

Group Representations

June 5, 2026

Preface

These notes are based on materials by [Nicolas Mascot](#) (Trinity College Dublin), [Benjamin Steinberg](#) (Carleton University), and [Alex Bartel](#) (Glasgow University).

Contents

Preface	i
1 Introduction	1
1.1 Group Actions	1
1.2 Linear Representations	2
1.3 Permutation Representations	2
1.4 Morphisms of Representations	3
1.5 New Representations from Old	4
1.6 Irreducibility and Indecomposability	6
1.7 Exercises	7
2 The Module Point of View	9
2.1 Modules over a Ring	9
2.2 Representations as Modules	10
2.3 Semi-simplicity	11
2.4 Maschke's Theorem	12
2.5 Exercises	13
3 Character Theory	16
3.1 Schur's Lemma	16
3.2 Dot Products	17
3.3 Conjugacy and Class Functions	17
3.4 Traces	17
3.5 The Character of a Representation	18
3.6 Characters on Inverses and Kernels	19
3.7 Invariants and the Character of Hom	19
3.8 Tensor Products and Symmetric Powers	20
3.9 First Orthogonality and the Main Theorem	21
3.10 Exercises	22
4 Character Tables	24
4.1 Decomposition of the Regular Representation	24
4.2 Wedderburn on $\mathbb{C}[G]$	25
4.3 The Number of Irreducible Representations	27
4.4 Isotypic Components	28
4.5 The Character Table	28
4.6 The Conjugacy Principle and Conjugacy Classes in S_n	29

4.7	Example: Character Table of S_4	30
4.8	Representations of Abelian Groups	30
4.9	Exercises	31
5	Induced Representations	34
5.1	Restriction and Induction	34
5.2	Definition(s) of the Induced Representation	34
5.3	Example: Permutation Representations	36
5.4	Induced Characters	37
5.5	Frobenius Reciprocity	38
5.6	Exercises	40
6	Fourier Analysis on Finite Groups	42
6.1	The Function Algebra $L(G)$	42
6.2	Matrix Coefficients	43
6.3	Fourier Analysis on Abelian Groups	44
6.4	Cayley Graphs and Eigenvalues	45
6.5	Fourier Analysis on Non-Abelian Groups	46
6.6	Exercises	47
7	Burnside's Theorem	50
7.1	A Little Number Theory	50
7.2	The Dimension Theorem	51
7.3	Burnside's Theorem	53
7.4	Exercises	56
A	Solutions to Exercises	57
A.1	Chapter 1	57
A.2	Chapter 2	59
A.3	Chapter 3	61
A.4	Chapter 4	63
A.5	Chapter 5	67
A.6	Chapter 6	69
A.7	Chapter 7	72

Chapter 1

Introduction

Group representation theory studies groups by letting them act on vector spaces via linear maps, thereby *representing* abstract group elements as concrete invertible matrices. This allows the full power of linear algebra to be brought to bear on group-theoretic problems. The present chapter introduces the two key notions: group actions on sets, and linear representations as group actions on vector spaces.

1.1 Group Actions

The *Erlangen programme*, introduced by Felix Klein in 1872, proposes that groups do not exist in the void—they are meant to move the points of *spaces*. We obtain a much clearer understanding of a group by specifying what it acts on.

Example 1.1. • The linear group $\mathrm{GL}_n(\mathbb{R})$ ($n \in \mathbb{N}$) moves the points of the vector space \mathbb{R}^n by matrix multiplication.

- The symmetric group S_n ($n \in \mathbb{N}$) permutes the elements of the set $\{1, 2, \dots, n\}$.
- The cyclic group $C_n = \mathbb{Z}/n\mathbb{Z}$ ($n \in \mathbb{N}$) can be thought of as the group of rotations of the plane which stabilise a regular n -gon, acting on its vertices.

