,0)(0,1)\right) = f(0,0) = 0 \\
f(0,1) + f(1,0) &= f\left((1,1)\right) = f(1_A) = 1
\end{aligned}$$

There are two solutions, we must set one of $f(1,0), f(0,1)$ to be 1, and the other to be 0. So A has two 1-dimensional modules.

Recall (Example 3.1.5) 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, ρ_0 and ρ_1. So this is consistent.

For any algebra A, there is a canonical A-module, namely A itself. If we set $M = A$ as vector spaces and let the module structure

$$\tilde{m}\colon A \times M \to M$$

be the algebra structure, then 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 of course the regular representation V_{reg}.

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.

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 representation notation, this says

$$f(\rho_M(g)(x)) = \rho_N(g)(f(x))$$

so f is G-linear.

Conversely, if $f\colon M \to N$ is G-linear then

$$f((\lambda_1 g_1 + \ldots + \lambda_t g_t)(x)) = (\lambda_1 g_1 + \ldots + \lambda_t g_t) f(x)$$

by linearity and G-linearity of f, so f is A-linear. $\square$

Definition 3.2.8. A **submodule** of an A-module M is a subspace $N \subseteq M$ such that

$$ax \in N, \quad \forall a \in A, x \in N$$

Definition 3.2.9. 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 structure does obey the axioms) and that these definitions agree with the definitions of subrepresentations and 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 $M \oplus N$.

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 Sheet 9). Finally, there's no generalisation of the trivial representation. So group algebras are quite special.

Lemma 3.2.10. *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) $\mathrm{Hom}_A(M \oplus N, L) = \mathrm{Hom}_A(M, L) \oplus \mathrm{Hom}_A(N, L)$

When we proved this for representations (Corollary 1.8.4) we first proved it for the spaces of all linear maps (Lemma 1.8.1) and deduced for G-linear maps by taking invariant subrepresentations. We can't use exactly the same argument here, because $\mathrm{Hom}(M, N)$ is not an A-module, and there's no such thing as an invariant submodule. However, we just need to adapt the proof slightly.

Proof. (i) In Lemma 1.8.1 we proved that

$$\begin{aligned} P\colon\ \mathrm{Hom}(L, M \oplus N) &\to \mathrm{Hom}(L, M) \oplus \mathrm{Hom}(L, N) \\ f &\mapsto (\pi_M \circ f, \pi_N \circ f) \end{aligned}$$

was an isomorphism of vector spaces. Since π_M and π_N are A-linear, P takes A-linear maps to A-linear maps. Also, the inverse to P is

$$\begin{aligned} P^{-1}\colon\ \mathrm{Hom}(L, M) \oplus \mathrm{Hom}(L, N) &\to \mathrm{Hom}(L, M \oplus N) \\ (f, g) &\mapsto \iota_M \circ f + \iota_N \circ g \end{aligned}$$

which also takes A-linear maps to A-linear maps. So P induces the required isomorphism. (ii) is proved similarly. $\square$

This gives a (slightly!) different proof of Corollary 1.8.4.

Now 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 $x \in M$, $y \in N$.

Lemma 3.2.11. *Every module over $A \oplus B$ is isomorphic to $M \oplus N$ for some A-module M and some B-module N.*

Proof. Consider the elements 1_A and 1_B in $A \oplus B$. They satisfy the following:

$$1_A^2 = 1_A, \quad 1_B^2 = 1_B, \quad 1_A 1_B = 1_B 1_A = 0, \quad 1_{A \oplus B} = 1_A + 1_B$$

Now let L be any $A \oplus B$-module. So we have linear maps

$$\begin{aligned} 1_A &\colon L \to L \\ 1_B &\colon L \to L \end{aligned}$$

Define $M = \mathrm{Im}(1_A)$, and $N = \mathrm{Im}(1_B)$. Then 1_A is a projection from L onto M, because if $m \in M$ then by definition $m = 1_A(l)$ for some $l \in L$, so

