M3/4/5P12 Group Representation Theory

Rebecca Bellovin

April 10, 2017

1 Administrivia

Comments, complaints, and corrections:

E-mail me at r.bellovin@imperial.ac.uk. The course website is `wwwf.imperial.ac.uk/~rbellovi/teaching/m3p12.html`; there will be no blackboard page.

Office hours:

Thursdays 4:30-5:30, starting January 19.

Problem sessions:

Problem sessions will be on the Tuesday session of odd-numbered weeks, starting on January 24.

Other reading:

Previous versions of this course have been taught by James Newton (`https://nms.kcl.ac.uk/james.newton/M3P12.html`), Ed Segal (`http://wwwf.imperial.ac.uk/~epsegal/repthy.html`), and Matthew Towers (`https://sites.google.com/site/matthewtowers/m3p12`). Lecture notes and sample problem sheets are available from their website; we will cover similar material, though somewhat rearranged.

Recommended reference books include:

- G. James and M. Liebeck, *Representations and Characters of Groups.*
- J.-P. Serre, *Linear Representations of Finite Groups.*
- J.L. Alperin, Local Representation Theory.

2 Introduction to representations

2.1 Motivation

Our ultimate goal is to study groups (and in this course, we will only study finite groups). Recall:

Definition 2.1. A *group* G is a set equipped with an associative multiplication map $G \times G \to G$ such that there is an identity element e (i.e., $e \cdot g = g \cdot e = g$ for all $g \in G$) and every element has an inverse (i.e. for every $g \in G$, there is some $g^{-1} \in G$ so that $g \cdot g^{-1} = g^{-1} \cdot g = e$).

Groups generally show up as symmetries of objects we are interested in, but it is difficult to study them directly. For example, it is much more fruitful to view D_8 as the symmetry group of the square than to write down its multiplication table.

Theorem 2.2. *Let G be a group with $|G| = p^a q^b$ for p, q prime numbers. Then G has a proper normal subgroup.*

The easiest proof is via techniques from representation theory, but it is not obvious how to attack it by "bare hands". The proof requires a bit of algebraic number theory, so we may not be able to cover it, but the proof is in James and Liebeck's book.

There are also applications to physics and chemistry: J.-P. Serre wrote his book because his wife was a chemist.

The structure of the course will be:

1. Representations: definitions and basic structure theory
2. Character theory
3. Group algebras

Since we understand linear algebra much better than abstract group theory, we will attempt to turn groups into linear algebra.

Informally, a representation will be a way of writing elements of a group as matrices. For example, let $G = C_4 = e, g, g^2, g^3$, with $g^4 = e$. Consider also the 2×2 matrices

$$I = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), M = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right), M^2 = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right), M^3 = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$$

Since $M^4 = I$, this forms a finite cyclic group of order 4, and $g \mapsto M$ defines an isomorphism with C_4. Thus, we have embedded C_4 as a subgroup of $\mathrm{GL}_2(\mathbf{C})$.

We further observe that M can be diagonalized: its characteristic polynomial is $\det(\lambda I - M) = \lambda^2 + 1$, which has two distinct roots, $\pm i$. The eigenspaces are generated by $\left(\begin{smallmatrix} 1 \\ -i \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 \\ i \end{smallmatrix}\right)$, so after changing basis, we see that our embedding is actually built out of two embeddings $C_4 \to \mathbf{C}^\times$ given by $g \mapsto i$, $g \mapsto -i$.

2.2 Definitions

2.2.1 First definitions

Recall from last time: We defined a group homomorphism $C_4 \to \mathrm{GL}_2(\mathbf{C})$ by sending a generator $g \mapsto M = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. If $P = \left(\begin{smallmatrix} i & -1 \\ i & 1 \end{smallmatrix}\right)$, then $M' = PMP^{-1} = \left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right)$.

Definition 2.3 (Preliminary version)**.** Let G be a group. A *representation* of G is a homomorphism $\rho : G \to \mathrm{GL}_d(\mathbf{C})$ (so $\rho(gh) = \rho(g)\rho(h)$). That is, for every $g \in G$ we have a matrix $\rho(g)$, and $\rho(gh) = \rho(g)\rho(h)$ for all $g, h \in G$. We call d the *dimension* of ρ.

Two representations $\rho, \rho' : G \to \mathrm{GL}(\mathbf{C}^d)$ are *equivalent* if there is some matrix $P \in \mathrm{GL}(\mathbf{C}^d)$ such that $\rho' = P\rho P^{-1}$.

Observe that our definition implies that if $e \in G$ is the identity, $\rho(e) = \mathrm{I}_d$. For any $g \in G$, we further have that $\rho(g^{-1}) = \rho(g)^{-1}$.

Example 2.4.

1. Suppose that $\rho(g) = \mathrm{Id}$ for all $g \in G$. This is called the *trivial representation*.

2. Let $d = |G|$ and let the elements of the standard basis correspond to elements of G. That is, choose some ordering of the elements of G and let $\{e_{g_1}, \ldots, e_{g_d}\}$ be the standard basis of $\mathbf{C}^d$. Define a representation by setting $\rho(g)(e_h) = e_{gh}$ for all $g, h \in G$. This is called the *regular representation.*

3. Let $G = C_n$, the cyclic group of order n with generator g, and let $\rho : G \to \mathrm{GL}_1(\mathbf{C})$ be defined by sending g to some nth root of unity ζ. For example, we could set $\zeta = e^{2\pi i/n}$. But any choice of $e^{2a\pi i/n}$ works, as well. To be more concrete, if $n = 4$, we could send g to i, -1, $-i$, or 1; the last case is the trivial 1-dimensional representation.

4. Let $G = S_n$, the group of permutations of n elements. Let $\{e_1, \ldots, e_n\}$ be the standard basis of $\mathbf{C}^n$; we define a representation by setting $\rho(g)(e_i) = e_{g(i)}$. This is called the *permutation representation.*

5. More generally, let X be a set with a left-action of G; recall that this means there is an "action map" $G \times X \to X$ (which we write $(g, x) \mapsto g \cdot x$) such that $(gh) \cdot x = g \cdot (h \cdot x)$. Let $d = |X|$ and let elements of the standard basis of $\mathbf{C}^d$ correspond to elements of X; write the basis $\{e_x\}_{x \in X}$. Then we define a representation $\rho : G \to \mathrm{GL}_d(\mathbf{C})$ by setting $\rho(g)(e_x) = e_{g \cdot x}$.

   If $X = G$, this construction recovers the regular representation. If $G = S_n$ and $X = \{1, \ldots, n\}$, this recoves the permutation representation.

Note that we do not require a representation to be an *injective* homomorphism! In fact, for the trivial representation, the kernel is all of G. For the 1-dimensional representations of C_n we wrote down earlier, ρ is injective if and only if ζ is a *primitive* nth root of 1, that is, $\zeta^n = 1$ and n is the smallest positive integer with this property. If ρ is injective, we say that it is a *faithful* representation.

2.2.2 Cleaner definitions

Recall from linear algebra that every finite dimensional vector space has a basis, but a basis is not unique. Moreover, if $g \in G$ and $\rho : G \to \mathrm{GL}_d(\mathbf{C})$ is a representation, we can view $\rho(g)$ as an invertible linear transformation $V \to V$, where V is a d-dimensional complex vector space. Thus, it is cleaner to rewrite our definitions as follows:

Definition 2.5. A *representation* of G is a pair (V, ρ) where V is a finite-dimensional complex vector space, and $\rho : G \to \mathrm{GL}(V)$ is a homomorphism.

Recall that $\mathrm{GL}(V) := \{f : V \xrightarrow{\sim} V\}$.

If we pick a basis of V, we may write ρ in terms of matrices as before:

Choose a basis $\mathcal{B} = (b_1, \ldots, b_d)$ of V. This choice of basis gives us an isomorphism $\mathbf{C}^d \xrightarrow{\sim} V$, and therefore an isomorphism $\mathrm{GL}_d(\mathbf{C}) \xrightarrow{\sim} \mathrm{GL}(V)$. We therefore have a representation $\rho_{\mathcal{B}} : G \to \mathrm{GL}_d(\mathbf{C})$, in the sense of the previous lecture.

If we need to distinguish the two notions of representations, we will refer to homomorphisms $\rho : G \to \mathrm{GL}_d(\mathbf{C})$ as *matrix representations.*

Lemma 2.6. *Let $\rho : G \to \mathrm{GL}(V)$ be a representation, and let $\mathcal{B} = (b_1, \ldots, b_d)$ and $\mathcal{B}' = (b'_1, \ldots, b'_d)$ be bases of V. Then $\rho_{\mathcal{B}}$ and $\rho_{\mathcal{B}'}$ are equivalent. Conversely, if $\rho_1, \rho_2 : G \to \mathrm{GL}_d(\mathbf{C})$ are equivalent matrix representations, there is a representation (V, ρ) such that ρ_1 and ρ_2 can be obtained by choosing bases $\mathcal{B}_1$ and $\mathcal{B}_2$ of V.*

Proof. Let P denote the change-of-basis matrix taking $\mathcal{B}$ to $\mathcal{B}'$, that is, $Pb_i = b'_i$. Then for every $g \in G$, $\rho_{\mathcal{B}'} = P\rho_{\mathcal{B}}P^{-1}$, so $\rho_{\mathcal{B}}$ and $\rho_{\mathcal{B}'}$ are equivalent.

For the converse, suppose that ρ_1 and ρ_2 are equivalent, and let $P \in \mathrm{GL}_d(\mathbf{C})$ be a matrix such that $\rho_2(g) = P\rho_1(g)P^{-1}$ for all $g \in G$. Let V be the underlying vector space of $\mathbf{C}^d$. Then we can think of ρ_1 as a representation $\rho : G \to \mathrm{GL}(V)$ by forgetting about the standard basis on $\mathbf{C}^d$. If we let $\mathcal{B}_1$ denote the standard basis of $\mathbf{C}^d$, $\rho_1(g) = \rho_{\mathcal{B}_1}$ (because we forgot the standard basis and then remembered it again).

Now let $\mathcal{B}_2$ denote the basis of $\mathbf{C}^d$ given by the columns of P^{-1}. Then for every $g \in G$, the matrix of $\rho(g)$ with respect to $\mathcal{B}_2$ is given by $P\rho_1(g)P^{-1}$, as desired. $\square$

2.3 Homomorphisms of representations

Let (V, ρ_V) and (W, ρ_W) be representations of G.

Definition 2.7. A linear map $f : V \to W$ is *G-linear* if $f \circ \rho_V(g) = \rho_W(g) \circ f$ for every $g \in G$.

Recall that a map $f : V \to W$ is linear if $f(av_1 + bv_2) = af(v_1) + bf(v_2)$ for $a, b \in \mathbf{C}$ and $v_1, v_2 \in V$.

In other words, for every element $g \in G$, we have a commutative square:

$$\begin{tikzcd} V \arrow[r, "\rho_V(g)"] \arrow[d, "f"] & V \arrow[d, "f"] \\ W \arrow[r, "\rho_W(g)"] & W \end{tikzcd}$$

Definition 2.8. Let (V, ρ_V) and (W, ρ_W) be representations of G. A map $f : V \to W$ is said to be a *homomorphism* of representations if it is G-linear, and it is said to be an *isomorphism* of representations if it is G-linear and invertible.

Exercise 2.9. Check that if f is an isomorphism of representations, so is f^{-1}.

Proposition 2.10. *Let (V, ρ_V) and (W, ρ_W) be representations of G, and let $\mathcal{B}_V$ and $\mathcal{B}_W$ be bases of V and W, respectively. If $f : V \to W$ is a linear map and $[f]_{\mathcal{B}_V,\mathcal{B}_W}$ denotes the matrix representing f with respect to the chosen bases, then f is G-linear if and only if $[f]_{\mathcal{B}_V,\mathcal{B}_W}\rho_V(g) = \rho_W(g)[f]_{\mathcal{B}_V,\mathcal{B}_W}$ for all $g \in G$.*

Proof. This follows by unwinding the definition; trace through the commutative diagram above, and write down the matrix associated to each map. □

Corollary 2.11. *Let (V, ρ_V) and (W, ρ_W) be d-dimensional representations of G, and let $\mathcal{B}_V$ and $\mathcal{B}_W$ be bases of V and W, respectively. Then (V, ρ_V) and (W, ρ_W) are isomorphic if and only if $\rho_{V,\mathcal{B}_V}$ and $\rho_{W,\mathcal{B}_W}$ are equivalent matrix representations.*

When we discussed the regular representation, there was some question about how to enumerate elements of G. It doesn't matter, and the reason it doesn't matter is because re-ordering the elements of G is just changing the basis of the underlying vector space. So different orderings for the elements of G give different *matrix* representations but isomorphic abstract representations.

2.4 Direct sums and indecomposable representations

Let us begin with an example, namely the regular representation of $C_2 = \{e, g\}$. This is a 2-dimensional representation $(V_{\text{reg}}, \rho_{\text{reg}})$, and we choose the basis (b_e, b_g); the action of C_4 is given by $\rho_{\text{reg}}(g)(b_e) = b_g$ and $\rho_{\text{reg}}(g)(b_g) = b_e$.

We also have two 1-dimensional representations, (V_0, ρ_0) and (V_1, ρ_1), given in coordinates by $\rho_i(g) = (-1)^i \in \mathrm{GL}_1(\mathbf{C})$.

It turns out we can define homomorphisms $(V_i, \rho_i) \to (V_{\text{reg}}, \rho_{\text{reg}})$:

- Choose a basis element $v_0 \in V_0$, and define a linear transformation $V_0 \to V_{\text{reg}}$ via $v_0 \mapsto b_e + b_g$. Since $\rho_{reg}(g)(b_e + b_g) = b_e + b_g$ (exercise!), this map is C_2-linear.

- Choose a basis element $v_1 \in V_1$, and define a linear transformation $V_1 \to V_{\mathrm{reg}}$ via $v_1 \mapsto b_e - b_g$. Since $\rho_{reg}(g)(b_e - b_g) = b_g - b_e$ (exercise!), this maps is C_2-linear.

Thus, we have a linear transformation $V_0 \oplus V_1 \to V_{\mathrm{reg}}$, and since $\langle b_e + b_g \rangle \cap \langle b_e - b_g \rangle = \{0\}$, it is an isomorphism.

We will see that we can define a representation $(V_0 \oplus V_1, \rho_1 \oplus \rho_2)$ so that this is actually an isomorphism of representations.

Recall that if V, W are finite-dimensional complex vector spaces, their *direct sum* $V \oplus W$ consists of ordered pairs (v, w) with $v \in V, w \in W$. Defining addition by $(v_1, w_1)+(v_2, w_2) := (v_1+v_2, w_1+w_2)$ and scaling by $a \cdot (v, w) := (a \cdot v, a \cdot w)$ for $a \in \mathbf{C}$ makes $V \oplus W$ into another finite-dimensional complex vector space.

If we are have finite-dimensional complex vector spaces V_1, V_2, we may define the direct sum $V_1 \oplus V_2$. If we have linear transformations $f_1 : V_1 \to W$ and $f_2 : V_2 \to W$, where W is another finite-dimensional complex vector space, we may define a new linear transformation $f_1 \oplus f_2 : V_1 \oplus V_2 \to W$ via $(f_1 \oplus f_2)(v_1, v_2) := f_1(v_1) + f_2(v_2)$.

If we are given linear transformations $T_V : V \to V$ and $T_W : W \to W$, we may also define a new linear transformation $T_V \oplus T_W : V \oplus W \to V \oplus W$ by setting $(T_V \oplus T_W)(v, w) := (T_V(v), T_W(w))$. This permits us to define the direct some of two group representations:

Definition 2.12. Let (V, ρ_V) and (W, ρ_W) be representations of a finite group G. The direct sum $(V \oplus W, \rho_V \oplus \rho_W)$ is defined by setting $(\rho_V \oplus \rho_W)(g) := \rho_V(g) \oplus \rho_W(g) \in \mathrm{GL}(V \oplus W)$.

Suppose that $\mathcal{B}_V = (v_1, \ldots, v_{d_V})$ and $\mathcal{B}_W = (w_1, \ldots, w_{d_W})$ are bases for V and W, respectively, and let $\rho_{V,\mathcal{B}_V}$ and $\rho_{W,\mathcal{B}_W}$ be the associated matrix representations. Then $V \oplus W$ is $d_V + d_W$-dimensional, and

$$((v_1, 0), \ldots, (v_{d_V}, 0), (0, w_1), \ldots, (0, w_{d_W}))$$

is a basis. The matrix representation associated to $\rho_V \oplus \rho_W$ with respect to this basis is given by

$$\begin{pmatrix} \rho_{V,\mathcal{B}_V}(g) & 0 \\ 0 & \rho_{W,\mathcal{B}_W} \end{pmatrix}$$

for each $g \in G$.

Proposition 2.13. *The map $V_0 \oplus V_1 \to V_{\mathrm{reg}}$ we defined earlier is an isomorphism of representations of C_2.*

Proof. It is an isomorphism of vector spaces, so it is enough to prove that it is C_2-linear. But this follows from the definition of $\rho_0 \oplus \rho_1$. □

We can also see this on the level of matrices: The matrix representation associated to $\rho_0 \oplus \rho_1$ with respect to $((v_0, 0), (0, v_1)$ is given by

$$(\rho_0 \oplus \rho_1)(e) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad (\rho_0 \oplus \rho_1)(g) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

On the other hand, the matrix representation associated to ρ_{reg} with respect to the basis (b_e, b_g) is given by

$$\rho_{\text{reg}}(e) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \rho_{\text{reg}}(g) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Since the underlying representations are isomorphic, their matrix representations are equivalent, so there is some $P \in \mathrm{GL}_2(\mathbf{C})$ such that $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) = P \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) P^{-1}$. Taking $P = \left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$ suffices.

Definition 2.14. A representation (V, ρ_V) of G is *decomposable* if it is isomorphic (as a representation) to the direct sum of smaller representations, i.e., if there are non-zero representations (V_1, ρ_1) and (V_2, ρ_2) such that $(V, \rho) \cong (V_1 \oplus V_2, \rho_1 \oplus \rho_2)$. A representation is *indecomposable* if no such decomposition exists.

We also make the following observation: Suppose that (V, ρ_V) and (W, ρ_W) are representations of G. We have a linear map $V \to V \oplus W$ which is injective, and it is G-linear. So $V \oplus W$ actually contains subspaces which are preserved by the linear transformations $(\rho_V \oplus \rho_W)(g)$.

2.5 Subrepresentations and Irreducible Representations

Before we define subrepresentations, recall the notion of a vector subspace:

Definition 2.15. If V is a finite-dimensional complex vector space, a *subspace* of V is a subset $W \subset V$ which is itself a complex vector space.

In particular, W must be a group under addition (so $0 \in W$ and if $w \in W$, so is $-w$), and W is preserved under scaling (i.e., if $w \in W$ and $\lambda \in \mathbf{C}$, $\lambda w \in W$.

For example, $\{0\} \subset V$ is a subspace. As another (more interesting) example, suppose we have a linear transformation $f : V_1 \to V_2$. Then we can define the kernel $\ker(f) := \{v \in V_1 : f(v) = 1\}$ and the image $\mathrm{im}(f) := \{f(v) \in V_2 : v \in V_1\}$. The kernel is a vector subspace of V_1 and the image is a vector subspace of V_2.