Definition 1.2 (Group action). Let G be a group and X be a set. An *action* $G \curvearrowright X$ of G on X is a map

$$G \times X \longrightarrow X, \quad (g, x) \longmapsto g \cdot x,$$

satisfying

- $(gh) \cdot x = g \cdot (h \cdot x)$ for all $g, h \in G$ and $x \in X$,
- $1_G \cdot x = x$ for all $x \in X$.

Remark 1.3. The axioms imply that for each $g \in G$ the map

$$\rho_g: X \longrightarrow X, \quad x \longmapsto g \cdot x$$

is a bijection with inverse $\rho_{g^{-1}}$, since $\rho_{g^{-1}} \circ \rho_g = \rho_{1_G} = \mathrm{id}_X$. Thus an action of G on X is equivalently a group morphism $G \rightarrow \mathrm{Sym}(X)$, where $\mathrm{Sym}(X)$ denotes the group of all bijections $X \rightarrow X$.

1.2 Linear Representations

A linear representation is a group action on a set that carries the additional structure of a vector space, with the requirement that every group element acts by a linear map.

Definition 1.4 (Linear representation). Let K be a field and $n \in \mathbb{N}$. A (linear) representation of G over K of degree n is a group morphism

$$\rho: G \longrightarrow \mathrm{GL}_n(K).$$

So a representation of G is an action of G on a set which is a vector space, such that every $g \in G$ acts by a linear transformation. The elements of G are thereby *represented* by invertible matrices.

Example 1.5. • $\mathrm{GL}_n(\mathbb{R}) \curvearrowright \mathbb{R}^n$ is actually a representation of $\mathrm{GL}_n(\mathbb{R})$: the identity map $\mathrm{GL}_n(\mathbb{R}) \rightarrow \mathrm{GL}_n(\mathbb{R})$ is a group morphism of degree n over \mathbb{R} .

- The map

$$\mathbb{C}^\times \longrightarrow \mathrm{GL}_2(\mathbb{R}), \quad a + bi \longmapsto \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

is a representation of \mathbb{C}^\times of degree 2 over \mathbb{R} .

- For any field K , the map

$$(K, +) \longrightarrow \mathrm{GL}_2(K), \quad x \longmapsto \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$$

is a representation of the additive group $(K, +)$ of degree 2 over K .

- The *trivial representation*: the constant map $G \rightarrow \mathrm{GL}_1(K) = K^\times$, $g \mapsto 1$, is a degree-1 representation of any G over any field K , denoted $\mathbf{1}$. (More generally, $g \mapsto I_n$ is a degree- n representation, but “trivial” will henceforth always mean the case $n = 1$.)

Coordinate-free formulation

It is often convenient to work with a vector space V without fixing a basis.

Definition 1.6. Alternatively, a representation of G over K is a group morphism

$$\rho: G \longrightarrow \mathrm{GL}(V),$$

where V is a K -vector space and $\mathrm{GL}(V)$ denotes the group of K -linear automorphisms of V . The *degree* (or *dimension*) of the representation is $\dim_K V$.

By choosing a basis of V we obtain an isomorphism $\mathrm{GL}(V) \simeq \mathrm{GL}_{\dim V}(K)$, recovering the matrix formulation. The two definitions are therefore equivalent.

Notation 1.7. Instead of $\rho(g)(v)$ we often write $\rho_g(v)$, or simply gv when ρ is clear from context.

1.3 Permutation Representations

Every group action on a set gives rise to a linear representation in a canonical way.

Definition 1.8 (Permutation representation). Let $G \curvearrowright X$ be a group action. Define the K -vector space

$$K[X] = \left\{ \sum_{x \in X}^{\text{finite}} \lambda_x e_x \mid \lambda_x \in K \right\}$$

with formal basis $\{e_x \mid x \in X\}$ indexed by X . The formula

$$g \cdot e_x := e_{g \cdot x}, \quad g \in G, x \in X,$$

extended linearly to all of $K[X]$, defines a representation

$$\rho: G \longrightarrow \text{GL}(K[X]).$$

This is called the *permutation representation* attached to $G \curvearrowright X$. Its degree is $\#X$.