$$1_A(m) = 1_A^2(l) = 1_A(l) = m$$

Similiarly 1_B is a projection from L onto N. But for any $x \in L$ we have

$$x = 1_{A \oplus B}(x) = 1_A(x) + 1_B(x)$$

So $1_B(x) = 0$ iff $x = 1_A(x)$, i.e. $M = \mathrm{Im}(1_A) = \mathrm{Ker}(1_B)$. Similarly $N = \mathrm{Im}(1_B) = \mathrm{Ker}(1_A)$. So by Lemma 1.5.4,

$$L = \mathrm{Im}(1_A) \oplus \mathrm{Ker}(1_A) = M \oplus N$$

as vector spaces. Now take $x \in M$, i.e. $1_A(x) = x$. Then for $(a, b) \in A \oplus B$ we have

$$\begin{aligned} (a, b)(x) &= (a, b) 1_A(x) \\ &= (a, b)(1_A, 0)(x) \\ &= (a, 0)(x) \\ &= 1_A (a, 0)(x) \in M \end{aligned}$$

So M is a submodule, and furthermore 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 a B-module. $\square$

Example 3.2.12. 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 $V \oplus W$ where V and W are vector spaces.

Recall that A is isomorphic to $\mathbb{C}[C_2]$, so A-modules are the same as representations of C_2. So every representation of C_2 should canonically split up into a pair of vector spaces. This is true: every representation V of C_2 is a direct sum $V = U \oplus W$, where U is a trivial representation and W is the direct sum of copies of the sign representation (U and W are the ± 1 eigenspaces for the generator of C_2).

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.

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 $(f \circ g)^* = g^* \circ f^*$. $\square$

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^*.

Recall that a module over A_V is the same thing as an algebra homomorphism $A_V \to \mathrm{Hom}(M, M)$ for some vector space M. There's an obvious homomorphism $A_V \to \mathrm{Hom}(V, V)$, namely the identity! So the vector space V is automatically an A_V-module. It has A-module structure

$$\begin{aligned} \hat{m} \colon A_V \times V &\to V \\ (f, x) &\mapsto f(x) \end{aligned}$$

If we pick a basis for V this becomes the action of $\mathrm{Mat}_{n\times n}(\mathbb{C})$ on $\mathbb{C}^n$ (column vectors). We'll prove shortly that in fact this is the only A_V-module (apart from direct sums of V with itself).

Recall (Lemma 1.8.9) that if W is any representation of a group G, and V_{reg} is the regular reprentation, then there is a natural isomorphism of vector spaces

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

This fact generalizes to arbitrary algebras:

Lemma 3.3.2. *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 1.8.9, i.e. we define

$$\begin{array}{rcl} T \colon M & \to & \mathrm{Hom}_A(A, M) \\ x & \mapsto & T_x \end{array}$$

where

$$\begin{array}{rcl} T_x \colon A & \to & M \\ a & \mapsto & ax \end{array}$$

Then the inverse to T is

$$\begin{aligned} T^{-1} \colon \mathrm{Hom}_A(A, M) &\to M \\ f &\mapsto f(1_A) \end{aligned}$$

□

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

$$A_V = \bigoplus_{k=1}^{n} (A_V)_{\bullet k}$$

□

Corollary 3.3.4. *The only A_V-linear maps from V to V are scalar multiples of the identity, i.e.*

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

Proof. We have an isomorphism of vector spaces (Lemma 3.3.2)

$$\begin{aligned} A_V &= \mathrm{Hom}_{A_V}(A_V, A_V) \\ &= \mathrm{Hom}_{A_V}(V^{\oplus n}, V^{\oplus n}) \\ &= \mathrm{Hom}_{A_V}(V, V)^{\oplus n^2} \end{aligned}$$

Since $\dim A_V = n^2$, we must have $\dim \mathrm{Hom}_{A_V}(V, V) = 1$. □

So we've shown that the A_V-module A_V is isomorphic to a direct sum of copies of V. Now we can prove that in fact *any* A_V-module is isomorphic to a direct sum of copies of V.

Theorem 3.3.5. *Let M be any A_V-module. Then we have an isomorphism of A_V-modules*

$$M = V^{\oplus k}$$

where $k = \dim \mathrm{Hom}_{A_V}(V, M)$.