We can specify a subspace of V by giving a set of *generators*: Let $\{v_1, \ldots, v_n\}$ be a subset of V. The *span* of $\{v_1, \ldots, v_n\}$, or the *subspace generated by* $\{v_1, \ldots, v_n\}$, is the set

$$W := \langle v_1, \ldots, v_n \rangle := \{a_1 v_1 + \ldots + a_n v_n : a_i \in \mathbf{C}\}$$

Then W is a subset of V and a vector space, so it is a subspace of V. Note that we do not assume that the v_i are linearly independent! They generate W but need not form a basis of W.

Let $T : V \to V$ be a linear transformation, and let $W \subset V$ be a subspace. We say that T *stabilizes* or *preserves* W if $T(w) \in W$ for every $w \in W$. In other words, T carries W to itself. Thus, it also defines a linear transformation $W \to W$, which we denote $T|_W$. We call this the *restriction* of T. If W is 1-dimensional, then T preserves W if and only if W consists of eigenvectors for T, i.e., if there is some $\lambda \in \mathbf{C}$ such that $T(w) = \lambda w$ for every $w \in W$.

We can describe this in terms of matrices: Suppose that $\mathcal{B}_V := (w_1, \dots, w_{d_W}, v_{d_W+1}, \dots, v_{d_V})$ is a basis of V such that $\mathcal{B}_W := (w_1, \dots, w_{d_W})$ is a basis of W (exercise: check that we can always find such a basis!). Let $T : V \to V$ be a linear transformation which preserves W. Then the matrix $[T]_{\mathcal{B}_V}$ is of the form $\left(\begin{smallmatrix} [T|_W]_{\mathcal{B}_W} & * \\ 0 & * \end{smallmatrix}\right)$.

Now we can define subrepresentations:

Definition 2.16. Let (V, ρ_V) be a representation of G. A *subrepresentation* is a vector subspace $W \subset V$ such that $\rho_V(g) : V \to V$ preserves W for each $g \in G$.

Thus, $(W, \{\rho_V(g)|_W\})$ is another representation of G (since $\rho_V(g)$ is invertible on V, $\rho_V(g)|_W$ is invertible on W).

The zero subspace $\{0\} \subset V$ is a subrepresentation of V, but not a very interesting one.

Suppose that (V_1, ρ_1) and (V_2, ρ_2) are representations of a finite group G, and suppose that we have a homomorphism of representations $f : V_1 \to V_2$. Then we may again define its kernel and image:

$$\ker(f) := \{v \in V_1 : f(v) = 0\} \qquad \operatorname{im}(f) := \{f(v) \in V_2 : v \in V_1\}$$

Then $\ker(f)$ is a subrepresentation of V_1 and $\operatorname{im}(f)$ is a subrepresentation of V_2. Since both of these are vector subspaces, it is enough to prove that they are preserved by $\rho_1(g)$ and $\rho_2(g)$, respectively. But that follows from G-linearity of f.

We considered representations of C_2 earlier, and we defined a C_2-linear homomorphism $V_0 \to V_{\text{reg}}$ (where V_0 is equipped with the trivial representation). This homomorphism is injective, and its image is the vector subspace $\langle b_e + b_g \rangle \subset V_{\text{reg}}$. Thus, this is a subrepresentation of V_{reg}.

More generally, if (V, ρ_V) is a representation of a finite group G, a 1-dimensional subrepresentation of V is a 1-dimensional subspace $W = \langle w \rangle \subset V$ such that w is an eigenvector for every $\rho_V(g)$.

Definition 2.17. A representation (V, ρ_V) of G is *reducible* if there is a non-zero proper subrepresentation $W \subset V$, i.e., if $0 \neq W \neq V$. We say that V is *irreducible* if there is no such subrepresentation.

Example 2.18. Any 1-dimensional representation is irreducible.

Lemma 2.19. *If (V, ρ_V) is an irreducible representation of a finite group G, then it is indecomposable.*

Proof. Suppose that V is decomposable. Then $V \cong V_1 \oplus V_2$ with $V_1, V_2 \neq 0$ and there are representations $\rho_i : G \rightrightarrows \mathrm{GL}(V_i)$ such that $(V, \rho_V) \cong (V_1 \oplus V_2, \rho_1 \oplus \rho_2)$. But this implies that there are injective G-linear maps $f_i : V_i \to V \cong V_1 \oplus V_2$. Then $\operatorname{im}(f_1)$ and $\operatorname{im}(f_2)$ are subrepresentations of V, and they are non-zero because V_1 and V_2 were assumed non-zero. But since $\dim V = \dim V_1 + \dim V_2$, $\dim V_i \neq 0$ implies $\dim V_i < \dim V$ so $V_i \neq V$. Thus, $\operatorname{im}(f_1)$ and $\operatorname{im}(f_2)$ are non-zero proper subrepresentations of V. $\square$

In terms of matrices, we think of being decomposable as being able to choose a basis so that the matrix representation will have blocks down the diagonal and zeros elsewhere. We think of being decomposable as being able to choose a basis so that the matrix representation is upper-triangular except for blocks on the diagonal. For example, if (V, ρ_V) is a 3-dimensional representation with a 2-dimensional subrepresentation, we can find a basis of V so that $\rho_V(g) = \left(\begin{smallmatrix} * & * & * \\ * & * & * \\ 0 & 0 & * \end{smallmatrix}\right)$ for every $g \in G$.

Example 2.20. We give an example of an irreducible 2-dimensional representation of $S_3 \cong D_6$. Embed an equilateral triangle into $\mathbf{R}^2$ with vertices at $(1, 0)$, $(-1/2, \sqrt{3}/2)$, and $(-1/2, -\sqrt{3}/2)$. Then "counterclockwise rotation" and "reflection over the x-axis" generate D_3, so using the standard basis of $\mathbf{R}^2 \subset \mathbf{C}^2$, we get a homomorphism $\rho : D_6 \to \mathrm{GL}_2(\mathbf{R}) \subset \mathrm{GL}_2(\mathbf{C})$. The matrix for "counterclockwise rotation" is $\left(\begin{smallmatrix} -1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & -1/2 \end{smallmatrix}\right)$, and the matrix for "reflection over the x-axis" is $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$.

To see that this representation is irreducible, we need to check that these two matrices do not have a common eigenvector. But the eigenspaces of $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ are generated by $\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right)$, and they have different eigenvalues. Since neither of these is an eigenvector of $\left(\begin{smallmatrix} 1/2 & -\sqrt{3}/2 \\ -\sqrt{3}/2 & -1/2 \end{smallmatrix}\right)$, we are done.

2.6 Maschke's theorem

We can now start studying the structure of representations. Previously, we have defined direct sums of representations and decomposable representations, and we have defined subrepresentations and irreducible representations. We showed that irreducible representations are indecomposable. The goal for today is to show the converse:

Theorem 2.21 (Maschke's Theorem)**.** *If (V, ρ_V) is a reducible representation of a finite group G, then it is decomposable.*

The finiteness hypothesis on G is crucial here! If $G = \mathbf{Z}$, we may define a representation

$$\rho : G \to \mathrm{GL}_2(\mathbf{C}); \qquad \rho(n) := \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$$

Then the only non-zero proper subrepresentation is the one generated by $\langle \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) \rangle$. Thus, this representation is reducible but indecomposable.

We formalize this argument somewhat. Recall the following definition:

Definition 2.22. Let V be a finite-dimensional complex vector space, and let $W \subset V$ be a subspace. A *complement* of W is a subspace $W' \subset V$ such that the natural map $W \oplus W' \to V$, i.e., the map defined by $(w, w') \mapsto w + w'$, is an isomorphism.

Note that complements are not unique. In fact, any subspace $W' \subset V$ with $W \cap W' = \{0\}$ and $\dim W' = \dim V - \dim W$ is a complement of W.

We make a similar definition for representations:

Definition 2.23. Let (V, ρ_V) be a representation of a finite group G and let $W \subset V$ be a subrepresentation. A subrepresentation $W' \subset V$ is *complementary* to W if the natural map $W \oplus W' \to V$ given by $(w, w') \to w + w'$ induces an isomorphism of representations $\rho_W \oplus \rho_{W'} \xrightarrow{\sim} \rho_V$. That is, W' is complementary as a subspace, and is also a subrepresentation.

Thus, we can rephrase Maschke's theorem as the statement that if G is finite, every subrepresentation has a complementary representation. Before we prove it, we state a corollary:

Corollary 2.24. *Every finite-dimensional complex representation (V, ρ_V) of a finite group G is isomorphic to a direct sum*

$$V \cong V_1 \oplus V_2 \oplus \cdots \oplus V_r$$

where (V_i, ρ_i) is an irreducible representation of G.

Proof. This follows by induction on the dimension of V. If V is 1-dimensional, we have already seen that V is irreducible. Now let V be an arbitrary representation of G and suppose we know the result for all representations of dimension less than $\dim V$. Then V is either an irreducible representation, or $V \cong W \oplus W'$ for $\{0\} \neq W, W' \subsetneq V$ (as representations) by Theorem 2.21. But $\dim W, \dim W' < \dim V$ so W and W' are isomorphic to direct sums of irreducible representations. Therefore, V is also isomorphic to a direct sum of irreducible representations. □

We will prove Maschke's theorem by constructing complementary subrepresentations.

Lemma 2.25. *Let V be a finite-dimensional complex vector space and let $f : V \to V$ be a linear transformation such that $f \circ f = f$. Then $\ker(f) \subset V$ and $\operatorname{im}(f) \subset V$ are complementary subspaces.*

Let (V, ρ_V) be a representation of a finite group G and let $f : V \to V$ be a homomorphism of representations such that $f \circ f = f$. Then $\ker(f) \subset V$ and $\operatorname{im}(f)$ are complementary subrepresentations of V.

Proof. We have seen that $\ker(f)$ and $\operatorname{im}(f)$ are subspaces of V, and if V is a representation and f is G-linear, that they are subrepresentations. By the rank-nullity theorem, $\dim \ker(f) + \dim \operatorname{im}(f) = \dim V$, so it suffices to show that $\ker(f) \cap \operatorname{im}(f) = \{0\}$. So choose some $v \in \ker(f) \cap \operatorname{im}(f)$, so that $v = f(v')$ and $f(v) = 0$. But we assumed $f \circ f = c$, so

$$0 = f(v) = f(f(v')) = f(v') = v$$

Thus, $v = 0$, as desired. □

Given a finite-dimensional vector space V and a subspace $W \subset V$, any linear transformation $f : V \to W$ with $f|_W = \mathrm{id}$ is an example of a map as in the lemma. We call this a *projection* from V to W. We can build a projection explicitly as follows: Choose a basis $\mathcal{B}_V = (w_1, \ldots, w_{d_W}, v_{d_W+1}, \ldots, v_{d_V})$ with $\mathcal{B}_W = (w_1, \ldots, w_{d_W})$ a basis for W. Then we define $f : V \to W$ to be the linear transformation associated to the matrix

$$\begin{pmatrix} \mathrm{Id}_{d_W} & 0 \\ 0 & 0 \end{pmatrix}$$

where the upper-left is the identity $d_W \times d_W$ matrix, and there are zeros everywhere else.

We see that it is not hard to construct complementary subspaces, but we need to construct complementary subspaces that are also preserved by G. For this, we need a way to construct G-linear projections.

Definition 2.26. Let V, W be finite-dimensional complex vector spaces. We define

$$\mathrm{Hom}(V, W) := \{f : V \to W : f \mathrm{isalineartransformation}\}$$

Since we can add and subtract linear transformations and scale them by complex numbers, $\mathrm{Hom}(V, W)$ is again a finite-dimensional vector space, of dimension $\dim V \cdot \dim W$.

If V and W are additionally representations of a finite group G, we can make $\mathrm{Hom}(V, W)$ into a representation of G:

Definition 2.27. Let (V, ρ_V) and (W, ρ_W) be finite-dimensional complex representations of a finite group G. We define an action of G on $\mathrm{Hom}(V, W)$ by setting $g \cdot f : V \to W$ to be $(g \cdot f)(v) = (\rho_W(g) \circ f \circ \rho_V(g^{-1}))(v)$ for all $g \in G$, $v \in V$.

It is straightforward to check that for each g, this is a linear transformation $\mathrm{Hom}(V, W) \to \mathrm{Hom}(V, W)$.

Note that we do not require elements of $\mathrm{Hom}(V, W)$ to be G-linear, even when V and W are representations of G. In fact,

Lemma 2.28. *A linear transformation $f : V \to W$ is G-linear if and only if $g \cdot f = f$.*

Proof. Exercise. □

Given a representation (V, ρ_V), the subset $V^G := \{v \in G : \rho_V(g)(v) = v \mathrm{forall} g \in G\}$ is a trivial subrepresentation of V. Thus, the inclusion $V^G \to V$ is a G-linear map. We can also define a G-linear homomorphism the other way:

Lemma 2.29. *Define $e : V \to V^G$ by setting $e(v) := \frac{1}{|G|} \sum_{g \in G} \rho_V(g)(v)$ is G-linear. In addition, it satisfies $e \circ e = e$.*

Proof. We first check that for any $v \in V$, $e(v) \in V^G$. Let $g' \in G$. Then

$$\rho_V(g')(e(v)) = \frac{1}{|G|}\sum_{g\in G}\rho_V(g')\rho_V(g)(v) = \frac{1}{|G|}\sum_{g\in G}\rho_V(g'g)(v) = \frac{1}{|G|}\sum_{g\in G}\rho_V(g)(v)$$

where the last equality follows because the set $\{g'g\}_{g\in G} = G$.

Furthermore, if $v \in V^G$, then

$$e(v) = \frac{1}{|G|}\sum_{g\in G}\rho_V(g)(v) = \frac{1}{|G|}\sum_{g\in G} v = \frac{1}{|G|}\cdot|G|\cdot v = v$$

Thus, $e : V \to V^G$ is the identity on V^G, so $e \circ e = e$.

It remains to check that e is G-linear. The first two parts of this proof imply that $\rho_V(g')(e(v)) = e(v)$ for all $g' \in G$ and all $v \in V$, so we need to show that $e(\rho_V(g')v) = e(v)$ for all $g' \in G$ and all $v \in V$. But

$$e(\rho_V(g)v) = \frac{1}{|G|}\sum_{g\in G}\rho_V(g)(\rho_V(g')v) = \frac{1}{|G|}\sum_{g\in G}\rho_V(gg')(v) = \frac{1}{|G|}\sum_{g\in G}\rho_V(g)(v) = e(v)$$

where we use again that $\{gg'\}_{g\in G} = G$. □

of 2.21. Let (V, ρ_V) be a representation of a finite group G, and let W be a subrepresentation. Choose a projection (of vector spaces, not representations) $\widetilde{f} : V \to W$. There is no reason for $\widetilde{f}$ to be G-linear, so we modify it.

Define $f : V \to W$ by setting

$$f := e(f) = \frac{1}{|G|}g \cdot f$$

We can write f down more explicitly, by unwinding the definition of the action of G on $\mathrm{Hom}(V, W)$:

$$f(v) = \frac{1}{|G|}\sum_{g\in G}(\rho_V(g) \circ \widetilde{f} \circ \rho_V(g^{-1}))(v)$$

By construction, $f \in \mathrm{Hom}(V, W)^G$, so f is G-linear.

We need to check further that $f|_W : W \to W$ is the identity map. But if $w \in W$, then $\rho_V(g^{-1})(w) \in W$ since the action of G preserves W. We also chose $\widetilde{f} : V \to W$ to be the identity on W, so

$$f(w) = \frac{1}{|G|}\sum_{g\in G}(\rho_V(g) \circ \widetilde{f} \circ \rho_V(g^{-1}))(w) = \frac{1}{|G|}\sum_{g\in G}\rho_V(g)(\rho_V(g^{-1})(w)) = \frac{1}{|G|}\sum_{g\in G} w = w$$

as desired.

Finally, we set $W' := \ker(f)$. Since f is G-linear, this is a subrepresentation of V complementary to $\mathrm{im}(f)$. Since $f \circ f = f$ and $\mathrm{im}(f) = W$, W and W' are complementary subrepresentations of V and we are done. □

2.7 Schur's lemma

Now that we have shown that representations of finite groups can be decomposed as the direct sum of irreducible representations, we wish to study homomorphisms between irreducible representations in more detail. The key result is the following:

Theorem 2.30 (Schur's Lemma)**.** *Let (V, ρ_V) and (W, ρ_W) be irreducible finite-dimensional complex representations of a finite group G.*

1. *If $f : V \to W$ is G-linear, then f is either 0 or an isomorphism.*

2. *Let $f : V \to V$ be a G-linear map. Then $f = \lambda \mathbf{1}_V$ for some $\lambda \in \mathbf{C}$. That is, f is multiplication by a scalar.*

Proof. 1. Recall that if f is G-linear, both $\ker(f) \subset V$ and $\operatorname{im}(f) \subset W$ are subrepresentations. Since V and W are assumed irreducible, we must have either $\ker(f) = \{0\}$ (in which case f is injective) or $\ker(f) = V$ (in which case $f = 0$), and we must have either $\operatorname{im}(f) = 0$ (in which case $f = 0$) or $\operatorname{im}(f) = W$ (in which case f is surjective). So either $f = 0$ or f is both injective and surjective, i.e., an isomorphism.

2. Certainly for any $\lambda \in \mathbf{C}$, $\lambda \mathbf{1}_V : V \to V$ is G-linear. Now for any $\lambda \in \mathbf{C}$ and any G-linear $f : V \to V$, consider the linear transformation $\lambda \mathbf{1}_V - f : V \to V$. This is clearly G-linear as well, so either $\lambda \mathbf{1}_V - f = 0$ or $\lambda \mathbf{1}_V - f$ is an isomorphism. But $\lambda \mathbf{1}_V - f$ fails to be an isomorphism if and only if λ is a root of the characteristic polynomial of the matrix representing f (with respect to some basis of V). Since any polynomial over $\mathbf{C}$ of degree d has d (not necessarily distinct) roots, there is some $\lambda \in \mathbf{C}$ such that $f = \lambda \mathbf{1}_V$.

□

We can use Schur's lemma to classify representations of finite abelian groups:

Lemma 2.31. *Let G be a finite abelian group and let (V, ρ_V) be a finite-dimensional complex representation. For any $g \in G$, $\rho_V(g) : V \to V$ is a G-linear homomorphism.*

Proof. We need to check that for any $g' \in G$, $\rho_V(g') \circ \rho_V(g) = \rho_V(g) \circ \rho_V(g')$. But this follows because G is abelian. □

Corollary 2.32. *Let (V, ρ_V) be a non-zero irreducible finite-dimensional complex representation of a finite abelian group G. Then V is 1-dimensional.*

Proof. For each element $g \in G$, $\rho_V(g) : V \to V$ is G-linear. Since V is irreducible, Theorem 2.30 implies that there is some $\lambda_g \in \mathbf{C}$ such that $\rho_V(g) = \lambda \mathbf{1}_V$. But this implies that every element of V is an eigenvector for every $\rho_V(g)$, and therefore generates a 1-dimensional subrepresentation of V. But this contradicts the irreducibility of V unless V is itself 1-dimensional. □

3 Uniqueness of decomposition

Now that we have Schur's lemma, we are almost ready to prove that the decomposition of representations into irreducibles ("irreps") is unique. That is, we would like to prove

Theorem 3.1. *Let (V, ρ_V) be a finite-dimensional complex representation of a finite group G, and let $V \cong V_1 \oplus \cdots \oplus V_r$ and $V \cong V_1' \oplus \cdots \oplus V_{r'}'$ be two decompositions of V into irreducible subrepresentations. Then $r = r'$ and the decompositions are the same, up to reordering the irreducible subrepresentations.*

Proof. We first show that for each i, one of the V_j' is isomorphic to V_i. This shows that the sets of irreducible subrepresentations are the same. Let $e_j : V \to V_j'$ denote projection to the jth factor; this is G-linear by construction, and $e_1 + \ldots + e_{r'} : V \to V$ is the identity map. Now by assumption, there is a non-zero G-linear map $f_i : V_i \to V$, so $(e_1 + \cdots + e_{r'}) \circ f_i$ is non-zero and G-linear. If each $e_j \circ f_i$ were zero, their sum would be, as well (since the images of the e_j are linearly independent). Thus, there is some non-zero G-linear map $e_j \circ f_i : V_i \to V_j'$, and since V_j' is irreducible, it must be an isomorphism.