Example 1.9. Let $G = S_3$ act on $X = \{1, 2, 3\}$ in the natural way. For $\sigma = (1\ 2\ 3)$ and $\tau = (1\ 2)$ in G , we have

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

Indeed, σ sends $e_1 \mapsto e_2$, $e_2 \mapsto e_3$, $e_3 \mapsto e_1$, giving the first matrix (columns are images of basis vectors).

Definition 1.10 (Regular representation). In the special case where $X = G$ with G acting on itself by left multiplication $g \cdot x := gx$, the corresponding permutation representation $\rho: G \rightarrow \text{GL}(K[G])$ is called the *regular representation* of G over K .

The regular representation has degree $\#G$ and plays a central role in the theory: it contains every irreducible representation as a subrepresentation (a fact we will establish later).

1.4 Morphisms of Representations

Just as one studies groups via group homomorphisms, one studies representations via structure-preserving maps between them.

Equivalent representations

Let $\rho: G \rightarrow \text{GL}(V)$ be a representation of degree n over K . Picking a basis \mathcal{B}_1 of V yields a matrix representation $\rho_1: G \rightarrow \text{GL}_n(K)$; picking a different basis \mathcal{B}_2 yields $\rho_2: G \rightarrow \text{GL}_n(K)$. If $P \in \text{GL}_n(K)$ is the change-of-basis matrix from \mathcal{B}_1 to \mathcal{B}_2 , then

$$\rho_2(g) = P^{-1} \rho_1(g) P \quad \text{for all } g \in G.$$

Two representations related in this way are considered the same.

Example 1.11. Label the vertices of an equilateral triangle by 1, 2, 3. The symmetry group S_3 acts on the triangle, giving a representation $\rho: S_3 \rightarrow \text{GL}(\mathbb{R}^2)$: for $\sigma = (1\ 2\ 3)$ and $\tau = (1\ 2)$, $\rho(\sigma)$ is a

rotation by $2\pi/3$ and $\rho(\tau)$ is a reflection. With respect to the standard basis of \mathbb{R}^2 :

$$\rho_1: S_3 \rightarrow \mathrm{GL}_2(\mathbb{R}), \quad \rho_1(\sigma) = \begin{pmatrix} -1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & -1/2 \end{pmatrix}, \quad \rho_1(\tau) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

With a better-adapted basis one obtains the equivalent representation

$$\rho_2: S_3 \rightarrow \mathrm{GL}_2(\mathbb{R}), \quad \rho_2(\sigma) = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, \quad \rho_2(\tau) = \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}.$$

Definition 1.12 (Morphism of representations). Let G be a group, K a field, and $\rho_1: G \rightarrow \mathrm{GL}(V_1)$, $\rho_2: G \rightarrow \mathrm{GL}(V_2)$ two representations of G over K . A *morphism* from ρ_1 to ρ_2 is a K -linear map $T: V_1 \rightarrow V_2$ such that

$$T(\rho_1(g)(v)) = \rho_2(g)(T(v)) \quad \text{for all } g \in G, v \in V_1,$$

or equivalently, using the shorthand gv ,

$$T(gv) = gT(v).$$

In other words, the diagram

$$\begin{array}{ccc} V_1 & \xrightarrow{\rho_1(g)} & V_1 \\ T \downarrow & & \downarrow T \\ V_2 & \xrightarrow{\rho_2(g)} & V_2 \end{array}$$

commutes for every $g \in G$. An *isomorphism* of representations is a bijective morphism; isomorphic representations are also called *equivalent*.

Notation 1.13. The set of all morphisms from ρ_1 to ρ_2 is a K -vector space denoted $\mathrm{Hom}_G(V_1, V_2)$, and is also called the space of G -linear or G -equivariant maps. When $V_1 = V_2 = V$, we write $\mathrm{End}_G(V) := \mathrm{Hom}_G(V, V)$, which is a K -algebra under composition.

1.5 New Representations from Old

Definition 1.14 (Trivial representation). Let G be a group and K a field. Viewing $V = K$ as a one-dimensional vector space over itself, the *trivial representation* is the morphism

$$\mathbf{1}: G \longrightarrow \mathrm{GL}(V), \quad g \mapsto \mathrm{id}_V.$$

Every $g \in G$ acts as the identity.