Proof. By Lemma 3.3.2 and Lemma 3.3.3 we have isomorphisms of vector spaces

$$\begin{aligned} M &= \mathrm{Hom}_{A_V}(A_V, M) \\ &= \mathrm{Hom}_{A_V}(V^{\oplus n}, M) \\ &= \mathrm{Hom}_{A_V}(V, M)^{\oplus n} \end{aligned}$$

So if $k = \dim \mathrm{Hom}_{A_V}(V, M)$ then

$$\dim M = nk = (\dim V)^{\oplus k}$$

So M is isomorphic as a vector space to $V^{\oplus k}$, but we must show that the A_V-module structures agree. Let $\{f_1, \ldots, f_k\}$ be a basis for $\mathrm{Hom}_{A_V}(V, M)$, and let

$$F = (f_1, \ldots, f_k) \in \mathrm{Hom}_{A_V}(V, M)^{\oplus k} = \mathrm{Hom}_{A_V}(V^{\oplus k}, M)$$

It's sufficient to prove that

$$F \colon V^{\oplus k} \to M$$

is a surjection, then it must be an isomorphism since the dimensions of space are equal. So pick $x \in M$, and let's prove that x is the image of F. Under the isomorphism between M and $\mathrm{Hom}_{A_V}(A_V, M)$, x corresponds to

$$\begin{aligned} T_x \colon A_V &\to M \\ a &\mapsto ax \end{aligned}$$

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

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad , \ldots , \quad e_n = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$$

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. $\square$

[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. We have

$$\mathrm{Hom}_{A_V}(V, V) = \mathbb{C} = \mathrm{Hom}(\mathbb{C}, \mathbb{C})$$

(Corollary 3.3.4). 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 $f_{ij} \in \mathrm{Hom}_{A_V}(V, V)$ is just a complex number, so f is given by a 2×2-matrix and

$$f(x_1, x_2) = \begin{pmatrix} f_{11} & f_{12} \\ f_{21} & f_{22} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$$

Writing it this way, it should be clear that we have an isomorphism of algebras

$$\begin{aligned} \mathrm{Hom}_{A_V}(V^{\oplus 2}, V^{\oplus 2}) &= \mathrm{Mat}_{2\times 2}(\mathbb{C}) \\ &= \mathrm{Hom}(\mathbb{C}^2, \mathbb{C}^2) \end{aligned}$$

(i.e. composition of A_V-linear maps corresponds to multiplication of matrices). More generally,

$$\begin{aligned} \mathrm{Hom}_{A_V}(V^{\oplus k}, V^{\oplus l}) &= \mathrm{Mat}_{k\times l}(\mathbb{C}) \\ &= \mathrm{Hom}(\mathbb{C}^k, \mathbb{C}^l) \end{aligned}$$

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. Let A be an algebra. An A-module M is **simple** if it contains no non-trivial submodules.

Example 3.4.2. (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'.

(iii) If $A = \mathrm{Hom}(V, V)$ then the A-module V is simple. We know that every A-module is isomorphic to $V^{\oplus k}$ for some k, so in particular $\dim V$ divides $\dim M$ for all A-modules M. So if M is a submodule of V then either $\dim M = 0$, or $\dim M = \dim V$, i.e. $M = V$.

Schur's Lemma is really a fact about simple modules:

Proposition 3.4.3. *Let M and N be simple A-modules. Then*

$$\dim \mathrm{Hom}_A(M, N) = \begin{cases} 1 & \text{if } M \text{ and } N \text{ are isomorphic} \\ 0 & \text{if } M \text{ and } N \text{ are not isomorphic} \end{cases}$$

Proof. Use the identical proof to Theorem 1.6.1 and Proposition 1.8.5. □

Definition 3.4.4. 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 3.4.5. 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 3.4.6. *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 3.4.7. 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 3.4.5 shows that the algebra $\langle 1, x \rangle$ is not semi-simple.

By Theorem 3.3.5, 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 3.4.8 (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.]

Notice that (i) $\Rightarrow$ (ii) by definition. The harder parts are that (ii)$\Rightarrow$ (iii) and (iii)$\Rightarrow$(i). We'll prove them both in stages.