We rewrite our two decompositions as $V \cong \oplus_i V_i^{r_i}$ and $V \cong \oplus_i V_i^{s_i}$, where the V_i are distinct irreducible representations of G. We need to prove that $r_i = s_i$ for all i. But for any j,

$$\mathrm{Hom}(V_j, \oplus_i V_i^{r_i})^G \cong \mathbf{C}^{r_j}$$

and similarly

$$\mathrm{Hom}(V_j, \oplus_i V_i^{s_i})^G \cong \mathbf{C}^{s_j}$$

Thus, $r_j = s_j$ for all j. $\square$

We need to say a bit more about homomorphisms of representations first.

Lemma 3.2. *Let V, V', and W be vector spaces. Then we have natural isomorphisms*

1. $\mathrm{Hom}(W, V \oplus V') \cong \mathrm{Hom}(W, V) \oplus \mathrm{Hom}(W, V')$
2. $\mathrm{Hom}(V \oplus V', W) \cong \mathrm{Hom}(V, W) \oplus \mathrm{Hom}(V', W)$

If V, V', and W carry representations of a finite group G, these are isomorphisms of representations.

Proof. First of all, note that all of these spaces are complex vector spaces with dimension $\dim W \cdot (\dim V + \dim V')$. Second, recall that we have homomorphisms

$$V \underset{e_V}{\overset{i_V}{\rightleftarrows}} V \oplus V' \underset{i_{V'}}{\overset{e_{V'}}{\rightleftarrows}} V'$$

given by

$$i_V(v) = (v, 0); \qquad e_V(v, v') = v; \qquad i_{V'}(v') = (0, v'); \qquad e_{V'}(v, v') = v'$$

It follows that $i_V \circ e_V + i_{V'} \circ e_{V'} = \mathbf{1} : V \oplus V' \to V \oplus V'$. Moreover, if V, V', and W are representations, all four of these maps are G-linear.

1. To define a linear transformation $P : \mathrm{Hom}(W, V \oplus V') \to \mathrm{Hom}(W, V) \oplus \mathrm{Hom}(W, V')$, we choose $f \in \mathrm{Hom}(W, V \oplus V')$. Then $e_V \circ f \in \mathrm{Hom}(W, V)$ and $e_{V'} \circ f \in \mathrm{Hom}(W, V')$, and we send f to $(e_V \circ f, e_{V'} \circ f) \in \mathrm{Hom}(W, V) \oplus \mathrm{Hom}(W, V')$. On the other hand, given $(h, h') \in \mathrm{Hom}(W, V) \oplus \mathrm{Hom}(W, V')$, we may define $Q(h, h')\,\mathrm{Hom}(W, V \oplus V')$ via $Q(g, g') := i_V \circ g + i_{V'} \circ g'$. Composing these two linear transformations, we see

   $$(Q \circ P)(f) = i_V \circ (e_V \circ f) + i_{V'}(e_{V'} \circ f) = \mathbf{1}_{V \oplus V'} \circ f = f$$

   Therefore, our map $\mathrm{Hom}(W, V \oplus V') \to \mathrm{Hom}(W, V) \oplus \mathrm{Hom}(W, V')$ is injective. Since both sides are vector spaces of the same dimension, this implies that our map is an isomorphism.

   We need to check that if V, V', and W are representations of G, then this isomorphism is G-linear. Recall that if $g \in G$, then $\rho_{\mathrm{Hom}(W, V \oplus V')}(f) = \rho_{V \oplus V'}(g) \circ f \circ \rho_W(g^{-1})$. Then

   $$\begin{aligned} P(\rho_{\mathrm{Hom}(W,V\oplus V')}(f)) &= P(\rho_{V\oplus V'}(g) \circ f \circ \rho_W(g^{-1})) \\ &= (e_V \circ (\rho_{V\oplus V'}(g) \circ f \circ \rho_W(g^{-1})), e_{V'} \circ (\rho_{V\oplus V'}(g) \circ f \circ \rho_W(g^{-1}))) \\ &= (\rho_V(g) \circ e_V \circ f \circ \rho_W(g^{-1}), \rho_{V'}(g) \circ e_{V'} \circ f \circ \rho_W(g^{-1})) \\ &= (\rho_{\mathrm{Hom}(W,V)}(g)(e_V \circ f), \rho_{\mathrm{Hom}(W,V')}(g)(e_{V'} \circ f)) \\ &= \rho_{\mathrm{Hom}(W,V)\oplus\mathrm{Hom}(W,V')}(g)(e_V \circ f, e_{V'} \circ f) \\ &= \rho_{\mathrm{Hom}(W,V)\oplus\mathrm{Hom}(W,V')}(g) \circ P(f) \end{aligned}$$

   so P is G-linear.

2. To define a linear transformation $S : \mathrm{Hom}(V \oplus V', W) \to \mathrm{Hom}(V, W) \oplus \mathrm{Hom}(V', W)$, we choose $f \in \mathrm{Hom}(V \oplus V', W)$. Then $f \circ i_V \in \mathrm{Hom}(V, W)$ and $f \circ i_{V'} \in \mathrm{Hom}(V', W)$, and we send f to $(f \circ i_V, f \circ i_{V'}) \in \mathrm{Hom}(V, W) \oplus \mathrm{Hom}(V', W)$. On the other hand, given $(h, h') \in \mathrm{Hom}(V, W) \oplus \mathrm{Hom}(V', W)$, $g \circ e_V, g' \circ e_{V'} \in \mathrm{Hom}(V \oplus V', W)$, so we may define a linear transformation $T : \mathrm{Hom}(V, W) \oplus \mathrm{Hom}(V', W) \to \mathrm{Hom}(V \oplus V', W)$ by sending $(g, g') \mapsto g \circ e_V + g' \circ e_{V'}$. Composing these two maps, we see

   $$(f \circ i_V) \circ e_V + (f \circ i_{V'}) \circ e_{V'} = f \circ \mathbf{1}_{V \oplus V'} = f$$

   Therefore, our map $\mathrm{Hom}(V \oplus V', W) \to \mathrm{Hom}(V, W) \oplus \mathrm{Hom}(V', W)$ is injective, and since the two vector spaces have the same dimension, it is an isomorphism.

We need to check that S is G-linear when our vector spaces are representations. Indeed,

$$\begin{aligned} S(\rho_{\mathrm{Hom}(V\oplus V'),W}(g)(f)) &= S(\rho_W(g)\circ f\circ \rho_{V\oplus V'}(g^{-1})) \\ &= (\rho_W(g)\circ f\circ \rho_{V\oplus V'}(g^{-1})\circ i_V, \rho_W(g)\circ f\circ \rho_{V\oplus V'}(g^{-1})\circ i_{V'}) \\ &= (\rho_W(g)\circ f\circ i_V\circ \rho_V(g^{-1}), \rho_W(g)\circ f\circ i_{V'}\circ \rho_{V'}(g^{-1})) \\ &= (\rho_{\mathrm{Hom}(V,W)}(g)(f\circ i_V), \rho_{\mathrm{Hom}(V',W)}(g)(f\circ i_{V'}) \\ &= \rho_{\mathrm{Hom}(V,W)\oplus \mathrm{Hom}(V',W)}(g)(f\circ i_V, f\circ i_{V'} \\ &= \rho_{\mathrm{Hom}(V,W)\oplus \mathrm{Hom}(V',W)}(g)\circ S(f) \end{aligned}$$

so S is G-linear, as desired.

□

3.1 The Regular Representation

Let G be a finite group. Recall the definition of the regular representation of G: V_{reg} has a basis $\{b_g\}_{g\in G}$ indexed by elements of G, and the action of G is given by $\rho_{\mathrm{reg}}(g')(b_g) = b_{g'g}$. We wish to study the decomposition of V_{reg} into irreducible representations. We can say more:

Theorem 3.3. *Let $V_{\mathrm{reg}} \cong V_1 \oplus \cdots V_r$ be the decomposition of the regular representation into irreducible subrepresentations. Then if W is an irreducible representation of G, the number of V_i isomorphic to W is $\dim W$.*

This has an important consequence:

Corollary 3.4. *A finite group G has only finitely many irreducible representations, up to isomorphism, and they all have dimension at most $|G|$.*

It also has a numerical consequence:

Corollary 3.5. $|G| = \sum_W (\dim W)^2$*, where the sum runs over the irreducible representations of G.*

This lets us sharpen the previous corollary, because it implies that the irreducible representations have dimension at most $\sqrt{|G|}$.

Example 3.6. Consider $G = S_3$. We can write down all of its irreducible representations. We saw on the first problem sheet that the 3-dimensional permutation representation is the direct sum of the trivial representation and a 2-dimensional representation. Since the permutation does not contain any non-trivial 1-dimensional representation, this 2-dimensional representation is irreducible. There is another 1-dimensional representation of S_3, namely the *sign representation*, which sends each transposition to -1. So we have two 1-dimensional representations and one irreducible 2-dimensional representation. Since $|S_3| = 6 = 1^2 + 1^2 + 2^2$, we have found every irreducible representation of S_3.

Example 3.7. Let $G = D_8$. On the first problem sheet, you found that there are four 1-dimensional representations of D_8. If $V_{\text{reg}} \cong V_1^{\oplus d_1} \oplus \cdots \oplus V_r^{\oplus d_r}$ with $d_i = \dim V_i$, then we have $8 = d_1^2 + \ldots + d_r^2$. The only solutions to this equation (with $d_i \geq 1$ and $d_i \in \mathbf{N}$) are for $r = 8$ and $d_i = 1$, $r = 2$ and $d_i = 2$, and $r = 5$ with one $d_i = 2$ and the rest equal to 1. Since there are exactly four 1-dimensional representations, the last is the case.

Lemma 3.8. *Let W be an irreducible representation of G. Define the* evaluation map $\text{ev} : \text{Hom}(V_{\text{reg}}, W)^G \to W$ *via* $f \mapsto f(b_e)$*. This map is an isomorphism.*

Proof. First we prove that ev is injective. So suppose that $\text{ev}(f) = f(b_e) = 0$ for some $f \in \text{Hom}(V_{\text{reg}}, W)^G$. But then$f : V_{\text{reg}} \to W$ is G-linear, so $f(b_g) = f(\rho_{\text{reg}}(g)b_e) = \rho_W(g)f(b_e) = 0$ for all $g \in G$, so $f = 0$.

Now we prove that this map is surjective. Choose some $w \in W$; we will construct a G-linear $f : V_{\text{reg}} \to W$ with $f(b_e) = w$. But it is enough to specify $f(b_g)$ for all $g \in G$, so we set $f(b_g) := \rho_W(g)(w)$ and extend by linearity. We check that f is G-linear: for $g' \in G$ and $\{a_g\}_{g \in G}$,

$$(f \circ \rho_{\text{reg}}(g'))(b_g) = f(b_{g'g}) = \rho_W(g'g)(w)$$
$$(\rho_W(g') \circ f)(b_g) = \rho_W(g')(\rho_W(g)(w)) = \rho_W(g'g)(w)$$

Since the two maps agree on basis vectors, they are the same. □

4 Duals and Tensor Products

Recall the following definition:

Definition 4.1. Let V be a vector space. The *dual vector space* is $V^* := \text{Hom}(V, \mathbf{C})$.

This is a special case of the construction $\text{Hom}(V, W)$, with $W = \mathbf{C}$. It is clear that $\dim V^* = \dim V$; in fact, if we choose a basis $(v_1, \ldots, v_d)$ for V, we may define a *dual basis* $(f_1, \ldots, f_d)$, where

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

Suppose that (V, ρ_V) is a representation of G. Then we have defined a representation (V^*, ρ_V^*) by setting

$$\rho_V^*(g) := \rho_{\text{Hom}(V,\mathbf{C})}(g) : f \mapsto f \circ \rho_V(g^{-1})$$

We call this the *dual representation.*

Lemma 4.2. *Let V be a finite-dimensional vector space. Then there is a map $h : V \to (V^*)^*$, defined by letting $h(v)$ be the linear map $h(v) : V^* \to \mathbf{C}$ with $h(v)(f) = f(v)$. If V is a representation of a finite group G, then this isomorphism is G-linear.*

Example 4.3. Let $\rho : G \to \mathrm{GL}_1(\mathbf{C})$ be a 1-dimensional matrix representation. If we write down ρ^*, we get

$$\rho^*(g)(f) = f \circ \rho_V(g^{-1})) = \rho_V(g^{-1}) \cdot f$$

since $\rho^*(g^{-1})$ is just multiplication by a scalar. So the matrix for ρ^* (with respect to any basis of $\mathbf{C}$) is ρ^{-1}.

We wish to consider dual matrix representations more generally. We may choose a basis for V and view it as the set of column vectors of length d; then V^* is the set of row vectors of length d.

Proposition 4.4. *Let (V, ρ_V) be a representation of G, let $\mathcal{B}$ be a basis of V, and let $\mathcal{B}^*$ be the dual basis for V^*. Then the matrix representation $\rho^*_{V,\mathcal{B}^*} : G \to \mathrm{GL}_d(\mathbf{C})$ is given by $\rho^*_{V,\mathcal{B}^*}(g) = (\rho_V(g)^{-1})^t$, where the t refers to taking the transpose.*

Proof. Let $\mathcal{B} = (v_1, \dots, v_d)$ and let $\mathcal{B}^* = (f_1, \dots, f_d)$. Then for any $g \in G$, if $\rho_{V,\mathcal{B}}(g^{-1}) = (g_{kj})$,

$$\rho^*_{V,\mathcal{B}^*}(g)(f_i)(v_j) = f_i(\rho_V(g^{-1})(v_j)) = f_i(\sum_{k=1}^{d} g_{kj} v_k) = g_{ij}$$

It follows that $\rho^*_{V,\mathcal{B}^*}(g)(f_i) = \sum_j g_{ij} f_j$. □

Proposition 4.5. *A representation (V, ρ_V) is irreducible if and only if (V^*, ρ^*_V) is irreducible.*

Proof. Suppose $V \cong W \oplus W'$, where W, W' are also representations. Then $V^* = \mathrm{Hom}(V, \mathbf{C}) \cong \mathrm{Hom}(W, \mathbf{C}) \oplus \mathrm{Hom}(W', \mathbf{C})$, so V^* is also decomposable (since $\dim W^* = \dim W$ and $\dim W'^* = \dim W'$). Since $(V^*)^* \cong V$ via a G-linear isomorphism, the same argument shows that if V^* is reducible, so is V. □

Thus, given an irreducible representation of G, we may take its dual to obtain another one. However, V^* may very well be isomorphic to V. For example, consider the 2-dimensional irreducible representation (V_2, ρ_2) of S_3. Explicitly, $\rho_2(123) = \begin{pmatrix} -1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & -1/2 \end{pmatrix}$ and $\rho_2(23) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. But these matrices are equal to their own inverse transposes, so $V = V^*$.

Now we turn to tensor products. They can be fairly abstract, but we will give a more hands-on discussion.

Definition 4.6. Let V and W be finite-dimensional complex vector spaces with bases $(v_1, \dots, v_{d_V})$ and $(w_1, \dots, w_{d_W})$, respectively. Then we define $V \otimes W$ to be the vector space with basis given by the symbols $\{v_i \otimes w_j\}$. It has dimension $d_V \cdot d_W$.

If $v = \sum_i a_i v_i$ and $w = \sum_j b_j w_j$, we define $v \otimes w := \sum_{i,j} a_i b_j (v_i \otimes w_j)$. Be careful: not every element of $V \otimes W$ is of the form $v \otimes w$.

If (V, ρ_V) and (W, ρ_W) are representations of G, we can also define a representation $(V \otimes W, \rho_{V \otimes W})$:

Definition 4.7. For $g \in G$, we define $\rho_{V\otimes W}(g) : V \otimes W \to V \otimes W$ by setting $\rho_{V\otimes W}(g)(v_i \otimes w_t) := \rho_V(g)(v_i) \otimes \rho_W(g)(w_t)$.

If $\rho_V(g)$ has matrix M and $\rho_W(g)$ has matrix N (with respect to the chosen bases), then $\rho_{V\otimes W}(g)$ sends

$$\begin{aligned} v_i \otimes w_t \mapsto & \left(\sum_{j=1}^{d_V} M_{ji} v_j\right) \otimes \left(\sum_{s=1}^{d_W} N_{st} w_s\right) \\ &= \sum_{j,s} M_{ji} N_{st} v_j \otimes w_s \end{aligned}$$

So in terms of matrices, $\rho_{V\otimes W}(g)$ is given by a $d_V d_W \times d_V d_W$ matrix we call $M \otimes N$, whose entries are $[M \otimes N]_{(j,s),(s,t)} = M_{ji} N_{st}$.

We have given a construction in terms of bases, but we would like to know that if we change our choice of bases of V and W, we get an equivalent representation. Fortunately, we can give another description of $V \otimes W$:

Proposition 4.8. *The vector space $V \otimes W$ is isomorphic to* $\mathrm{Hom}(V^*, W)$*. If V and W are representations of G, there is a G-linear isomorphism.*

Proof. Let $(f_1, \ldots, f_{d_V})$ be the dual basis for V^*. Then we define $h_{it} : V^* \to W$ by setting $h_{ti}(f_i) = w_t$, and $h_{ti}(f_j) = 0$ if $i \neq j$; the set $\{h_{it}\}$ forms a basis for $\mathrm{Hom}(V^*, W)$. Concretely, $\mathrm{Hom}(V^*, W)$ can be viewed as the vector space of $d_W \times d_V$ matrices, and h_{ti} corresponds to the linear transformation with a 1 in the (t, i)-entry and 0s elsewhere.

Now we define a linear transformation $\mathrm{Hom}(V^*, W) \to V \otimes W$ via $h_{ti} \mapsto v_i \otimes w_t$. This is clearly an isomorphism, because $\mathrm{Hom}(V^*, W)$ and $V \otimes W$ have the same dimension, and we are simply sending basis vectors to distinct basis vectors.

It remains to check that this linear transformation is G-linear. It is enough to compute the matrix representing $\rho_{\mathrm{Hom}(V^*,W)}(g)$ with respect to $\{h_{ti}\}$. Suppose that $\rho_V(g)$ is represented by the matrix M (with respect to the chosen basis). Recall also that $\rho_{\mathrm{Hom}(V^*,W)}(g)$ acts via $h_{ti} \mapsto \rho_W(g) \circ h_{ti} \circ \rho_{V^*}(g^{-1})$. Moreover, the matrix for $\rho_{V^*}(g^{-1})$ with respect to $\{f_i\}$ is given by M^t, so $\rho_{V^*}(g^{-1})$ sends $f_k \mapsto \sum_j M_{kj} f_j$. So $h_{ti} \circ \rho_{V^*}(g^{-1})$ sends $f_k \mapsto M_{ki} w_t$. If $\rho_W(g)$ is represented by the matrix N (with respect to $\{w_s\}$), then $\rho_W(g) \circ h_{ti} \circ \rho_{V^*}(g^{-1})$ sends $f_k \mapsto M_{ki} \left(\sum_j N_{st} w_s\right)$.