Definition 1.15 (Direct sum). Let V and W be representations of G over K . Their *direct sum* $V \oplus W \simeq V \times W$ is again a representation of G , via

$$g(v, w) = (gv, gw) \quad (g \in G, v \in V, w \in W).$$

Definition 1.16 (Hom-representation and dual). Let V and W be representations of G over K . The space $\text{Hom}(V, W)$ of K -linear maps from V to W becomes a representation of G by

$$(gT)(v) = g(T(g^{-1}v)) \quad (g \in G, T \in \text{Hom}(V, W), v \in V).$$

The special case $V = W$ gives $\text{End}(V) = \text{Hom}(V, V)$. The special case $W = \mathbf{1}$ gives the *dual representation* $V^\vee = \text{Hom}(V, \mathbf{1})$, with G -action

$$(g\ell)(v) = \ell(g^{-1}v) \quad (g \in G, \ell \in V^\vee, v \in V).$$

Remark 1.17. A linear map $T \in \text{Hom}(V, W)$ is G -invariant (i.e. fixed by the G -action on $\text{Hom}(V, W)$) if and only if $T(gv) = gT(v)$ for all $g \in G$, i.e. if and only if T is a morphism of representations. Thus

$$\text{Hom}(V, W)^G = \text{Hom}_G(V, W).$$

Definition 1.18 (Tensor product of vector spaces). Let V and W be vector spaces over K . Their *tensor product* $V \otimes_K W$ is the K -vector space generated by symbols $v \otimes w$ ($v \in V, w \in W$) subject to the relations

$$\begin{aligned} (v + v') \otimes w &= v \otimes w + v' \otimes w, \\ v \otimes (w + w') &= v \otimes w + v \otimes w', \\ (kv) \otimes w &= v \otimes (kw) = k(v \otimes w), \end{aligned}$$

for all $v, v' \in V, w, w' \in W, k \in K$. Concretely, if v_1, \dots, v_n is a basis of V and w_1, \dots, w_m is a basis of W , then the nm symbols $v_i \otimes w_j$ form a basis of $V \otimes W$, so $\dim(V \otimes W) = \dim V \cdot \dim W$. A general element is a finite sum $\sum_k \tilde{v}_k \otimes \tilde{w}_k$ (not necessarily a pure tensor). Tensor product is associative and distributes over direct sums: $(U \otimes V) \otimes W \simeq U \otimes (V \otimes W)$ and $(U \oplus V) \otimes W \simeq (U \otimes W) \oplus (V \otimes W)$.

Definition 1.19 (Tensor product representation). Let V and W be representations of G over K . The vector space $V \otimes W$ becomes a representation of G via

$$g(v \otimes w) = (gv) \otimes (gw) \quad (g \in G, v \in V, w \in W),$$

extended linearly to all of $V \otimes W$. The associativity and distributivity of Definition 1.18 carry over to G -representations.

Remark 1.20 (Kronecker product). If g acts on V by the $n \times n$ matrix $A = (a_{ij})$ in a basis v_1, \dots, v_n , and on W by the $m \times m$ matrix $B = (b_{kl})$ in w_1, \dots, w_m , then g acts on $V \otimes W$ by the *Kronecker product*

$$A \otimes B = \begin{pmatrix} a_{11}B & \cdots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{n1}B & \cdots & a_{nn}B \end{pmatrix} \in \mathcal{M}_{nm}(K),$$

with respect to the basis $v_1 \otimes w_1, \dots, v_1 \otimes w_m, \dots, v_n \otimes w_1, \dots, v_n \otimes w_m$.