Lemma 3.4.9. *For any algebra, there is a natural isomorphism of algebras*

$$A^{op} = \mathrm{Hom}_A(A, A)$$

Proof. We know (Lemma 3.3.2) that for any A-module M there is a natural isomorphism of vector spaces

$$T\colon M \to \mathrm{Hom}_A(A, M)$$

where x maps to

$$T_x\colon a \mapsto ax$$

Setting $M = A$, we get an isomorphism of vector spaces

$$T\colon A \to \mathrm{Hom}_A(A, A)$$

where a maps to

$$T_a\colon b \mapsto ba$$

Then

$$T_{a_1 a_2}\colon b \mapsto ba_1 a_2 = (T_{a_2} \circ T_{a_1})(b)$$

so

$$T_{a_1 a_2} = T_{a_2} \circ T_{a_1}$$

i.e. T is an algebra homomorphism from A^{op} to $\mathrm{Hom}_A(A, A)$. □

Proof of Theorem 3.4.8(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 3.4.9,

$$\begin{aligned} A^{op} &= \mathrm{Hom}_A(A, A) \\ &= \bigoplus_{i,j} \mathrm{Hom}_A(M_i^{\oplus m_i}, M_j^{\oplus m_j}) \\ &= \mathrm{Hom}_A(M_1^{\oplus m_1}, M_1^{\oplus m_1}) \oplus \ldots \oplus \mathrm{Hom}_A(M_k^{\oplus m_k}, M_k^{\oplus m_k}) \end{aligned}$$

by Schur's Lemma. Also by Schur's Lemma, $\mathrm{Hom}_A(M_i, M_i) = \mathbb{C}$, and we claim that this implies

$$\mathrm{Hom}_A(M_i^{\oplus m_i}, M_i^{\oplus m_i}) = \mathrm{Mat}_{m_i \times m_i}(\mathbb{C})$$

We argued this at the end of Section 3.3 in the case $A = A_V$ and $M_i = V$, but actually our argument only used the fact that $\mathrm{Hom}_{A_V}(V, V) = \mathbb{C}$ so it applies to an arbitrary simple module M_i. 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

$$A = \mathrm{Mat}_{m_1 \times m_1}(\mathbb{C})^{op} \oplus \ldots \oplus \mathrm{Mat}_{m_k \times m_k}(\mathbb{C})^{op}$$

But $\mathrm{Mat}_{m_1 \times m_1}(\mathbb{C})^{op}$ is a matrix algebra by Lemma 3.3.1. □

Lemma 3.4.10. *If A and B are semi-simple algebras then so is $A \oplus B$.*

Proof. By Lemma 3.2.11 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

$$M = M_1 \oplus \ldots \oplus M_k$$
$$N = N_1 \oplus \ldots \oplus N_l$$

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. □

Every matrix algebra is semi-simple, so this proves that (iii)⇒(i) in Theorem 3.4.8, and completes the proof of the Theorem.

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 3.4.11. *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 3.2.11 and Theorem 3.3.5, 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 3.4.12. *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 3.4.8 ((ii)$\Rightarrow$(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 3.4.13. *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 3.4.12(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 1.8.7, Corollary 1.8.8 and Corollary 1.8.10 as special cases. But we also have a new result, which is a special case of Corollary 3.4.12(ii):

Corollary 3.4.14. *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*

$$\mathrm{Mat}_{d_1\times d_1}(\mathbb{C}) \oplus \ldots \oplus \mathrm{Mat}_{d_r\times d_r}(\mathbb{C})$$

Notice that for $G = C_2$ we found this isomorphism

$$\mathbb{C}[C_2] \xrightarrow{\sim} \mathbb{C} \oplus \mathbb{C}$$

explicitly (and the case $G = C_3$ is in Problem Sheet 8). In fact we can always find an explicit isomorphism, as we now describe.