It follows that $\rho_{\mathrm{Hom}(V^*,W)}(g)$ sends h_{ti} to $\sum_{j,s} M_{ji} N_{st} h_{sj}$, which is the formula we wrote down for $\rho_{V^*\otimes W}(g)$. □

Example 4.9. Suppose that V is 1-dimensional, so that $\rho_V(g)$ is just multiplication by a scalar λ_g, for every $g \in G$. Then if the matrix representing $\rho_W(g)$ with respect to some basis is N_g, the matrix representing $\rho_{V\otimes W}(g)$ is $\lambda_g N_g$.

In particular, if V and W are both 1-dimensional, tensoring the representations simply multiplies them.

Suppose $G = S_n$, and ρ_V and ρ_W are both the sign representation. Then $\rho_{V\otimes W}$ is the trivial representation.

5 Character theory

5.1 Definitions and basic properties

There are two definitions of the word "character" you might come across in representation theory. The first is that a character is a 1-dimensional representation. We will not use this terminology in this course, to avoid confusion.

Definition 5.1. Let $M = (M_{ij})$ be a $d \times d$ matrix. Then the *trace* of M is $\mathrm{Tr}(M) = \sum_i M_{ii}$ (the sum of the diagonal entries).

If $f : V \to V$ is a linear transformation, we choose a basis $\mathcal{B}$ of V, and define $\mathrm{Tr}(f) := \mathrm{Tr}([f]_{\mathcal{B}})$.

Recall that if M, N are $d \times d$ matrices, then $\mathrm{Tr}(MN) = \mathrm{Tr}(NM)$. As a result, if $P \in \mathrm{GL}_d(\mathbf{C})$ is invertible, then $\mathrm{Tr}(PMP^{-1}) = \mathrm{Tr}(M)$. Thus, the trace of a linear transformation is independent of the chosen basis.

Definition 5.2. Let (V, ρ_V) be a finite-dimensional complex representation of a finite group G. The *character* associated to (V, ρ_V) is the function $\chi_V : G \to \mathbf{C}$ given by $\chi_V(g) = \mathrm{Tr}(\rho_V(g))$.

This is generally *not* a homomorphism, because traces are not multiplicative.

Example 5.3. If (V, ρ_V) is a 1-dimensional representation of G, then $\chi_V(g) = \rho_V(g)$ for all $g \in G$.

Example 5.4. Let (V, ρ_V) be the irreducible 2-dimensional representation of S_3. Then $\chi_V(1) = 2$, $\chi_V(123) = -1$, and $\chi_V(23) = 0$.

Lemma 5.5. *Let (V, ρ_V) be a representation of G. Then for all $g, h \in G$, $\chi_V(hgh^{-1}) = \chi_V(g)$.*

Proof. Since $\rho_V(h)$ is invertible,

$$\chi_V(hgh^{-1}) = \mathrm{Tr}(\rho_V(h)\rho_V(g)\rho_V(h^{-1}) = \mathrm{Tr}(\rho_V(g)) = \chi_V(g)$$

□

Since (12) and (13) are conjugate to (23), and (132) is conjugate to (123), in the previous example we actually know all values of χ_V.

Lemma 5.6. *Suppose (V, ρ_V) and (W, ρ_W) are isomorphic representations of a finite group G. Then $\chi_V = \chi_W$.*

Proof. We choose bases $\mathcal{B}_V$ and $\mathcal{B}_W$ for V and W, respectively. This choice of bases gives us corresponding matrix representations $\rho_{V,\mathcal{B}_V}, \rho_{W,\mathcal{B}_W} : G \rightrightarrows \mathrm{GL}_d(\mathbf{C})$. Since our representations are isomorphic, there is some matrix $P \in \mathrm{GL}_d(\mathbf{C})$ such that $\rho_{V,\mathcal{B}_V}(g) = P\rho_{W,\mathcal{B}_W}(g)P^{-1}$ for all $g \in G$. $\square$

We are going to prove the converse, that is, that if (V, ρ_V) and (W, ρ_W) are representations of G such that $\chi_V = \chi_W$, then $(V, \rho_V) \cong (W, \rho_W)$.

Proposition 5.7. *Let (V, ρ_V) be a representation of G.*

1. $\chi_V(e) = \dim V$
2. $\chi_V(g^{-1}) = \overline{\chi(g)}$ *(where the bar refers to complex conjugation)*
3. *For all $g \in G$, $|\chi_V(g)| \leq \dim(V)$, with equality if and only if $\rho_V(g) = \lambda \mathbf{1}$ for some $\lambda \in \mathbf{C}$.*

Proof.

1. Since $\rho_V(e) = \mathbf{1}$, $\chi_V(e) = \mathrm{Tr}(\mathbf{1}) = \dim V$.
2. Since $\rho_V(g)$ is an invertible matrix with finite order (if $g^n = e$, then $\rho_V(g)^n = \mathbf{1}$), we can choose a basis $\mathcal{B}$ of V so that the associated matrix $\rho_{V,\mathcal{B}}(g)$ is a diagonal matrix, with diagonal entries $\lambda_1, \ldots, \lambda_d$. The λ_i must be roots of unity, so $\lambda^{-1} = \overline{\lambda}_i$. Thus, $\rho_{V,\mathcal{B}}(g^{-1})$ is also a diagonal matrix, with entries $\overline{\lambda}_1, \ldots, \overline{\lambda}_d$. It follows that
$$\chi_V(g^{-1}) = \lambda_1^{-1} + \ldots + \lambda_d^{-1} = \overline{\lambda}_1 + \ldots + \overline{\lambda}_d = \overline{\chi_V(g)}$$
3. We may again write $\chi_V(g) = \lambda_1 + \ldots + \lambda_d$, where the λ_i are roots of unity. By the triangle inequality,
$$|\chi_V(g)| \leq \sum_i |\lambda_i| = d$$
so $|\chi_V(g)| \leq \dim V$. We have equality if and only if $\lambda_i = r_i e^{i\theta}$ for a single argument $\theta \in [0, 2\pi)$ and $r_i \in \mathbf{R}$. Since the λ_i all have absolute value 1, $r_i = 1$ for all i, so we have the desired equality if and only if $\lambda_1 = \lambda_2 = \ldots = \lambda_d$, in which case $\rho_V(g)$ is multiplication by a scalar.

$\square$

Corollary 5.8. *If (V, ρ_V) is a representation of G, then $\rho_V(g) = \mathbf{1}$ if and only if $\chi_V(g) = \dim V$.*

Proof. It is clear that if $\rho_V(g) = \mathbf{1}$, then $\chi_V(g) = \dim V$.

If $\chi_V(g) = \dim V$, then $|\chi_V(g)| = \dim V$, so the previous proposition implies that $\rho_V(g)$ is multiplication by $\lambda \in \mathbf{C}$. Then $\chi_V(g) = \lambda \cdot \dim V$, and if $\chi_V(g) = \dim V$ we must have $\lambda = 1$. $\square$

Thus, the character of a representation detects whether or not a representation is faithful.

Proposition 5.9. *Let (V, ρ_V) and (W, ρ_W) be representations of G.*

1. $\chi_{V \oplus W}(g) = \chi_V(g) + \chi_W(g)$
2. $\chi_{V \otimes W}(g) = \chi_V(g)\chi_W(g)$
3. $\chi_{V^*}(g) = \overline{\chi_V(g)}$
4. $\chi_{\mathrm{Hom}(V,W)}(g) = \overline{\chi_V(g)}\chi_W(g)$

Proof. Choose bases for V and W, and let M and N be the matrices associated to $\rho_V(g)$ and $\rho_W(g)$, respectively.

1. The matrix for $(\rho_V \oplus \rho_W)(g)$ with respect to the chosen bases is the block-diagonal matrix
$$\begin{pmatrix} M & 0 \\ 0 & N \end{pmatrix}$$
so $\chi_{V \oplus W}(g) = \mathrm{Tr}\left(\begin{smallmatrix} M & 0 \\ 0 & N \end{smallmatrix}\right) = \mathrm{Tr}(M) + \mathrm{Tr}(N) = \chi_V(g) + \chi_W(g)$.
2. The matrix $M \otimes N$ has entries $[M \otimes N]_{(j,s),(i,t)} = M_{ji}N_{st}$, so its trace is
$$\mathrm{Tr}(M \otimes N) = \sum_{i,t} [M \otimes N]_{(i,t),(i,t)} = \sum_{i,t} M_{ii}N_{tt} = \mathrm{Tr}(M)\,\mathrm{Tr}(N)$$
so the result follows.
3. Recall that the matrix for $\rho_{V^*}(g)$ with respect to the dual basis is $(M^{-1})^t$. Taking transposes preserves traces, so
$$\chi_{V^*}(g) = \mathrm{Tr}(\rho_{V^*}(g)) = \mathrm{Tr}((M^{-1})^t) = \mathrm{Tr}(M^{-1}) = \chi_V(g^{-1}) = \overline{\chi_V(g)}$$
4. This follows from the isomorphism (of representations) $V \otimes W \cong \mathrm{Hom}(V^*, W)$ and the previous two parts.

$\square$

5.1.1 The regular character

Let χ_{reg} denote the character of the regular representation.

Proposition 5.10. *For any finite group G, $\chi_{\text{reg}}(e) = |G|$ and $\chi_{\text{reg}}(g) = 0$ for $g \neq e$. In addition, $\chi_{\text{reg}}(g) = \sum_i d_i \chi_{V_i}(g)$, where the sum ranges over irreducible representations (V_i, ρ_{V_i}) and $d_i := \dim V_i$.*

Proof. Recall that $\chi_{\text{reg}}(e) = \dim V_{\text{reg}}$, since this is the case for every representation. Since $\dim V_{\text{reg}} = |G|$, $\chi_{\text{reg}}(e) = |G|$.

Recall that the regular representation is given by $\rho_{\text{reg}}(g)(b_h) = b_{gh}$, so the matrix the (b_{gh}, b_h) entries equal to 1 and 0 everywhere else. Thus, the trace is 0 unless there is some h such that $gh = h$. But this is impossible unless $g = e$.

For the last part, recall that $V_{\text{reg}} \cong \oplus_i V_i^{\oplus \dim V_i}$. Since $\chi_{V \oplus W} = \chi_V + \chi_W$, this implies that $\chi_{\text{reg}}(g) = \sum_i d_i \chi_{V_i}$. $\square$

Example 5.11. If $G = C_n$, then we may write $\rho_{\text{reg}} = \sum_k \chi_k$, where $\chi_k = \rho_k$ is the 1-dimensional representation $g \mapsto e^{2\pi i k/n}$. This implies that $\sum_{k=0}^{n-1} e^{2\pi i k/n} = 0$, and that for any integer $s \in [1, n-1]$, $\sum_{k=0}^{n-1} e^{2\pi i k s/n} = 0$ (because both sides are $\chi_{\text{reg}}(g^s)$).

5.2 Inner products of characters

The set of characters of representations turns out to have a lot of structure, which is what makes the concept useful.

Definition 5.12. Let $C(G)$ denote the set of functions $f : G \to \mathbf{C}$, and let $C_{cl}(G)$ denote the set of functions $f : G \to \mathbf{C}$ which are constant on each conjugacy class of G, i.e., such that $f(hgh^{-1}) = f(g)$ for all $g, h \in G$.

Both $C(G)$ and $C_{cl}(G)$ are finite-dimensional complex vector spaces: Given a function $f : G \to \mathbf{C}$, we can scale it by setting $(\lambda f)(g) := \lambda \cdot f(g)$ for $\lambda \in \mathbf{C}$, and given two functions $f, f' : G \rightrightarrows \mathbf{C}$, we can add them by setting $(f + f')(g) := f(g) + f'(g)$.

There is a basis for $C(G)$ given by the functions $\delta_g : G \to \mathbf{C}$, which is defined by $\delta_g(g) = 1$ and $\delta_g(h) = 0$ for $h \neq g$.

If $f, f' \in C(G)$ are constant on conjugacy classes of G, then so are λf and $f + f'$, so the same arguments imply that $C_{cl}(G)$ is a vector space (and indeed, a subspace of $C(G)$).

Characters can be viewed as elements of $C_{cl}(G)$. The dimension of $C(G)$ is $|G|$, and the dimension of $C_{cl}(G)$ is equal to the number of conjugacy classes of G.

Using our choice of basis for $C(G)$, we have an inner product on $C(G)$:

Definition 5.13. Let $\xi, \psi : G \rightrightarrows G$ be elements of $C(G)$. We define

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

where $\overline{\psi(g)}$ means complex conjugation.

Note that $\langle \xi, \psi \rangle \neq \langle \psi, \xi \rangle$. In fact, $\langle \xi, \psi \rangle = \overline{\langle \psi, \xi \rangle}$, and $\langle \xi, \psi \rangle$ is linear in the first factor and conjugate-linear in the second factor, i.e., $\langle \lambda\xi, \mu\psi \rangle = \lambda\overline{\mu}\langle \xi, \psi \rangle$ for any $\lambda, \mu \in \mathbf{C}$. Furthermore, $\langle \xi, \xi \rangle = \frac{1}{|G|} \sum_g |\xi(g)|^2 \geq 0$ with equality if and only if $\xi = 0$.

This is the list of properties defining a *Hermitian inner product.* Notice that our basis is not quite orthonormal with respect to this inner product:

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

Our first goal is the following theorem:

Theorem 5.14. *Let (V, ρ_V) and (W, ρ_W) be representations of G and let χ_V and χ_W be the associated characters. Then*

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

Before we start proving it, we record some corollaries:

Corollary 5.15. *If (V, ρ_V) and (W, ρ_W) are irreducible representations of G, then $\langle \chi_V, \chi_W \rangle = 1$ if they are isomorphic, and $\langle \chi_V, \chi_W \rangle = 0$ otherwise.*

Proof. This follows from Schur's lemma, combined with the theorem. □

Corollary 5.16. *Let $\chi_1, \dots, \chi_r$ denote the irreducible characters of G. Then*

1. *$\chi_1, \dots, \chi_r$ are orthonormal elements of $C_{cl}(G)$.*
2. *We have an inequality: the number of conjugacy classes of G is at least r.*
3. *If (V, ρ_V) is any representation of G, then $V \cong \oplus_i V_i^{\langle \chi_V, \chi_i \rangle}$ and $\chi_V = \sum_i \langle \chi_V, \chi_i \rangle \chi_i$.*
4. *If (V, ρ_V) is a representation of G, it is irreducible if and only if $\langle V, V \rangle = 1$.*

Proof. 1. This follows from the previous corollary.

2. Since the χ_i are orthonormal, they are linearly independent. Therefore $\dim C_{cl}(G) \geq r$, and $\dim C_{cl}(G)$ is the number of conjugacy classes of G.

3. Recall that $V \cong \oplus_i V_i^{\dim \operatorname{Hom}(V,V_i)^G}$. The result then follows from the theorem.

4. We may write $V \cong \oplus V_i^{\oplus m_i}$ for some multiplicities m_i. Then

$$\langle \chi_V, \chi_V \rangle = \sum_{i,j} m_i m_j \langle \chi_i, \chi_j \rangle = \sum_i m_i^2$$

Then $\langle \chi_V, \chi_V \rangle = 1$ exactly when one of the m_i is 1 and the rest are 0.

□

Next we give a pair of useful lemmas.

Lemma 5.17. *Let V be a vector space. Then $f \mapsto \operatorname{Tr}(f)$ gives us a linear map $\operatorname{Tr} : \operatorname{Hom}(V,V) \to \mathbf{C}$. That is, if $f_1, f_2 \in \operatorname{Hom}(V,V)$ and $\lambda_1, \lambda_2 \in \mathbf{C}$, then $\operatorname{Tr}(\lambda_1 f_1 + \lambda_2 f_2) = \lambda_1 \operatorname{Tr}(f_1) + \lambda_2 \operatorname{Tr}(f_2)$.*

Proof. Pick a basis for V, and let M and N be the matrices representing f_1 and f_2, respectively. Then

$$\begin{aligned}\operatorname{Tr}(\lambda_1 f_1 + \lambda_2 f_2) = \operatorname{Tr}(\lambda_1 M + \lambda_2 N) &= \sum_{i=1}^{d} (\lambda_1 M_{ii} + \lambda_2 N_{ii}) \\ &= \lambda_1 \sum_{i=1}^{d} M_{ii} + \lambda_2 \sum_{i=1}^{d} N_{ii} = \lambda_1 \operatorname{Tr}(f_1) + \lambda_2 \operatorname{Tr}(f_2)\end{aligned}$$

□

Lemma 5.18. *Let V be a vector space, with a subspace $W \subset V$, and let $\pi : V \to W$ be a projection to W (so $\pi|_W = \mathbf{1}_W$). Then $\operatorname{Tr}(\pi) = \dim W$.*

Proof. Recall that W and $\ker(\pi)$ are complementary subspaces of V, so the natural map $W \oplus \ker(\pi) \to V$ is an isomorphism. If we choose bases $\mathcal{B}_W$ and $\mathcal{B}_\pi$ for W and $\ker(\pi)$, respectively, their union is a basis for V. If we write π as a matrix with respect to this basis, we get a matrix of the form

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

Therefore, $\operatorname{Tr}(\pi) = \operatorname{Tr}(\mathbf{1}_W) = \dim W$. □

Proof of Theorem. Recall that we can view $\operatorname{Hom}(V,W)$ as a representation of G, and the space of G-linear maps is its invariant subspace: $\operatorname{Hom}(V,W)^G \subset \operatorname{Hom}(V,W)$. Then we constructed a projection map $e : \operatorname{Hom}(V,W) \to \operatorname{Hom}(V,W)^G$ via $f \mapsto \frac{1}{|G|} \sum_{g \in G} \rho_{\operatorname{Hom}(V,W)}(g)(f)$.

We are interested in computing $\dim \operatorname{Hom}(V,W)^G$, and it suffices to compute $\operatorname{Tr}(e)$. But since $e : \operatorname{Hom}(V,W) \to \operatorname{Hom}(V,W)^G$ is a linear combination of the maps $\rho_{\operatorname{Hom}(V,W)}(g)e : \operatorname{Hom}(V,W) \to \operatorname{Hom}(V,W)^G$, we see that

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

However, $\operatorname{Tr}(\rho_{\operatorname{Hom}(V,W)}(g)) = \chi_{\operatorname{Hom}(V,W)}(g)$, and we proved earlier that $\chi_{\operatorname{Hom}(V,W)}(g) = \overline{\chi_V(g)}\chi_W(g)$. Therefore,

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

Since in this case $\langle \chi_W, \chi_V\rangle$ is a real number, $\langle \chi_W, \chi_V\rangle = \langle \chi_V, \chi_W\rangle$, as desired. $\square$

Example 5.19. Let $G = C_4 = \langle g : g^4 = e\rangle$. Consider the 2-dimensional matrix representation $\rho : G \to \mathrm{GL}_2(\mathbf{C})$ given by $\rho(g) = \left(\begin{smallmatrix} i & 2 \\ 1 & -i\end{smallmatrix}\right)$. Since $\rho(g^2) = \left(\begin{smallmatrix} i & 2 \\ 1 & -i\end{smallmatrix}\right)^2 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1\end{smallmatrix}\right)$, we have

$$\chi(e) = 2 \qquad \chi(g) = 0 \qquad \chi(g^2) = 2 \qquad \chi(g^3) = 0$$

Now the irreducible characters of G are those coming from the 1-dimensional matrix representations $\rho_k : G \to \mathrm{GL}_1(\mathbf{C})$; $\rho_k(g) := i^k$ for $k = 0, 1, 2, 3$. So we have

$$\chi_k(e) = 1 \qquad \chi_k(g) = i^k \qquad \chi_k(g^2) = (-1)^k \qquad \chi_k(g^3) = (-i)^k$$

Now we compute $\langle \chi, \chi_k\rangle$:

$$\begin{aligned}\langle \chi, \chi_k\rangle &= \frac{1}{4}\left(2\cdot\overline{1} + 0\cdot\overline{i^k} + 2\cdot\overline{(-1)^k} + 0\cdot\overline{(-i)^k}\right)\\ &= \frac{1}{4}\left(2 + 2\cdot(-1)^k\right) = \frac{1}{2}\left(1+(-1)^k\right)\\ &= \begin{cases} 1 & \text{if } k = 0, 2\\ 0 & \text{if } k = 1, 3\end{cases}\end{aligned}$$

Thus, ρ is isomorphic to the direct sum of ρ_0 and ρ_2.