Proposition 1.21. For representations V and W of G there is a natural isomorphism of G -representations

$$V \otimes W \simeq \text{Hom}(V^\vee, W).$$

Proof. The linear isomorphism $\phi: V \otimes W \xrightarrow{\sim} \text{Hom}(V^\vee, W)$, $v \otimes w \mapsto (\ell \mapsto \ell(v)w)$, intertwines the G -actions: $\phi(g(v \otimes w)) = \phi(gv \otimes gw)$ is the map $\ell \mapsto \ell(gv)gw$, and $(g \cdot \phi(v \otimes w))(\ell) = g \phi(v \otimes w)(g^{-1}\ell) = g(\ell(gv)w) = \ell(gv)gw$. \square

1.6 Irreducibility and Indecomposability

Definition 1.22 (Subrepresentation). Let V be a representation of G . A *subrepresentation* of V is a subspace $W \subseteq V$ that is *stable* under G : $gw \in W$ for all $g \in G$ and $w \in W$.

Example 1.23. The subspace

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

is a subrepresentation of V , called the space of G -invariants. It is isomorphic to a direct sum of copies of the trivial representation $\mathbf{1}$. Note also that $V^G = \text{Hom}_G(\mathbf{1}, V)$.

Definition 1.24 (Irreducible representation). A representation V is *irreducible* (or *simple*) if $V \neq \{0\}$ and its only subrepresentations are $\{0\}$ and V itself.

Example 1.25. Consider again $G = S_3 \curvearrowright X = \{1, 2, 3\}$ and the permutation representation $V = K[X]$. The vector $v = e_1 + e_2 + e_3$ is fixed by every $g \in G$, so $W = \text{span}\{e_1 + e_2 + e_3\}$ is a nontrivial subrepresentation isomorphic to $\mathbf{1}$. Hence V is *not* irreducible.

Definition 1.26 (Indecomposable representation). A representation V is *indecomposable* if $V \neq \{0\}$ and it is not isomorphic to a direct sum $V_1 \oplus V_2$ with $V_1, V_2 \neq \{0\}$.

Every irreducible representation is indecomposable: if $V = V_1 \oplus V_2$ with both V_i subrepresentations, then V_1 is a subrepresentation of V , so by irreducibility $V_1 \in \{\{0\}, V\}$, and correspondingly $V_2 \in \{V, \{0\}\}$ – so one of V_1, V_2 is zero. The converse fails in general, as the next example shows.

Example 1.27. Take $G = (K, +)$ with the representation $\rho: G \rightarrow \text{GL}_2(K)$, $x \mapsto \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ from Example 1.5. The subspace spanned by the first standard basis vector e_1 is stable, giving a subrepresentation isomorphic to $\mathbf{1}$, so ρ is *reducible*. However, ρ is *indecomposable*: $\text{span}\{e_1\}$ has no G -stable complement in K^2 . Indeed, any complement would be one-dimensional, spanned by some $u = (a, b)^\top$ with $b \neq 0$. For each $x \in K$ stability requires $\rho(x)u = \mu u$ for some scalar $\mu \in K$; reading the second component gives $\mu = 1$, and the first component then yields $a + xb = a$, i.e. $xb = 0$ for all $x \in K$. Since $b \neq 0$ and K contains a non-zero element, this is impossible.

Effect on matrices

Let $\rho: G \rightarrow \text{GL}_n(K)$ be a representation. In terms of matrices:

- ρ is *reducible* if and only if there exists $P \in \text{GL}_n(K)$ such that all matrices $P^{-1}\rho(g)P$ are upper block-triangular of the form $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$.

- ρ is decomposable if and only if there exists $P \in \text{GL}_n(K)$ such that all matrices $P^{-1}\rho(g)P$ are block-diagonal of the form $\begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}$.

Example 1.28. Return once more to the permutation representation $V = K[X]$ of $G = S_3 \curvearrowright X = \{1, 2, 3\}$. We have seen that $W = \text{span}\{e_1 + e_2 + e_3\} \simeq \mathbf{1}$ is a subrepresentation. Consider its candidate complement

$$W' = \left\{ \sum_{x \in X} \lambda_x e_x \in V \mid \sum_{x \in X} \lambda_x = 0 \right\}.$$

One checks that W' is also a subrepresentation. If $3 \neq 0$ in K , then $V = W \oplus W'$ and V is decomposable. But if $K = \mathbb{Z}/3\mathbb{Z}$, then $e_1 + e_2 + e_3 \in W'$ (since $1 + 1 + 1 = 0$ in K), so $W \subset W'$ and the decomposition fails; in this case V is indecomposable.