Recall that if A_V is a matrix algebra, then V is an A_V-module and the module structure map

$$A_V \to \mathrm{Hom}(V, V)$$

is an isomorphism (actually it's the identity). So if $A = \bigoplus_{i=1}^r A_{V_i}$ is a direct sum of matrix algebras, then $V_1, \ldots, V_r$ are the simple A-modules, and the direct sum of the module structure maps

$$A \to \bigoplus_{i=1}^r \mathrm{Hom}(V_i, V_i)$$

is an isomorphism (again it's the identity). Now let G be a group, and let

$$\rho_i \colon G \to \mathrm{Hom}(U_i, U_i)$$

be the irreps of G. Then each U_i is a simple $\mathbb{C}[G]$-module, and has module structure

$$\tilde{\rho}_i : \mathbb{C}[G] \to \mathrm{Hom}(U_i, U_i)$$

(the linear extension of ρ_i). Since $\mathbb{C}[G]$ is isomorphic to a direct sum of matrix algebras, the map

$$(\tilde{\rho}_1, \ldots, \tilde{\rho}_r) \colon \mathbb{C}[G] \to \bigoplus_{i=1}^r \mathrm{Hom}(U_i, U_i)$$

is an isomorphism.

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

$$\begin{aligned} \mathbb{C}[G] &\xrightarrow{\sim} \mathbb{C} \oplus \mathbb{C} \oplus \mathrm{Mat}_{2\times 2}(\mathbb{C}) \\ \sigma &\mapsto \left(1, 1, \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix}\right) \\ \tau &\mapsto \left(1, -1, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right) \end{aligned}$$

(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

$$\begin{aligned} \mathbb{C}[G] &\to \mathrm{Mat}_{4\times 4}(\mathbb{C}) \\ \sigma &\mapsto \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \omega & 0 \\ 0 & 0 & 0 & \omega^{-1} \end{pmatrix} \\ \tau &\mapsto \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \end{aligned}$$

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 1-dimensional.

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. $\square$

Now let $A = \mathbb{C}[G]$ for a group G. If $g \in G$ is in the centre of G, then clearly $\lambda g \in A$ lies in Z_A for any $\lambda \in \mathbb{C}$. However, Z_A is larger than this.

Proposition 3.5.3. *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 to the space of class functions

$$\mathbb{C}_{cl} \subset \mathbb{C}^G$$

Now we can give a very quick proof of Theorem 2.3.3, that for any group G

$$\#\{\text{conjugacy classes in } G\} = \#\{\text{irreps of } G\}$$

Let $U_1, \ldots, U_r$ be the irreps of G. Then we know from Corollary 3.4.14 that we have an isomorphism

$$\mathbb{C}[G] = \bigoplus_{i=1}^{r} \mathrm{Hom}(U_i, U_i)$$

Since it's clear that $Z_{A \oplus B} = Z_A \oplus Z_B$, this implies that

$$Z_{\mathbb{C}[G]} = \bigoplus_{i=1}^{r} Z_{\mathrm{Hom}(U_i, U_i)}$$

So it has a basis given by the elements $\{\mathbf{1}_{U_i}\}$, and hence $\dim Z_{\mathbb{C}[G]}$ is the number of irreps of G. Since $\dim Z_{\mathbb{C}[G]}$ is also the number of conjugacy classes in G, this proves the theorem.

In fact this proof is the same as our original proof, we're just able to explain it more easily now. In our original proof we had maps

$$\theta_i \in \mathrm{Hom}_G(V_{reg}, V_{reg})$$

and we considered the subspace Θ that they spanned. We now know that that $\mathrm{Hom}_G(V_{reg}, V_{reg})$ is $\mathbb{C}[G]^{op}$, and it's isomorphic to

$$\bigoplus_{i=1}^{r} \mathrm{Hom}(U_i, U_i)$$

The maps θ_i are exactly the elements $\mathbf{1}_{U_i}$, and their span Θ is actually $Z_{\mathbb{C}[G]}$.

In our original proof we actually expressed each class function $\delta_{[g]}$ as a linear combination of the maps θ_i, using Lemma 2.3.4. In our more sophisticated language, the result is that the isomorphism

$$\mathbb{C}[G] \to \bigoplus_{i=1}^{r} \mathrm{Hom}(U_i, U_i)$$

sends

$$z_{[g]} \mapsto \left(\lambda_1^{[g]} \mathbf{1}_{U_1}, \ldots, \lambda_r^{[g]} \mathbf{1}_{U_r}\right)$$

where $\lambda_i^{[g]} = \chi_i(g) \frac{|[g]|}{\dim U_i}$.