Example 5.20. Let $G = D_8 = \langle s, t : s^4 = t^2 = e, tst = s^{-1}\rangle$, and consider again the 4-dimensional representation (V, ρ_V) coming from its action on the vertices of a square. Explicitly,

$$\rho_V(s) = \begin{pmatrix} 0 & 0 & 0 & 1\\ 1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\end{pmatrix} \qquad \rho_V(t) = \begin{pmatrix} 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\\ 0 & 1 & 0 & 0\\ 1 & 0 & 0 & 0\end{pmatrix}$$

The conjugacy classes of D_8 are $\{e\}, \{s, s^{-1}\}, \{s^2\}, \{t, s^2t\}, \{st, s^3t\}$, and since characters are constant on conjugacy classes, we can write down the values of χ_V:

	$\{e\}$	$\{s, s^{-1}\}$	$\{s^2\}$	$\{t, s^2t\}$	$\{st, s^3t\}$
$\chi_V(g)$	4	0	0	0	2

We first compute

$$\langle \chi_V, \chi_V \rangle = \frac{1}{8} \sum_{g \in D_8} |\chi_V(g)|^2 = \frac{1}{8}\left(4^2 + 2\cdot 0^2 + 0^2 + 2\cdot 0^2 + 2\cdot 2^2\right) = 3$$

Thus, V is reducible. There is an "easy" 1-dimensional subrepresentation, namely the one generated by $\begin{pmatrix} 1\\1\\1\\1 \end{pmatrix}$, which is isomorphic to the trivial representation ρ_{triv}. Indeed,

$$\langle \chi_V, \chi_{\text{triv}} \rangle = \frac{1}{8}\left((4\cdot 1) + 2\cdot(0\cdot 1) + (0\cdot 1) + 2\cdot(0\cdot 1) + 2\cdot(2\cdot 1)\right) = 1$$

so V_{triv} is isomorphic to a subrepresentation of V, and in fact $\dim \operatorname{Hom}(V_{\text{triv}}, V)^{D_8} = 1$, so the subspace generated by $\begin{pmatrix} 1\\1\\1\\1 \end{pmatrix}$ is the largest trivial subrepresentation of V.

There is a 3-dimensional complement $W \subset V$, so we can expand our table (using the fact that $\chi_{\text{triv}} + \chi_W = \chi_V$):

	$\{e\}$	$\{s, s^{-1}\}$	$\{s^2\}$	$\{t, s^2t\}$	$\{st, s^3t\}$
$\chi_V(g)$	4	0	0	0	2
$\chi_{\text{triv}}(g)$	1	1	1	1	1
$\chi_W(g)$	3	-1	-1	-1	1

Now we compute

$$\langle \chi_W, \chi_W \rangle = \frac{1}{8} \sum_{g \in D_8} |\chi_W(g)|^2 = \frac{1}{8}\left(3^2 + 2\cdot(-1)^2 + (-1)^2 + 2\cdot(-1)^2 + 2\cdot 1^2\right) = 2$$

so W is also reducible. It must therefore have a 1-dimensional subrepresentation, and the characters of the non-trivial 1-dimensional subrepresentations of D_8 are

	$\{e\}$	$\{s, s^{-1}\}$	$\{s^2\}$	$\{t, s^2t\}$	$\{st, s^3t\}$
$\chi_{+-}(g)$	1	1	1	-1	-1
$\chi_{-+}(g)$	1	-1	1	1	-1
$\chi_{--}(g)$	1	-1	1	-1	1

Then we may compute $\langle \chi_W, \chi_{+-} \rangle$, $\langle \chi_W, \chi_{-+} \rangle$, and $\langle \chi_W, \chi_{--} \rangle$, and we see that $\langle \chi_W, \chi_{--} \rangle = 1$. Thus, W is the direct sum of the 1-dimensional representation with $s, t \mapsto -1$ and a 2-dimensional representation W'.

Finally,

$$\langle \chi_{W'}, \chi_{W'} \rangle = \langle \chi_W - \chi_{--}, \chi_W - \chi_{--} \rangle = \langle \chi_W, \chi_W \rangle - 2\langle \chi_W, \chi_{--} \rangle + \langle \chi_{--}, \chi_{--} \rangle = 1$$

so W' is irreducible.

5.2.1 Character tables

A *character table* is a way of recording information about every irreducible character of a group. Let $\chi_1, \dots, \chi_r$ be the irreducible characters of G, and let $C_1, \dots, C_s$ be the conjugacy classes of G. We have seen that $r \leq s$.

The character table for G is a table with columns indexed by $C_1, \dots, C_s$ and rows indexed by $\chi_1, \dots, \chi_r$. For computational convenience, we will generally also add a line recording the size of the conjugacy classes. Last week, we gave the example of the character table of D_8:

	$\{e\}$	$\{s, s^{-1}\}$	$\{s^2\}$	$\{st, s^{-1}t\}$	$\{t, s^2t\}$
size of conjugacy class	1	2	1	2	2
$\chi_{\text{triv}}(g)$	1	1	1	1	1
$\chi_{+-}(g)$	1	1	1	-1	-1
$\chi_{-+}(g)$	1	-1	1	-1	1
$\chi_{--}(g)$	1	-1	1	$+1$	-1
$\chi_2(g)$	2	0	-2	0	0

A very small example is the character table of $C_2 = \langle g : g^2 = e \rangle$. There are two conjugacy classes and two characters, so we get

	$\{e\}$	$\{g\}$
size of conjugacy class	1	1
χ_1	1	1
χ_2	1	-1

Let's give a bigger example of a character table, and compute the character table of S_4. Recall that in a symmetric group, the conjugacy classes are indexed by the shape of the cycles. So the transpositions $(1\ 2), (1\ 3), (1\ 4), (2\ 3), (2\ 4), (3\ 4)$ are all conjugate, the 3-cycles $(1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3)$ are all conjugate, and so on. We start off with the trivial character and the sign character:

	$\{e\}$	$(1\ 2)$	$(1\ 2\ 3)$	$(1\ 2)(3\ 4)$	$(1\ 2\ 3\ 4)$
size of conjugacy class	1	6	8	3	6
χ_{triv}	1	1	1	1	1
χ_{sign}	1	-1	1	1	-1

We need to find the rest of the irreducible characters of S_4. To start with, consider the permutation representation $(V_{\text{perm}}, \rho_{\text{perm}})$; this is a 4-dimensional representation with basis (b_1, b_2, b_3, b_4), and S_4 acts by acting on the indices. That is, if $\sigma \in S_4$, then $\rho_{\text{perm}}(\sigma)(b_i) = b_{\sigma \cdot i}$. We can compute the character χ_{perm}:

$$\chi_{\text{perm}}(e) = 4 \qquad \chi_{\text{perm}}(1\ 2) = 2 \qquad \chi_{\text{perm}}(1\ 2\ 3) = 1 \qquad \chi_{\text{perm}}((1\ 2)(3\ 4)) = 0 \qquad \chi_{\text{perm}}(1\ 2\ 3\ 4) = 0$$

Now observe that $b_1 + b_2 + b_3 + b_4 \in V_{\text{perm}}$ is fixed by $\rho_{\text{perm}}(\sigma)$ for every $\sigma \in S_4$. Thus, the span of $b_1 + b_2 + b_3 + b_4$ is a 1-dimensional subrepresentation of V_{perm}, isomorphic to the trivial representation. Therefore, by Maschke's theorem there is a complementary subrepresentation $W \subset V_{\mathrm{perm}}$, i.e., $W \subset V_{\mathrm{perm}}$ is a subrepresentation, $W \cap \langle b_1 + b_2 + b_3 + b_4 \rangle = \{0\}$, and the map $W \oplus \langle b_1 + b_2 + b_3 + b_4 \rangle \to V$ (given by $(w, v) \mapsto w + v$) is an isomorphism.

This implies that W is 3-dimensional. We can use character theory to prove that W is irreducible. Since taking direct sums of representations translates to adding their characters, we can compute χ_W. Namely, $\chi_W = \chi_{\mathrm{perm}} - \chi_{\mathrm{triv}}$, so

$$\chi_W(e) = 3 \qquad \chi_W(1\ 2) = 1 \qquad \chi_W(1\ 2\ 3) = 0 \qquad \chi_W((1\ 2)(3\ 4)) = -1 \qquad \chi_W(1\ 2\ 3\ 4) = -1$$

Recall that a representation (W, ρ_W) is irreducible if and only if the inner product $\langle \chi_W, \chi_W \rangle = 1$. We compute

$$\langle \chi_W, \chi_W \rangle = \frac{1}{24} \left(3^2 + 6 \cdot 1^2 + 8 \cdot 0^2 + 3 \cdot (-1)^2 + 6 \cdot (-1)^2 \right) = 1$$

so W is indeed irreducible.

We add χ_W to our table:

	$\{e\}$	$(1\ 2)$	$(1\ 2\ 3)$	$(1\ 2)(3\ 4)$	$(1\ 2\ 3\ 4)$
size of conjugacy class	1	6	8	3	6
χ_{triv}	1	1	1	1	1
χ_{sign}	1	-1	1	1	-1
χ_W	3	1	0	-1	-1

There are more irreducible representations of S_4, because $1^2 + 1^2 + 3^2 = 11 < 24$. In fact, the squares of the dimensions of the remaining representations must add to 13, so we are looking for a 2-dimensional representation and a 3-dimensional representation.

One way to construct another 3-dimension representation is to take the tensor product $W' := V_{\mathrm{sign}} \otimes W$. This is 3-dimensional (because $\dim V_{\mathrm{sign}} = 1$ and $\dim W = 3$), and it is irreducible by an exercise on problem sheet #3. We can compute $\chi_{W'}$:

$$\chi_{W'} = \chi_{\mathrm{sign} \otimes W} = \chi_{\mathrm{sign}} \cdot \chi_W$$

Thus, our table is now

	$\{e\}$	$(1\ 2)$	$(1\ 2\ 3)$	$(1\ 2)(3\ 4)$	$(1\ 2\ 3\ 4)$
size of conjugacy class	1	6	8	3	6
χ_{triv}	1	1	1	1	1
χ_{sign}	1	-1	1	1	-1
χ_W	3	1	0	-1	-1
$\chi_{W'}$	3	-1	0	-1	1

Note that since $\chi_{W'} \neq \chi_W$, we know that W and W' are not isomorphic as representations.

Now we need to find the character of our mysterious 2-dimensional representation, which we will call (U, ρ_U). We add its row to the character table:

	$\{e\}$	$(1\ 2)$	$(1\ 2\ 3)$	$(1\ 2)(3\ 4)$	$(1\ 2\ 3\ 4)$
size of conjugacy class	1	6	8	3	6
χ_{triv}	1	1	1	1	1
χ_{sign}	1	-1	1	1	-1
χ_W	3	1	0	-1	-1
$\chi_{W'}$	3	-1	0	-1	1
χ_U	2	?	?	?	?

We know that U is the only irreducible 2-dimensional representation of S_4 (for dimension reasons). On the other hand $V_{\text{sign}} \otimes U$ is an irreducible 2-dimensional representation of S_4; it follows that it must be isomorphic to U, and so we must have $\chi_{\text{sign}} \cdot \chi_U = \chi_U$. But that, in turn, implies that $\chi_U(1\ 2) = \chi_U(1\ 2\ 3\ 4) = 0$, so the table is now

	$\{e\}$	$(1\ 2)$	$(1\ 2\ 3)$	$(1\ 2)(3\ 4)$	$(1\ 2\ 3\ 4)$
size of conjugacy class	1	6	8	3	6
χ_{triv}	1	1	1	1	1
χ_{sign}	1	-1	1	1	-1
χ_W	3	1	0	-1	-1
$\chi_{W'}$	3	-1	0	-1	1
χ_U	2	0	?	?	0

We also know that $\langle \chi_U, \chi_V \rangle = 0$ for any irreducible representation V not isomorphic to U. If we compute $\langle \chi_U, \chi_W \rangle$, we get

$$\begin{aligned}\langle \chi_U, \chi_W \rangle &= \frac{1}{24}\left(2 \cdot 3 + 6 \cdot (0 \cdot 1) + 8 \cdot (\chi_U(1\ 2\ 3) \cdot 0) + 3 \cdot (\chi_U((1\ 2)(3\ 4)) \cdot (-1)) + 6 \cdot (0 \cdot (-1))\right) \\ &= \frac{1}{24}\left(6 - 3\chi_U((1\ 2)(3\ 4))\right)\end{aligned}$$

Since this inner product must be 0, we see that $\chi_U((1\ 2)(3\ 4)) = 2$, and our table is now

	$\{e\}$	$(1\ 2)$	$(1\ 2\ 3)$	$(1\ 2)(3\ 4)$	$(1\ 2\ 3\ 4)$
size of conjugacy class	1	6	8	3	6
χ_{triv}	1	1	1	1	1
χ_{sign}	1	-1	1	1	-1
χ_W	3	1	0	-1	-1
$\chi_{W'}$	3	-1	0	-1	1
χ_U	2	0	?	2	0

Now we use $\langle \chi_U, \chi_{\text{triv}} \rangle = 0$:

$$\begin{aligned}\langle \chi_U, \chi_{\text{triv}} \rangle &= \frac{1}{24}\left(2 \cdot 1 + 6 \cdot (0 \cdot 1) + 8 \cdot (\chi_U(1\ 2\ 3) \cdot 1) + 3 \cdot (2 \cdot 1) + 6 \cdot (0 \cdot 1)\right) \\ &= \frac{1}{24}\left(8 + 8 \cdot \chi_U(1\ 2\ 3)\right)\end{aligned}$$

This implies that $\chi_U(1\ 2\ 3) = -1$, so we have completed our table:

	$\{e\}$	$(1\ 2)$	$(1\ 2\ 3)$	$(1\ 2)(3\ 4)$	$(1\ 2\ 3\ 4)$
size of conjugacy class	1	6	8	3	6
χ_{triv}	1	1	1	1	1
χ_{sign}	1	-1	1	1	-1
χ_W	3	1	0	-1	-1
$\chi_{W'}$	3	-1	0	-1	1
χ_U	2	0	-1	2	0

So we have shown that there is some irreducible 2-dimensional representation (U, ρ_U) of S_4, and we know the traces of $\rho_U(\sigma)$ for $\sigma \in S_4$.

We can say a bit more about (U, ρ_U), though. Observe that $\chi_U((1\ 2)(3\ 4)) = 2 = \chi_U(e)$. We showed earlier that for any character, $\chi(g) = \chi(e)$ if and only if $\rho(g) = \rho(e)$. Let $N \subset S_4$ be the normal subgroup generated by pairs of transpositions (e.g. $(1\ 2)(3\ 4)$); then we have shown that $\rho_U(\sigma) = \rho_U(e)$ for $\sigma \in N$. Thus, we can view the homomorphism $\rho_U : S_4 \to \mathrm{GL}(U)$ as the composition

$$\rho_U : S_4 \twoheadrightarrow S_4/N \cong S_3 \to \mathrm{GL}_w(U)$$

Indeed, we have an inclusion $S_3 \hookrightarrow S_4$ by thinking of a permutation of $\{1, 2, 3\}$ as a permutation of $\{1, 2, 3, 4\}$ which fixes 4. Composing with the projection $S_4 \twoheadrightarrow S_4/N$, we get a homomorphism $S_3 \to S_4/N$ between groups of the same order. But since $N \cap S_3 = \{e\}$ inside S_4, this homomorphism is injective, so it is an isomorphism.

Thus, (U, ρ_U) can be viewed as a 2-dimensional representation of S_3, and χ_U agrees with the character of the irreducible 2-dimensional representation of S_3. So actually, we already knew about (U, ρ_U)!

This motivates the following definition:

Definition 5.21. Let $N \lhd G$ be a normal subgroup of a finite group G, and let $(\overline{V}, \rho_{\overline{V}})$ be a representation of the quotient G/N. The *inflation* of $(\overline{V}, \rho_{\overline{V}})$ is the representation (V, ρ_V) of G, where $V = \overline{V}$ as vector spaces, and $\rho_V : G \to \mathrm{GL}(V)$ is the composition $G \twoheadrightarrow G/N \xrightarrow{\rho_{\overline{V}}} \mathrm{GL}(\overline{V})$. Equivalently, $\rho_V(g) := \rho_{\overline{V}}(gN)$.

Observe that the inflation V is irreducible as a representation of G if and only if $\overline{V}$ is irreducible as a representation of G/N.

5.2.2 Row and column orthogonality

Fact: Character tables are square, i.e., the number of irreducible representations of G is equal to the number of conjugacy classes of G.

We will prove this later on, but we assume it for now.

We have already proved that the rows of a character table can be related to each other:

$$\langle \chi_i, \chi_j \rangle := \frac{1}{|G|} \sum_{g \in G} \chi_i(g)\overline{\chi_j(g)} = \begin{cases} 0 & \text{if } i \neq j \\ 1 & \text{if } i = j \end{cases}$$

We refer to this as *row orthogonality*, because it tells us that the rows of a character table are mutually orthogonal.

We also have a result we refer to as *column orthogonality*:

Proposition 5.22. *Let $g \in G$, and let $C(g)$ denote the conjugacy class containing g. Then for any $h \in G$,*

$$\sum_{i=1}^{r} \overline{\chi_i(g)}\chi_i(h) = \begin{cases} 0 & \text{if } h \notin C(g) \\ \frac{|G|}{|C(g)|} & \text{if } h \in C(g) \end{cases}$$

Proof. Consider the class function $\delta_{C(g)} : G \to \mathbf{C}$, defined by $\delta_{C(g)}(h) = 1$ if $h \in C(g)$ and $\delta_{C(g)}(h) = 0$ otherwise. The set $\{\delta_{C(g)}\}_g$ forms a basis for the space of class functions $C_{cl}(G)$, where g ranges over representatives of each conjugacy class.

We proved earlier that $\{\chi_i\}_{i=1}^r$ are orthonormal (with respect to the inner product on $C(G)$), and therefore linearly independent. Therefore, if we assume that character tables are square, $\{\chi_i\}_i$ form another basis for $C_{cl}(G)$. We may therefore write

$$\delta_{C(g)} = \sum_{i=1}^{r} \langle \delta_{C(g)}, \chi_i \rangle \chi_i$$

We can compute directly that $\langle \delta_{C(g)}, \chi_i \rangle = \frac{|C(g)|}{|G|}\overline{\chi_i(g)}$, so

$$\delta_{C(g)} = \sum_{i=1}^{r} \frac{|C(g)|}{|G|}\overline{\chi_i(g)}\chi_i$$

Evaluating both sides on h, we see that

$$\sum_{i=1}^{r} \frac{|C(g)|}{|G|}\overline{\chi_i(g)}\chi_i(h) = \begin{cases} 0 & \text{if } h \notin C(g) \\ 1 & \text{if } h \in C(g) \end{cases}$$

Then we may multiply both sides by $\frac{|G|}{|C(g)|}$ to obtain the result. □

Example 5.23. Take $g = e$ in the previous proposition. Then it implies that

$$\sum_{i=1}^{r} \overline{\chi_i(e)}\chi_i(e) = \sum_{i=1}^{r} (\dim V_i)^2 = |G|$$

which is a familiar formula.

Example 5.24. We could have used column orthogonality to compute the last row of the character table for S_4:

	$\{e\}$	(1 2)	(1 2 3)	(1 2)(3 4)	(1 2 3 4)
size of conjugacy class	1	6	8	3	6
χ_{triv}	1	1	1	1	1
χ_{sign}	1	-1	1	1	-1
χ_W	3	1	0	-1	-1
$\chi_{W'}$	3	-1	0	-1	1
χ_U	2	?	?	?	?

Then column orthogonality (applied to each column with itself) implies that $\chi_U(1\ 2) = \chi_U(1\ 2\ 3\ 4) = 0$, $\chi_U(1\ 2\ 3) = \pm 1$, and $\chi_U((1\ 2)(3\ 4)) = \pm 2$. Comparing the (1 2 3) column with the $\{e\}$ column impies that $\chi_U(1\ 2\ 3) = -1$, and comparing the (1 2)(3 4) column with the (1 2 3) column implies that $\chi_U((1\ 2)(3\ 4)) = 2$.

We can reformulate our row and column orthogonality relations a bit. Let the conjugacy classes of G be $C_1, \ldots, C_r$, with representatives $g_1, \ldots, g_r$, respectively. Now define an $r \times r$ matrix B by setting

$$B_{ij} := \sqrt{\frac{|C_j|}{|G|}} \chi_i(g_j)$$

Proposition 5.25. *The matrix B is unitary, i.e., $B^{-1} = \overline{B}^T$.*

Proof. It is enough to show that $B\overline{B}^T = \mathbf{1}_r$. Indeed, this implies that $\det(B) \neq 0$ so B is invertible. Now

$$(B\overline{B}^T)_{ik} = \sum_j \left(\sqrt{\frac{|C_j|}{|G|}} \chi_i(g_j) \cdot \sqrt{\frac{|C_j|}{|G|}} \overline{\chi_k(g_j)} \right) = \frac{1}{|G|} \sum_j |C_j| \chi_i(g_j) \overline{\chi_k(g_j)} = \langle \chi_i, \chi_k \rangle$$

□

We can rephrase this as saying that $\{\delta_{C(g)}\}$ and $\{\chi_i\}$ both give bases for the space of class functions $C_{cl}(G)$. But $\{\chi_i\}$ is orthonormal and $\{\delta_{C(g)}\}$ is orthogonal but not orthonormal, so B is the change-of-basis matrix between $\{\chi_i\}$ and a rescaled version of $\{\delta_{C(g)}\}$.

5.2.3 Summary

Characters, and character tables, are a tool for assembling information about representations of a group, in a way that's convenient for computation.

We cannot recover a group from its character table. For example, D_8 and the quaternion group Q_8 are not isomorphic, but they have the same character table.

However, we can find the center of the group: $g \in G$ is in the center $Z(G)$ if and only if $C(g) = \{g\}$, which is the case if and only if $\sum_{i=1}^{r} |\chi_i(g)|^2 = |G|$.

We can also find all normal subgroups of G from the character table, so in particular, we can determine whether or not G is simple.

Definition 5.26. Let $\chi : G \to \mathbf{C}$ be a function. We define $\ker \chi := \{g \in G : \chi(g) = \chi(e)\}$.

We have proved that if (V, ρ_V) is a representation and χ_V is the associated character, then $\chi_V(g) = \chi_V(e)$ if and only if $\rho_V(g) = \rho_V(e) = \mathbf{1}_V$. Thus, $\ker \chi_V = \ker \rho_V$. But $\ker \rho_V \subset G$ is a normal subgroup of G, so G is simple if and only if $\ker \chi = \{e\}$ for every character χ.

Proposition 5.27. *Let G be a finite group and let $H \lhd G$ be a normal subgroup. Let $\chi_1, \ldots, \chi_r$ be the irreducible characters of G.*

1. *There is a representation (V, ρ_V) of G such that $\ker \rho_V = H$.*
2. *There is a subset $I \subset \{1, \ldots, r\}$ such that $H = \cap_{i \in I} \ker \chi_i$.*

Proof.

1. Consider the regular representation $(\overline{V}_{\mathrm{reg}}, \rho_{\overline{\mathrm{reg}}})$ of G/H, and let (V, ρ_V) be the inflation to G. The regular representation is faithful, so $\ker \rho_V = H$.
2. Let (V, ρ_V) again be the inflation of the regular representation of G/H. Then $V \cong V_1^{\oplus m_i} \oplus \cdots \oplus V_r^{m_r}$, where the V_i are the irreducible representations of G and the m_i are the multiplicities. Let $I := \{i : m_i > 0\}$. Then

$$H = \ker \rho_V = \cap_{i \in I} \ker \rho_i = \cap_{i \in I} \ker \chi_i$$

$\square$

6 Algebras and modules

6.1 Algebras

Up to this point, we have viewed representations of groups as vector spaces together with linear actions of groups. The vector space has an additive structure, and the group acts by multiplication, but we have treated these additive and multiplicative structures separately.

An algebra is a structure that has both addition and multiplication. A basic example is the set of $d \times d$ matrices $\mathrm{Mat}_d(\mathbf{C})$ — it is a vector space because we can add matrices and scale them by complex numbers, but we can also multiply matrices.

In other words, we have a map

$$\begin{aligned} m : \mathrm{Mat}_d(\mathbf{C}) \times \mathrm{Mat}_d(\mathbf{C}) &\to \mathrm{Mat}_d(\mathbf{C}) \\ (M, N) &\mapsto M \cdot N \end{aligned}$$

This map has the following important properties:

1. m is bilinear: $m(\lambda_1 M_1 + \lambda_2 M_2, N) = \lambda_1 m(M_1, N) + \lambda_2 m(M_2, N)$

2. m is associative: $m(m(L, M), N) = m(L, m(M, N))$, or equivalently, $(L \cdot M) \cdot N = L \cdot (M \cdot N)$

3. m is unital: there is an element $I_d \in \mathrm{Mat}_d(\mathbf{C})$ such that $m(M, I_d) = m(I_d, M) = M$ for all $M \in \mathrm{Mat}_d(\mathbf{C})$

We will define an algebra to be a complex vector space satisfying these properties:

Definition 6.1. An *algebra* is a vector space A equipped with a bilinear, associative, and unital multiplication map $m : A \times A \to A$.

We will write ab or $a \cdot b$ for $m(a, b)$.

We observe that the unit element of A is unique. Indeed, if 1_A and $1'_A$ are both unit elements of A, then $1'_A = 1_A \cdot 1'_A = 1_A$.

Given an algebra A, we can define a map $\mathbf{C} \to A$ via $\lambda \mapsto \lambda 1_A$. This map is compatible with addition and multiplication (it is a ring homomorphism, if you have seen rings before).

Example 6.2.

1. Let $A = \mathbf{C}$ with the usual vector space structure and m given by the usual multiplication.

2. Let $A = \mathbf{C} \oplus \mathbf{C}$, with multiplication given by
$$m((x_1, y_1), (x_2, y_2)) := (x_1 x_2, y_1 y_2)$$

3. Let A be the set of polynomials $\mathbf{C}[x]$, which is an infinite-dimensional vector space, with multiplication given the multiplication of polynomials.

4. Let $A = \mathbf{C} \oplus \mathbf{C}$, with multiplication given by
$$m((x_1, y_1), (x_2, y_2)) := (x_1 x_2, x_1 y_2 + x_2 y_1)$$
Alternatively, we can view A as a 2-dimensional complex vector space with basis $\{1, x\}$, with multiplication given by $1^2 = 1$, $1x = x1 = x$, and $x^2 = 0$ and extended bilinearly. The unit element is $(1, 0)$.

5. Let V be a vector space and let $A = \mathrm{Hom}(V, V)$. Multiplication is given by composition of maps, i.e., $fg := f \circ g$. If we pick a basis of V, A becomes isomorphic to $\mathrm{Mat}_d(\mathbf{C})$ for some d, and composition of maps becomes multiplication of matrices.

6. Suppose A and B are algebras. We can make the direct sum $A \oplus B$ into an algebra by defining multiplication by
$$m((a_1, b_1), (a_2, b_2)) = (a_1 a_2, b_1 b_2)$$
The unit element is $(1_A, 1_B)$.

For us, the most important example will be the group algebra:

Let G be a finite group, and let $\mathbf{C}[G]$ denote the set of formal linear combinations of elements of G:

$$\mathbf{C}[G] := \{\lambda_1[g_1] + \ldots + \lambda_s[g_s] : \lambda_i \in \mathbf{C}\}$$

We define addition via

$$(\lambda_1[g_1] + \ldots + \lambda_s[g_s]) + (\mu_1[g_1] + \ldots + \mu_s[g_s]) := (\lambda_1 + \mu_1)[g_1] + \ldots + (\lambda_s + \mu_2)[g_s]$$

and scaling via

$$\mu \cdot (\lambda_1[g_1] + \ldots + \lambda_s[g_s]) := (\mu\lambda_1[g_1] + \ldots + \mu\lambda_s[g_s]$$

so $\mathbf{C}[G]$ is a vector space. As a vector space, it is the same as the vector space V_{reg} that we have seen while studying the regular representation.

However, $\mathbf{C}[G]$ also has a multiplication map, which comes from the multiplication map on G. More specifically, we define $m([g],[h]) := [gh]$ and extend this to a bilinear map $m : \mathbf{C}[G] \times \mathbf{C}[G] \to \mathbf{C}[G]$. Explicitly,

$$(\lambda_1[g_1] + \ldots + \lambda_s[g_s]) \cdot (\mu_1[g_1] + \ldots + \mu_s[g_s]) := \sum_{g_k} \left(\sum_{g_i,g_j \text{ with } g_ig_j = g_k} \lambda_i\mu_j[g_k] \right)$$

This product is associative because multiplication in G is associative, and the unit element is $[e]$.

The group algebra $\mathbf{C}[G]$ is commutative if and only if G is an abelian group.

Example 6.3. Let $G = C_2 = \langle g : g^2 = e\rangle$. Then $\mathbf{C}[G] = \{\lambda_1[e] + \lambda_2[g] : \lambda_i \in \mathbf{C}\}$ is a 2-dimensional vector space, with multiplication

$$(\lambda_1[e] + \lambda_2[g]) \cdot (\mu_1[e] + \mu_2[g]) = (\lambda_1\mu_1 + \lambda_2\mu_2)[e] + (\lambda_1\mu_2 + \lambda_2\mu_1)[g]$$

Definition 6.4. Let A and B be algebras. A linear map $f : A \to B$ is an *algebra homomorphism* if $f(1_A) = 1_B$ and $f(a_1a_2) = f(a_1)f(a_2)$. An algebra homomorphism f is an *algebra isomorphism* if f is an isomorphism of vector spaces.

Example 6.5. Consider the map $f : \mathbf{C}[C_2] \to \mathbf{C} \oplus \mathbf{C}$ defined by $[e] \mapsto (1,1)$ and $[g] \mapsto (1,-1)$. This is clearly an isomorphism of vector spaces, since its image contains a basis of $\mathbf{C} \oplus \mathbf{C}$ and both vector spaces are 2-dimensional. To check that f is an algebra homomorphism, it is enough to check that if $x, y \in \mathbf{C}[C_2]$ are basis elements, then $f(xy) = f(x)f(y)$, since multiplication is bilinear on both sides. But

$$\begin{aligned}
f([e][e]) = f([e]) = (1,1) = (1,1)(1,1) = f([e])f([e]) \\
f([e][g]) = f([g]) = (1,-1) = (1,1)(1,-1) = f([e])f([g]) \\
f([g][e]) = f([g]) = (1,-1) = (1,-1)(1,1) = f([g])f([e]) \\
f([g][g]) = f([e]) = (1,1) = (1,-1)(1,-1) = f([g])f([g])
\end{aligned}$$

Recall that our algebras are not necessarily commutative.

Definition 6.6. Let A be an algebra with multiplication map m. The *opposite algebra* A^{op} is the algebra with the same underlying vector space, and with multiplication given by

$$\begin{aligned} m^{op} : A^{op} \times A^{op} &\to A^{op} \\ (a, b) &\mapsto m(b, a) \end{aligned}$$

The algebra axioms for A imply that A^{op} is also an algebra, and the unit element is the same. It is clear that m^{op} is the same as m if and only if A is commutative.

Proposition 6.7. *Let G be a finite group. Then $\mathbf{C}[G] \cong \mathbf{C}[G]^{op}$, with an isomorphism given by*

$$\begin{aligned} I : \mathbf{C}[G] &\to \mathbf{C}[G] \\ [g] &\mapsto [g^{-1}] \end{aligned}$$

Thus, even if A is non-commutative, it is possible for A and A^{op} to be abstractly isomorphic.

Proof. It is clear that I is an isomorphism of vector spaces, since it simply shuffles the given basis for $\mathbf{C}[G]$. We need to check that I is an algebra homomorphism. For this, it suffices to check that $m^{op}(I([g]), I([h])) = I(m([g], [h]))$ for all $g, h \in G$. But

$$m^{op}(I([g]), I([h])) = m^{op}([g^{-1}], [h^{-1}]) = m([h^{-1}], [g^{-1}]) = [h^{-1}g^{-1}]$$

and

$$I(m([g], [h])) = I([gh]) = [(gh)^{-1}] = [h^{-1}g^{-1}]$$

so both sides are equal. □

6.2 Modules

Now we will generalize the definition of a representation.

Definition 6.8. Let A be an algebra. A (left) A-module is a vector space M together with an algebra homomorphism $\rho : A \to \mathrm{Hom}(M, M)$.

Equivalently, an A-module is a vector space M together with an action map $A \times M \to M$ sending $(a, m) \mapsto a \cdot m := \rho(a)(m)$ satisfying

1. $a \cdot (m + n) = a \cdot m + a \cdot n$
2. $(a + b) \cdot m = a \cdot m + b \cdot m$
3. $(ab) \cdot m = a \cdot (b \cdot m)$

4. $1_A \cdot m = m$

Proposition 6.9. *Let G be a finite group. A $\mathbf{C}[G]$-module is the same thing as a representation of G.*

Proof. We explain how to go between representations of G and $\mathbf{C}[G]$-modules.

Suppose that $\rho : \mathbf{C}[G] \to \mathrm{Hom}(M, M)$ is the map making M into a $\mathbf{C}[G]$-module. Then we can restrict ρ to $G = \{[g]\}_{g \in G} \subset \mathbf{C}[G]$ to get a function $\rho_M : G \to \mathrm{Hom}(M, M)$. By the definition of an algebra homomorphism, $\rho([g][h]) = \rho([g]) \circ \rho([h])$ for any $g, h \in G$. In particular, if we take $h = g^{-1}$, we see that

$$\rho([g]) \circ \rho([g^{-1}]) = \rho([e]) = \mathbf{1}_M$$

Thus, each linear map $\rho([g]) : M \to M$ has an inverse, namely $\rho([g^{-1}])$. Thus, ρ_M is a function $G \to \mathrm{GL}(M)$, and we have seen that it is a group homomorphism. So (M, ρ_M) is a group representation.

On the other hand, suppose that $\rho : G \to \mathrm{GL}(M)$ is a representation of G. We may extend ρ linearly to $\mathbf{C}[G]$ to get a map $\widetilde{\rho} : \mathbf{C}[G] \to \mathrm{Hom}(M, M)$ given by

$$\widetilde{\rho}(\sum_g \lambda_g [g]) = \sum_g \lambda_g \rho(g)$$

This is a linear map, by construction, and it follows from the definition of multiplication in $\mathbf{C}[G]$ that $\widetilde{\rho}$ is an algebra homomorphism. Thus, M is a $\mathbf{C}[G]$ module. $\square$

Example 6.10. Let A be the algebra $\mathbf{C}$. Then an A-module is a vector space M and a homomorphism $\rho : \mathbf{C} \to \mathrm{Hom}(M, M)$. We must have $\rho(1) = \mathbf{1}_M$, and by linearity, we must have $\rho(\lambda) = \lambda \mathbf{1}_M$ for all $\lambda \in \mathbf{C}$. Thus, there is a unique ρ making M into an A-module. So a $\mathbf{C}$-module is the same thing as a vector space.

Example 6.11. Let $A = \mathbf{C} \oplus \mathbf{C}$. Recall that we showed that $A \cong \mathbf{C}[C_2]$. Let us classify 1-dimensional A-modules. In other words, if M is a 1-dimensional vector space, we need to classify algebra homomorphisms

$$\rho : \mathbf{C} \oplus \mathbf{C} \to \mathrm{Hom}(M, M) = \mathbf{C}$$

It suffices to specify $\rho(1,0)$ and $\rho(0,1)$, and we need these values to satisfy

$$\begin{aligned} (\rho(1,0))^2 = \rho((1,0)^2) = \rho(1,0) \qquad (\rho(0,1))^2 &= \rho((0,1)^2) = \rho(0,1) \\ \rho(1,0)\rho(0,1) = \rho((1,0)(0,1)) = \rho(0,0) = 0 \qquad \rho(0,1) + \rho(1,0) &= \rho((1,1)) = \rho(1_A) = 1 \end{aligned}$$

Since 0 and 1 are the only complex numbers satisfying $x^2 = x$, and we need the sum and product of $\rho(1,0)$ and $\rho(0,1)$ to be 1 and 0, respectively, we see that there are two solutions: $\rho(1,0) = 1$ and $\rho(0,1) = 0$, or $\rho(0,1) = 1$ and $\rho(1,0) = 0$. The fact that there are two solutions corresponds to the fact that C_2 has two isomorphism classes of representations.

Example 6.12. Recall that for any finite group G, we defined the the regular representation $(V_{\text{reg}}, \rho_{\text{reg}})$, and that the vector space V_{reg} is the same as the underlying vector space of $\mathbf{C}[G]$. Viewing V_{reg} as a $\mathbf{C}[G]$-modules, the action map

$$\mathbf{C}[G] \times V_{\text{reg}} \to V_{\text{reg}}$$

is the same as the multiplication map

$$\mathbf{C}[G] \times \mathbf{C}[G] \to \mathbf{C}[G]$$

We can extend this example a bit: for any algebra A, we can construct an A-module with underlying vector space A by defining the structure map

$$\begin{aligned} \rho : A &\to \operatorname{Hom}(A, A) \\ a &\mapsto m_a \end{aligned}$$

where $m_a : A \to A$ denotes the "multiplication by a" map sending $b \mapsto ab$. So A is acting on itself by left multiplication.

6.3 Module homomorphisms

Definition 6.13. Let A be an algebra and let M, N be A-modules. A *homomorphism* of A-modules (or an *A-linear map*) is a linear map $f : M \to N$ such that $f(am) = af(m)$ for all $a \in A$, $m \in M$.

We write $\operatorname{Hom}_A(M, N) := \{f : M \to N | f \text{ is } A - \text{linear}\}$. It is a subset of $\operatorname{Hom}(M, N)$, and it is easy to check that it is a vector subspace. If $M = N$, it is actually a subalgebra, because the composition of two A-linear maps is A-linear.

Now we check that if A is a group algebra, then homomorphisms of modules are the same as homomorphisms of representations

Proposition 6.14. *Let G be a finite group. Let $A = \mathbf{C}[G]$ and let M and N be A-modules, corresponding to representations (M, ρ_M) and (N, ρ_N). Then* $\operatorname{Hom}_A(M, N) = \operatorname{Hom}(M, N)^G$.

Proof. Suppose $f : M \to N$ is A-linear. In particular, it is a linear transformation and we need to check that it is G-linear. But

$$f(\rho_M(g)m) = f([g] \cdot m) = [g] \cdot f(m) = \rho_N(g)(f(m))$$

for all $g \in G$, $m \in M$, so this follows.

Conversely, suppose $f : M \to N$ is G-linear. Then f is linear and

$$f((\sum_{g\in G} \lambda_g[g])m) = f(\sum_{g\in G} (\lambda_g[g]\cdot m)) = f(\sum_{g\in G} \lambda_g \rho_M(g)(m)) = \sum_{g\in G} \lambda_g \rho_N(g)(f(m)) = (\sum_{g\in G} \lambda_g[g])\cdot f(m)$$

so f is A-linear. $\square$

6.4 Direct sums, submodules, and simple modules

Let A be an algebra and let M and N be A-modules. Then $M \oplus N$ is also an A-module if we define the action

$$A \times (M \oplus N) \to M \oplus N$$
$$a \cdot (m, n) = (a \cdot m, a \cdot n)$$

If $A = \mathbf{C}[G]$, then this corresponds to taking direct sums of representations.

There are inclusion maps $i_M : M \to M \oplus N$, $i_N : N \to M \oplus N$ and projection maps $p_M : M \oplus N \to M$, $p_N : M \oplus N \to N$, and they are module homomorphisms.

Exercise 6.15. Let A be an algebra and let L, M, N be A-modules. Prove that $\mathrm{Hom}_A(L \oplus M, N) \cong \mathrm{Hom}_A(L, N) \oplus \mathrm{Hom}_A(M, N)$ and $\mathrm{Hom}_A(L, M \oplus N) \cong \mathrm{Hom}_A(L, M) \oplus \mathrm{Hom}_A(L, N)$.

We can also define *submodules*, which correspond to subrepresentations:

Definition 6.16. Let A be an algebra and let M be an A-module, with $\rho : A \to \mathrm{Hom}(M, M)$ the structure map. A *submodule* of M is a vector subspace $M' \subset M$ such that $\rho(a)(m') \in M'$ for all $a \in A$, $m' \in M'$.

So a submodule is a vector supspace which is also stable under the action of A. The restricted action of A defines a structure map $\rho' : A \to \mathrm{Hom}(M', M')$.

Exercise 6.17. Let A be an algebra and let $f : M \to N$ be a homomorphism of A-modules. Then $\ker(f) \subset M$ and $\mathrm{im}(f) \subset N$ are submodules of M and N, respectively.

We claim that if $A = \mathbf{C}[G]$, then a submodule $M' \subset M$ is a subrepresentation of (M, ρ_M). Indeed,

$$\rho_M(g)(m') = [g] \cdot m' \in M'$$

for all $g \in G$ and $m' \in M'$, so M' is preserved by $\rho_M(g)$ for all $g \in G$. Conversely, suppose $M' \subset M$ is a subrepresentation. Then

$$(\sum_{g \in G} \lambda_g [g]) \cdot m' = \sum_{g \in G} \lambda_g \rho_M(g)(m') \in M'$$

for all $m' \in M'$ and all $\lambda_g \in \mathbf{C}$. Since every element $a \in A$ can be written as a linear combination of $\{[g]\}_{g \in G}$, this shows that $M' \subset M$ is a submodule.

Definition 6.18. Let A be an algebra. An A-module M is said to be *simple* if it contains no proper non-zero submodules.

Definition 6.19. Let A be an algebra and let M be an A-module. If $m \in M$, then *the submodule generated by* m is the set $A \cdot m := \{a \cdot m | a \in A\}$. It is a submodule because $b \cdot (a \cdot m) = (ba) \cdot m$.

Lemma 6.20. *Suppose M is a simple A-module and suppose $m \in M$ is non-zero. Then $A \cdot m = M$. Conversely, suppose that for every non-zero element $m \in M$, $A \cdot m = M$. Then M is a simple A-module.*

Proof. Since $A \cdot m \subset M$ is a submodule, it is either $\{0\}$ or M. But $1_A \cdot m = m \neq 0$, so $A \cdot m \neq \{0\}$, so $A \cdot m = M$.

Conversely, suppose we have a non-zero submodule $M' \subset M$. Then for some non-zero $m' \in M'$, $A \cdot m'$ is a submodule of M', not just M. Therefore, $A \cdot m' = M \subset M'$ and $M' = M$. $\square$

Example 6.21. Suppose M is 1-dimensional. Then M is simple because there are no proper non-zero vector subspaces.

Example 6.22. Suppose $A = \mathbf{C}[G]$ for some finite group G. Then an A-module M is simple if and only if the representation (M, ρ_M) is irreducible.

Example 6.23. Let $A = \mathrm{Mat}_d(\mathbf{C})$ and let $M = \mathbf{C}^{\oplus d}$. We make M into an A-module via the usual action of matrices on column vectors. Thus, we get a structure map $\rho : \mathrm{Mat}_d(\mathbf{C}) \to \mathrm{Hom}(\mathbf{C}^{\oplus d}, \mathbf{C}^{\oplus d})$ by setting $\rho(P)(v) := P \cdot v$ (this is actually an isomorphism!).

Then M is a simple A-module. Indeed, suppose $M' \subset M$ is an A-submodule. If $M' \neq \{0\}$, then after changing basis, we may assume that M' contains the first standard basis vector v_1. For each $v \in \mathbf{C}^{\oplus d}$, there is a matrix P_v such that $P_v \cdot v_1 = v$. Thus, $A \cdot v_1 = M \subset M'$. So the only non-zero submodule of $\mathbf{C}^{\oplus d}$ is $\mathbf{C}^{\oplus d}$ itself.

Remark 6.24. Suppose A is an algebra which finite-dimensional as a complex vector space, and suppose M is a simple A-module. Then for any $m \in M$, $A \cdot m = M$, so the map

$$\begin{aligned} A &\to M \\ a &\mapsto a \cdot m \end{aligned}$$

is a surjective linear map of vector spaces. So M is also finite-dimensional over $\mathbf{C}$.

Example 6.25. Here is an example of submodules that do not come from direct sums. Let A be the 2-dimensional algebra $\mathbf{C}[x]/x^2$ with basis $\{1, x\}$, unit 1, and multiplication defined by $x^2 = 0$.

Let M be A, considered as a module over itself. Then $A \cdot x \subset M$ is a non-zero submodule. But

$$(\lambda + \mu x) \cdot x = \lambda x + \mu x^2 = \lambda x$$

so as a vector subspace of M, $A \cdot x = \langle x \rangle$.

If $M = A \cdot x \oplus M'$, then $M' \subset M$ must be a 1-dimensional subspace such that $M' \cap A \cdot x = \{0\}$. In other words, as a vector space $M' = \langle \lambda + \mu x \rangle$ with $\lambda \neq 0$. But $(\lambda' + \mu' x) \cdot (\lambda + \mu x) = \lambda'\lambda + (\lambda'\mu + \lambda\mu')x$ — this is not an element of $\langle \lambda + \mu x \rangle$ unless $\mu' = 0$. So there is no equivalent of Maschke's theorem for modules over a general algebra.

We can classify all simple A-modules, though. Suppose M is a simple A-module. Since A is commutative, $x \cdot M := \{x \cdot m | m \in M\} \subset$ is a submodule of M (since $a \cdot (x \cdot m) = x \cdot (a \cdot m)$). Since M is simple, either $x \cdot M = \{0\}$ or $x \cdot M = M$. If the latter holds, then we may conclude that

$$x^2 \cdot M = x \cdot (x \cdot M) = x \cdot M = M$$

But $x^2 = 0$, so $x^2 \cdot M = M = \{0\}$.

Thus, if $M \neq \{0\}$, we must have $x \cdot m = 0$ for all $m \in M$, and the action of A is given by $(\lambda + \mu x) \cdot m = \lambda \cdot m$. If $\dim M > 1$, then M clearly has proper non-zero submodules. Thus, the simple A-modules are 1-dimensional vector spaces with $x \in A$ acting as 0.

Now that we have defined submodules and simple modules, we can state a generalization of Schur's lemma:

Theorem 6.26.
1. *Let A be an algebra and let M, N be simple A-modules. If $f : M \to N$ is a homomorphism of A-modules, then either $f = 0$ or f is an isomorphism.*
2. *Suppose A is an algebra which is finite-dimensional as a complex vector space. Let M be a simple A-module. Then an A-linear map $f : M \to M$ is multiplication by a scalar $\lambda \in \mathbf{C}$.*

Proof. The proofs are virtually the same as for G-linear maps of irreducible representations:

1. $\ker(f) \subset M$ and $\mathrm{im}(f) \subset N$ are submodules of M and N respectively, and since M and N are assumed simple, they are both either 0 or all of M or N.
2. Since A is finite-dimensional, so is M. Then f has an eigenvalue $\lambda \in \mathbf{C}$, so $\lambda 1_M - f : M \to M$ is an A-linear map which is not an isomorphism. Since M is assumed simple, $\lambda 1_M - f = 0$, which implies $f = \lambda 1_M$.

□

Remark 6.27. There was an early exercise to describe $\mathrm{Hom}(V^{\oplus r}, V^{\oplus r})^G$ for an irreducible representation (V, ρ_V) of G. We can now generalize this to state that for a finite-dimensional algebra A and a simple A-module M,

$$\mathrm{Hom}_A(M^{\oplus r}, M^{\oplus r}) \cong \mathrm{Mat}_r(\mathbf{C})$$

as algebras.

6.5 Semisimple modules and algebras

Definition 6.28. An A-module M is *semisimple* if it is isomorphic to the direct sum of simple A-modules.

Maschke's theorem states that if $A = \mathbf{C}[G]$, then every A-module is semisimple. But if $A = \mathbf{C}[x]/x^2$, then A is not semisimple as a module over itself.

Lemma 6.29. *If M is a semisimple A-module, then its decomposition into simple modules is unique, up to reordering.*

Proof. The proof is identical to the proof of Theorem 3.1 — if M' is a simple A-module, then $\dim \mathrm{Hom}_A(M', M)$ is the multiplicity of M' in any decomposition of M. $\square$

Lemma 6.30. *Let A be an algebra and let M be an A-module. Suppose that there is an isomorphism $\alpha : M \xrightarrow{\sim} N_1 \oplus \cdots \oplus N_r$, where the N_i are simple A-modules. If $L \subset M$ is a submodule, then there is a subset $I \subset \{1, \ldots, r\}$ such that $\alpha^{-1}(\oplus_{i\in I} N_i)$ is a complementary submodule to L.*

Proof. Let $I \subset \{1, \ldots, r\}$ be a maximal subset such that $\alpha^{-1}(\oplus_{i\in I} N_i) \cap L = \{0\}$. To prove the lemma, it suffices to show that $\alpha^{-1}(\oplus_{i\in I} N_i)$ and L together span M. Let X denote their span.

If $j \in I$, then $\alpha^{-1}(N_j) \subset X$, by construction. If $j \notin I$, consider $\alpha^{-1}(N_j) \cap X$. Since N_j is simple, either $\alpha^{-1}(N_j) \cap X = \{0\}$ or $\alpha^{-1}(N_j) \cap X = \alpha^{-1}(N_j)$. In the first case, $\alpha^{-1}(N_j) \cap L = \{0\}$, contradicting the maximality of I. Therefore $\alpha^{-1}(N_j) \cap X = \alpha^{-1}(N_j)$ and $\alpha^{-1}(N_j) \subset X$. Thus, $X \supset M$ and we are done. $\square$

Proposition 6.31. *Let A be an algebra and let M be a finite-dimensional semisimple A-module. Then any submodule $M_1 \subset M$ is also semisimple.*

Proof. We may write $\alpha : M \xrightarrow{\sim} N_1 \oplus \cdots \oplus N_r$, where the N_i are simple A-modules. Then M_1 has a complement $M_2 \subset M$ such that $\alpha|_{M_2} : M_2 \xrightarrow{\oplus}_{i\in I} N_i$ for some $I \subset \{1, \ldots, r\}$. Then there is a map $\beta : M \to \oplus_{i\notin I} N_i$ with kernel M_2. Since $M_1 \cap M_2 = \{0\}$ by definition, $\beta|_{M_1} \to \oplus_{i\notin I} N_i$ is an isomorphism and M_1 is semisimple. $\square$

Corollary 6.32. *A finite-dimensional A-module M is semisimple if and only if every submodule $L \subset M$ has a complementary submodule $L' \subset M$.*

Proof. We have seen that if M is semisimple, then every submodule $L \subset M$ has a complementary submodule $L' \subset M$.

To show the converse, we proceed by induction on $\dim M$. If $\dim M = 1$, then M is simple and therefore semisimple. Suppose that $\dim M = d$ and we know the corollary if $\dim M \leq d - 1$. If M is simple, we are done. If not, M has a proper non-zero submodule $M_1 \subset M$; by passing to a smaller submodule of M_1 if necessary, we may assume that M_1 is simple. There is a complementary submodule $M' \subset M$ such that $M_1 \oplus M' \xrightarrow{\sim} M$, and $0 < \dim M' < \dim M$.

We claim that every submodule $L \subset M'$ admits a complementary submodule $L' \subset M'$. Granting this, the inductive hypothesis implies that M' is the direct sum of simple A-modules. Since $M \cong M' \oplus M_1$, we are done.

Now we prove the claim. Recall that there are A-linear projection and inclusion maps $p_1 : M \to M_1$ and $i_1 : M_1 \to M$. Now we observe that $L \oplus M_1 \subset M$, so there is a complementary submodule $N \subset M$. We define $L' := \{n - i_1(p_1(n)) : n \in N\}$, and we claim that L' is a complementary submodule of $L \subset M'$.

We check first that $L' \subset M'$ and L' is a submodule. But $p_1(n - i_1(p_1(n))) = 0$, so $L' \subset M'$. Furthermore, L' is by definition the image of the map $\mathbf{1}_M - i_1 \circ p_1 : N \to M'$, and since $\mathbf{1}_M$, i_1, and p_1 are A-linear, so is $(\mathbf{1}_M - i_1 \circ p_1)|_N$, and its image is an A-module.

We next check that $L' \cap L = \{0\}$. But if $m \in L' \cap L$, then $m = n - i_1(p_1(n))$ for $n \in N$; then $i_1(p_1(n)) \in M_1$ and $n \in N$ is the sum of an element of L and an element of M_1. Since N is the complement of $L \oplus M_1$, this implies that $m = 0$.

Finally, we check that the natural map $L' \oplus L \to M'$ is an isomorphism. This map is injective, so it suffices to check that $\dim L' + \dim L = \dim M'$. Since $\dim N + \dim L = \dim M - \dim M_1 = \dim M'$, it further suffices to show that $\mathbf{1}_M - i_1 \circ p_1 : N \to M'$ is injective, so that $\dim L' = \dim N$. But if $m = i_1(p_1(m))$, then $m \in M_1$. Since $M_1 \cap N = \{0\}$, the restriction of $\mathbf{1}_M - i_1 \circ p_1$ to N is injective and we are done. □

Definition 6.33. Let A be an algebra. We say that A is semisimple if A is semisimple as a module over itself.

Example 6.34.

1. Let $A = \mathbf{C}[G]$. Then as a module over itself, $A \cong V_{\text{reg}}$, which decomposes as the direct sum of A-modules (corresponding to irreducible representations of G).
2. Let $A = \text{Mat}_d(\mathbf{C})$. Then if we consider matrix multiplication, left multiplication by $P \in A$ preserves columns of matrices. Thus, if we let N_i denote the ith column vectors, $A \cong V_1 \oplus \cdots V_d$ as an A-module.
3. On the other hand, $A = \mathbf{C}[x]/x^2$ is not semisimple, because $A \cdot x \subset A$ has no complementary submodule.
4. If A and B are semisimple algebras, then so is $A \oplus B$.

Proposition 6.35. *Let A be a finite-dimensional semisimple algebra. Then every finite-dimensional A-module M is semisimple.*

Proof. Let $m_1, \ldots, m_r$ be a basis for M. Then $m_1, \ldots, m_r$ generate M as an A-module, in the sense that the map

$$\begin{aligned} p : A^{\oplus r} &\to M \\ (a_1, \ldots, a_r) &\mapsto \sum_i a_i \cdot m_i \end{aligned}$$

is surjective. But $A^{\oplus r}$ is isomorphic to the direct sum of simple A-modules, so it is semisimple. Therefore, $\ker(p) \subset A^{\oplus r}$ has a complementary submodule $N \subset A^{\oplus r}$, which is also semisimple. But then the restriction $p|_N : N \to M$ is an isomorphism, and thus M is semisimple. □

Theorem 6.36. *Let A be a finite-dimensional semisimple algebra. Then there are finitely many isomorphism classes of simple A-modules. If $M_1, \ldots, M_r$ is a complete list of non-isomorphic simple A-modules, then there is an isomorphism of A-modules $A \cong \oplus_i M_i^{\dim M_i}$.*

Proof. The proof is virtually identical to the decomposition of the regular representation (which is the case $A = \mathbf{C}[G]$ for some finite group G). One checks that if $A \cong \oplus_i M_i^{d_i}$, then $d_i = \dim \mathrm{Hom}_A(A, M_i) = \dim M_i$. □

The semisimple algebra $\mathrm{Mat}_d(\mathbf{C})$ is particularly simple. As a module over itself, it is the direct sum of copies of $\mathbf{C}^{\oplus d}$ (viewed as the space of column vectors. Since every simple $\mathrm{Mat}_d(\mathbf{C})$-module appears as a summand of $\mathrm{Mat}_d(\mathbf{C})$, $V := \mathbf{C}^{\oplus d}$ is the only simple $\mathrm{Mat}_d(\mathbf{C})$-module (up to isomorphism). In addition, we can define an equivalence between finite-dimensional complex vector spaces and finite-dimensional $\mathrm{Mat}_d(\mathbf{C})$-modules.

If M is a finite-dimensional $\mathrm{Mat}_d(\mathbf{C})$-module, it is semisimple and therefore isomorphic (as a module) to $V^{\oplus s}$ for some s. Then $\mathrm{Hom}_A(V, M) \cong \mathrm{Hom}_A(V, V)^{\oplus s} \cong \mathbf{C}^{\oplus s}$.

On the other hand, if W is a finite-dimensional complex vector space we can make the tensor product $V \otimes W$ into a $\mathrm{Mat}_d(\mathbf{C})$-module by setting $a \cdot v \otimes w = (a \cdot v) \otimes w$.

This is an example of a concept called *Morita equivalence.*

Our next goal is to prove that every finite-dimensional semisimple algebra A is isomorphic to a direct sum of matrix algebras.

Lemma 6.37. *For any algebra A, $A^{op} \cong \mathrm{Hom}_A(A, A)$.*

Proof. If we view A as a left A-module over itself, right multiplication by $a \in A$ is an A-linear map

$$m_a : A \to Ab \qquad\qquad \mapsto ba$$

Moreover, every A-linear map $A \to A$ arises in this way: Given $f : A \to A$ which is A-linear,

$$f(b) = f(b \cdot 1_A) = b \cdot f(1_A)$$

so f is uniquely determined by its evaluation at 1_A.

Thus, we have constructed an isomorphism of vector spaces $A^{op} \to \mathrm{Hom}_A(A, A)$. We need to check that it is an algebra homomorphism. But

$$m^{op}(a, a') \mapsto (m_{a'a} : b \mapsto ba'a) = m_a \circ m_{a'}$$

as desired. □

Lemma 6.38. *Let V be a finite-dimensional complex vector space. Then* $\mathrm{Hom}(V, V)^{op}$ *is naturally isomorphic to* $\mathrm{Hom}(V^*, V^*)$*.*

Proof. Given $f \in \mathrm{Hom}(V, V)$, recall that we have defined $f^* \mathrm{Hom}(V^*, V^*)$ via $f^*(g) := g \circ f$, where $g \in V^*$. Then $f \mapsto f^*$ is an isomorphism of vector spaces, and since $(f_1 \circ f_2)^*(g) = g \circ (f_1 \circ f_2) = f_2^*(f_1^*(g))$, $(f_1 \circ f_2)^* = f_2^* \circ f_1^*$ and it is an isomorphism of algebras. $\square$

In particular, this lemma implies that the opposite of a matrix algebra is a matrix algebra, though an isomorphism between the two depends on a choice of basis.

Theorem 6.39 (Artin–Wedderburn)**.** *Let A be a finite-dimensional semisimple algebra. Then A is isomorphic to a direct sum of matrix algebras.*

Proof. Let M_i be a simple A-module. Then we have seen that $A \cong \oplus_i M_i^{\oplus \dim M_i}$. But then

$$\begin{aligned} A^{op} &\cong \mathrm{Hom}_A(A, A) \cong \oplus_{i,j} \mathrm{Hom}_A(M_i^{\oplus \dim M_i}, M_j^{\oplus \dim M_j}) \cong \oplus_i \mathrm{Hom}_A(M_i^{\oplus \dim M_i}, M_i^{\oplus \dim M_i}) \\ &\cong \oplus_i \mathrm{Mat}_{\dim M_i}(\mathbf{C}) \end{aligned}$$

Since the opposite of a matrix algebra is a matrix algebra, this shows that A is isomorphic to the direct sum of matrix algebras. $\square$

In particular, group algebras are direct sums of matrix algebras. But our construction depended on a choice of decomposition of A into simple modules.

We can actually be a bit more precise. Let $M_1, \ldots, M_r$ be a complete list of non-isomorphic simple A-modules, and let $\rho_i : A \to \mathrm{Hom}(M_i, M_i)$ be the structure map.

Corollary 6.40. *Let $\rho := \oplus_i \rho_i : A \to \oplus_i \mathrm{Hom}(M_i, M_i)$ be the direct sum of the ρ_i. This is an isomorphism of algebras.*

Proof. Both sides have the same dimension, namely $\sum_i (\dim M_i)^2$. Thus, to show it is an algebra isomorphism, it suffices to show it is injective. If $\rho(a) = 0$ for $a \in A$, then $\rho_i(a) = 0$ for all i. But since A is isomorphic (as a module) to a direct sum of copies of the M_i, this implies that multiplication by a is the zero map on A. In particular, $a = a \cdot 1_A = 0$. $\square$

Example 6.41. Consider $A = \mathbf{C}[C_2]$. We know there are two simple A-modules up to isomorphism, both 1-dimensional, corresponding to the two irreducible representations of C_2. If M_1 corresponds to the trivial representation and M_2 corresponds to the non-trivial representation, then $\rho_1 : \mathbf{C}[C_2] \to \mathrm{Hom}(M_1, M_1) \cong \mathbf{C}$ is given by sending $[g] \mapsto 1$ and $\rho_2 : \mathbf{C}[C_2] \to \mathrm{Hom}(M_2, M_2) \cong \mathbf{C}$ is given by sending $[g] \mapsto -1$. The direct sum of these two maps is

$$\begin{aligned} \rho : \mathbf{C}[C_2] &\to \mathbf{C} \oplus \mathbf{C} \\ 1 &\mapsto (1, 1) \\ [g] &\mapsto (1, -1) \end{aligned}$$

which is exactly the isomorphism we wrote down at the beginning.

Example 6.42. Let $A = \mathbf{C}[S_3]$. There are three irreducible representations of S_3: the trivial representation V_{triv}, the sign representation V_{sign}, and a 2-dimensional representation W. If we choose an appropriate basis for W, the representation is given by

$$(1\ 2\ 3) \mapsto \left(\begin{smallmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{smallmatrix}\right)$$
$$(2\ 3) \mapsto \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$$

where $\omega = e^{2\pi i/3}$.

So the map $\rho : \mathbf{C}[S_3] \to \mathbf{C} \oplus \mathbf{C} \oplus \mathrm{Mat}_2(\mathbf{C})$ is given by

$$(1\ 2\ 3) \mapsto (1, 1, \left(\begin{smallmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{smallmatrix}\right))$$
$$(2\ 3) \mapsto (1, -1, \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right))$$

6.6 The center of an algebra

Definition 6.43. Let A be an algebra. The *center* of A is defined to be

$$Z(A) := \{z \in A : az = za \text{ for all } a \in A\}$$

The center is a commutative subalgebra of A.

Proposition 6.44. *Let V be a finite-dimensional vector space and let $A := \mathrm{Hom}(V, V)$. Then $Z(A) = \{\lambda \mathbf{1}_V : \lambda \in \mathbf{C}\}$.*

Proof. If we choose a basis for V, A becomes a matrix algebra. Let e_{ij} be the matrix with a 1 in the (i, j) spot and 0s elsewhere. By considering the matrices which commute with all of the e_{ij}, the result follows. □

Corollary 6.45. *Let A be a finite-dimensional semisimple algebra. Then $Z(A)$ is isomorphic as an algebra to $\mathbf{C}^{\oplus r}$, where r is the number of isomorphism classes of simple A-modules.*

Proof. We have seen that A is isomorphic to $\oplus_i \mathrm{Hom}(M_i, M_i)$, where $M_1, \ldots, M_r$ is a complete list of non-isomorphic simple A-modules. It is clear that for any algebras B, B', $Z(B \oplus B') \cong Z(B) \oplus Z(B')$, so $Z(A) \cong \mathbf{C}^{\oplus r}$. □

Now we return to the setting of group algebras. If $A = \mathbf{C}[G]$ for a finite group G, this corollary shows that $Z(A) \cong \mathbf{C}^{\oplus r}$, where r is the number of isomorphism classes of irreducible representations of G.

Proposition 6.46. *Let $A = \mathbf{C}[G]$. Then $Z(A)$ is spanned by the elements $z_{C(g)} := \sum_{h \in C(g)} [h]$, where $C(g)$ denotes the conjugacy class of g.*

Proof. We may write an element $a \in \mathbf{C}[G]$ as $a = \sum_{g \in G} \lambda_g [g]$. Then $a \in Z(A)$ if and only if $[g']a = a[g']$ for all $g' \in G$. But this holds if and only if

$$\sum_{g \in G} \lambda_g [g] = \sum_{g \in G} \lambda_g [g' g g'^{-1}] \Leftrightarrow \lambda_g = \lambda_{g'^{-1} g g'} \text{ for all } g, g' \in G$$

But this is equivalent to

$$a = \lambda_{g_1} z_{C(g_1)} + \ldots + \lambda_{g_r} z_{C(g_r)}$$

where $g_1, \ldots, g_r$ are representatives of the conjugacy classes of G. □

But now we have shown that $\dim Z(\mathbf{C}[G])$ is equal to the number of conjugacy classes of G. We can finally prove that character tables are square:

Corollary 6.47. *Let G be a finite group. Then the number of isomorphism classes of irreducible representations of G is equal to the number of conjugacy classes of G.*

Proof. Both of these numbers are equal to the dimension of $Z(\mathbf{C}[G])$:

We have seen that $A \cong \oplus_{i=1}^r \operatorname{Hom}(M_i, M_i)$, where the M_i run over distinct irreducible representations, so $\dim Z(\mathbf{C}[G]) = r$.

On the other hand, we have proved that $\{z_{C(g)}\}$ span $Z(\mathbf{C}[G])$, so $\dim Z(\mathbf{C}[G])$ is equal to the number of conjugacy classes of G. □

7 Burnside's Theorem

This material is not examinable. We would like to finally apply representation theory to prove something about finite groups.

Theorem 7.1 (Burnside)**.** *Let G be a finite group of size $p^a q^b$ where p, q are distinct primes and $a, b \in \mathbf{N}$ with $a + b \geq 2$.*

Before we start proving this, we make some definitions about algebraic numbers.

Definition 7.2. Let $\alpha \in \mathbf{C}$. We say that α is an *algebraic number* if there is a polynomial $p(x) \in \mathbf{Q}[x]$ with rational coefficients such that $p(\alpha) = 0$. A polynomial $p(x)$ is said to be *monic* if $p(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$. We say that $\alpha \in \mathbf{C}$ is an *algebraic integer* if there is a monic polynomial $p(x) \in \mathbf{Z}[x]$ with integer coefficients such that $p(\alpha) = 0$.

If $\alpha \in \mathbf{C}$ is an algebraic number, there is a monic polynomial $p(x) \in \mathbf{Q}[x]$ of minimal degree having α as a root; $p(x)$ is unique and irreducible, and we call it the *minimal polynomial* of α. If $\alpha \in \mathbf{C}$ is an algebraic integer, its minimal polynomial has coefficients in $\mathbf{Z}$. The roots of $p(x)$ are called the *conjugates* of α.

Example 7.3. 1. The minimal polynomial of i is $x^2 + 1$, so i is actually an algebraic integer. The only other conjugate of i is $-i$.

2. More generally, if ζ is an nth root of 1, then ζ is a root of $x^n - 1 = 0$ so ζ is an algebraic integer. The minimal polynomial of ζ divides $x^n - 1$, so all of the conjugates of ζ are also nth roots of 1 (but not all nth roots of 1 are conjugates of ζ! the conjugates are the other roots of the *minimal* polynomial)

3. If $n \in \mathbf{Z}$, $n \neq 0$, then $1/n$ is an algebraic number (because it is a root of $nx - 1$), but not an algebraic integer. In fact, if $\alpha = m/n \in \mathbf{Q}$ with m and n coprime and $n > 1$, then α is a root of the polynomial $nx - m$, so $x - m/n$ is its minimal polynomial. Since it doesn't have integer coefficients, α is not an algebraic integer.

4. If $\alpha = \frac{1+\sqrt{5}}{2}$, then α is a root of $x^2 - x - 1$, so it is an algebraic integer.

We will need a couple of facts about algebraic numbers:

- If $\alpha, \beta \in \mathbf{C}$ are both algebraic numbers, then $\alpha\beta$ and $\alpha + \beta$ are also algebraic numbers. Similarly, if $\alpha, \beta \in \mathbf{C}$ are both algebraic integers, then so are $\alpha\beta$ and $\alpha + \beta$.

- If α and β are algebraic numbers, then the conjugates of $\alpha + \beta$ are of the form $\alpha' + \beta'$, where α' and β' are conjugates of α and β, respectively. If $r \in \mathbf{Q}$, then the conjugates of $r\alpha$ are of the form $r\alpha'$, where α' is a conjugate of α.

Lemma 7.4. *Let G be a finite group and let $\chi : G \to \mathbf{C}$ be a character of a representation of G. Then*

1. *For every $g \in G$, $\chi(g)$ is an algebraic integer*

2. *If $0 < |\chi(g)/\chi(e)| < 1$, then $\chi(g)/\chi(e)$ is not an algebraic integer.*

3. *If χ is an* irreducible *character and $g \in G$, then $|C(g)|\frac{\chi(g)}{\chi(e)}$ is an algebraic integer.*

Proof. 1. Recall that $\chi(g)$ is the sum of roots of 1. Indeed, if (V, ρ_V) is a representation such that $\chi = \chi_V$, then for any $g \in G$, we can choose a basis of V so that $\rho_V(g) = (\lambda_{ij})_{i,j}$ is diagonal (this follows by restricting ρ_V to the abelian group $\langle g \rangle \subset G$, and using the corollary to Schur's lemma that representations of abelian groups are direct sums of 1-dimensional representations). Since g has finite order, so does $\rho_V(g)$, and so there is some $n \geq 1$ such that $\lambda_{ii}^n = 1$ for all i. Therefore, $\chi(g)$ is the sum of algebraic integers, so is an algebraic integer itself.

2. The conjugates of $\chi(g)/\chi(e)$ all have the form $(\zeta_1' + \ldots + \zeta_d')/d$, which also satisfies $|(\zeta_1' + \ldots + \zeta_d')/d| \leq 1$. If $p(x) = x^n + \ldots + a_0 \in \mathbf{Z}[x]$ is the minimal polynomial of $\chi(g)/\chi(e)$, then $\pm a_0$ is the product of $\chi(g)/\chi(e)$ and all of its conjugates, and so $|a_0| < 1$. But we assumed that $p(x)$ has integer coefficients, so $a_0 = 0$. Moreover, since $p(x)$ is a minimal polynomial, it is irreducible, so $p(x) = x$, and therefore $\chi(g)/\chi(e) = 0$, contradicting our assumption that $0 < |\chi(g)/\chi(e)|$.

3. Let (V, ρ_V) be the irreducible representation such that $\chi = \chi_V$. Let $z = \sum_{h \in C(g)} [h] \in \mathbf{C}[G]$, so that $z \in Z(\mathbf{C}[G])$ by 6.46. It follows that multiplication by z defines a module homomorphism $m_z : V \to V$; by Schur's lemma this map is multiplication by a scalar $\lambda_z \in \mathbf{C}$.

   Since $m_z : V \to V$ is a linear transformation, it has a trace. On the one hand, the trace is $\lambda_z \dim V = \lambda_z \chi(e)$. On the other hand, $m_z = \sum_{h \in C(g)} \rho_V(h)$, so $\mathrm{Tr}(m_z) = \sum_{h \in C(g)} \chi_V(g) = |C(g)|\chi_V(g)$, and $\lambda_z = |C(g)| \frac{\chi(g)}{\chi(e)}$.

   We claim that λ_z is an algebraic integer. Indeed, we can view $m_z : \mathbf{C}[G] \to \mathbf{C}[G]$ as a module homomorphism from $\mathbf{C}[G]$ to itself, and λ_z is an eigenvalue. But with respect to the standard basis of $\mathbf{C}[G]$ (namely $\{[g]\}_{g \in G}$), m_z has integer coefficients. Therefore, its characteristic polynomial is monic with integer coefficients, and since the characteristic polynomial of a matrix kills eigenvalues of that matrix, λ_z is the root of a monic polynomial with integer coefficients, and so is an algebraic integer.

□

Corollary 7.5. *Let (V, ρ_V) be an irreducible representation of G. Then $\dim V$ divides $|G|$.*

Proof. We want to show that $|G|/\chi(e)$ is an integer; it is a rational number, so it suffices to prove it is an algebraic integer. By row orthogonality,

$$\sum_{g \in G} \chi_V(g)\overline{\chi_V(g)} = |G|$$

so

$$\sum_{g \in G} \frac{\chi_V(g)}{\chi_V(e)}\overline{\chi_V(g)} = \frac{|G|}{\chi(e)}$$

But the left side is equal to the sum of terms of the form $|C(g)|\frac{\chi_V(g)}{\chi_V(e)} \cdot \overline{\chi_V(g)}$; since these are algebraic integers, so is $\frac{|G|}{\chi(e)}$. □

Theorem 7.6 (Burnside)**.** *Let G be a finite group which has a conjugacy class of size p^s where p is a prime and $s \geq 1$. Then G is not simple.*

Proof. Choose some $g \in G$ with $|C(g)| = p^s$. Since $p^s > 1$, G is not abelian and $g \neq e$. Let $\chi_1, \ldots, \chi_r$ be the irreducible characters of G (with χ_1 the trivial character).

The column orthogonality relations (applied to e and g) imply that

$$1 + \sum_{i=2}^{r} \chi_i(g)\chi_i(e) = 0$$

so

$$\sum_{i=2}^{r} \chi_i(g)\chi_i(e)/p = -1/p$$

Since $-1/p$ is not an algebraic integer, there is some i such that $\chi_i(g)\chi_i(e)/p$ is not an algebraic integer. In fact, since $\chi_i(g)$ is an algebraic integer, $\chi_i(e)/p$ is not, and in particular, $p \not| \chi_i(e)$ and $\chi_i(g) \neq 0$.

Since $\chi_i(e)$ and $|C(g)|$ are relatively prime, Bézout's identity implies that there are integers a, b such that $a\chi_i(e) + b|C(g)| = 1$. Therefore,

$$a\chi_i(g) + b|C(g)|\frac{\chi_i(g)}{\chi_i(e)} = \frac{\chi_i(g)}{\chi_i(e)}$$

The left side is an algebraic integer, so the right side must be, as well. It follows that $|\chi_i(g)| = \chi_i(e)$, and so if (V_i, ρ_i) is the irreducible representation corresponding to χ_i, then $\rho_i(g) = \lambda \cdot \mathbf{1}_V$.

Now let $H = \{h \in G : \rho_i(h) = \lambda \cdot \rho_i(e) \text{ for } \lambda \in \mathbf{C}, \lambda \neq 0\}$. Then $H \subset G$ is a normal subgroup, and since $g \in H$ and $g \neq e$, $H \neq \{e\}$.

Assume G is simple. Then $H = G$ and for every $h \in G$, $\rho_V(h)$ is multiplication by a scalar. Since V is irreducible, this implies that $\dim V = 1$. Now let $H' \subset H = G$ be the kernel of ρ_i. Since $\chi_i \neq \chi_1$, V_i is not the trivial representation and so $H' \neq G$. Since G is simple, $H' = \{e\}$ and ρ_i is a faithful representation. But an injective homomorphism $\rho_i : G \to \mathrm{GL}_1(\mathbf{C})$ to an abelian group implies that G is abelian, contradicting the assumption that it has a conjugacy class with size bigger than 1. We conclude that G is not simple. $\square$

Now we can prove Burnside's $p^a q^b$ theorem.

Proof. Recall that if $|G| = p^a$ with $a \geq 2$, then G is not simple. Indeed, if G is abelian, the result is clear. If not, then the center $Z(G) \subset G$ is a subgroup with p-power order; if G is simple and non-abelian, then $Z(G) = \{e\}$. But the sizes of the conjugacy classes of G add up to $|G|$ and have p-power order (since for any $g \in G$, the centralizer of g $Z_G(g) := \{h \in G : hg = gh\} \subset G$ is a subgroup and $|C(g)| \cdot |Z_G(g)| = |G|$); since $\{e\}$ is a conjugacy class of size 1, and the sum of the sizes of the conjugacy classes is divisible by p, there must be at least p conjugacy classes of size 1. Thus, $|Z(G)| \geq p > 1$. If we let $H \subset Z(G)$ be a cyclic subgroup of order p, then $\{e\} \subsetneq H \subsetneq G$ is a normal subgroup and so G is not simple.

Now we consider the general case. One of Sylow's theorems implies that there is a subgroup $P \subset G$ with $|P| = p^a$. Choose $g \in Z(P)$; since $Z(P) \neq \{e\}$ by the previous paragraph, we may choose $g \neq e$. Then $|C(g)| \cdot |Z_G(g)| = |G|$. Since $P \subset Z_G(g)$, $p^a \mid |Z_G(g)$ and so $|C(g)| = q^r$ for some $r \geq 0$.

If $r = 0$, then $g \in Z(G)$ so $Z(G) \neq \{e\}$ and we can find a normal subgroup $\{e\} \subsetneq H \subsetneq G$ with $H \subset Z(G)$, as above.

If $r \geq 1$, Theorem 7.6 implies that G is not simple. $\square$