1.7 Exercises

Exercise 1.29 (Subrepresentations of degree 1). Let G be a group, K a field, and $\rho: G \rightarrow \text{GL}(V)$ a representation over K .

1. Show that if $\deg \rho = 1$ then ρ is irreducible and indecomposable.
2. Let $W = Kv \subseteq V$ be a one-dimensional subspace ($0 \neq v \in V$). Show that W is a subrepresentation if and only if v is a common eigenvector of all $\rho(g)$, $g \in G$.
3. Suppose $K = \mathbb{C}$, G is abelian, and $0 < \dim V < \infty$. Prove that V contains a subrepresentation of degree 1.

Hint: show that if $T, U: V \rightarrow V$ commute then each eigenspace of T is stable under U ; then induct on $\dim V$.

(Solution)

Exercise 1.30 (The dihedral group D_8). Let $G = D_8$ be the symmetry group of a square in \mathbb{R}^2 : it has 8 elements, namely the identity, rotations r, r^2, r^3 (with $r^4 = \text{id}$), and reflections s, s', t, t' . This gives a natural representation $\rho: D_8 \rightarrow \text{GL}(\mathbb{R}^2)$ of degree 2.

1. Write down the matrix of each $\rho(g)$ with respect to a convenient basis (specify it).
2. Deduce that ρ is faithful.
3. Using Exercise 1.29, prove that ρ is irreducible over \mathbb{R} .
4. Viewing ρ as a representation $\rho_{\mathbb{C}}$ over \mathbb{C} (same matrices, now complex), determine whether $\rho_{\mathbb{C}}$ is irreducible.

(Solution)

Exercise 1.31 (G -linear maps form a subspace). Let $\rho_1: G \rightarrow \text{GL}(V_1)$ and $\rho_2: G \rightarrow \text{GL}(V_2)$ be representations over a field K . Prove that $\text{Hom}_G(V_1, V_2)$ is a subspace of $\text{Hom}(V_1, V_2)$. (Solution)

Exercise 1.32 (Decomposition over \mathbb{R}). Over $K = \mathbb{R}$ and $G = S_3$, consider the permutation representation $\text{Perm}: S_3 \rightarrow \text{GL}_3(\mathbb{R})$ induced by $S_3 \curvearrowright \{1, 2, 3\}$, and the representation

$$\Delta: S_3 \rightarrow \text{GL}_2(\mathbb{R}), \quad (123) \mapsto \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, \quad (12) \mapsto \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$$

obtained by labelling the vertices of an equilateral triangle.

1. Prove that Δ is irreducible. Is it indecomposable?
2. Prove that $\text{Perm} \simeq \mathbf{1} \oplus \Delta$ as representations of S_3 .

(Solution)

Exercise 1.33 (Decomposition over $\mathbb{Z}/p\mathbb{Z}$). Redo Exercise 1.32 with $K = \mathbb{Z}/p\mathbb{Z}$ (p prime) in place of \mathbb{R} : is Δ still irreducible? Is it indecomposable? Does $\text{Perm} \simeq \mathbf{1} \oplus \Delta$ still hold? The answers may depend on p ; treat all cases. (Solution)

Chapter 2

The Module Point of View

The language of modules over a ring provides a unified framework that subsumes both the theory of vector spaces and the theory of group representations. Recasting representations as modules over the group ring reveals structural properties — subrepresentations, morphisms, semi-simplicity — as instances of general module-theoretic phenomena, and leads directly to the fundamental theorem of this chapter: Maschke's theorem.

2.1 Modules over a Ring

Definition 2.1 (Module, morphism of modules). Let R be a ring. An R -module is a set M equipped with two operations

$$M \times M \rightarrow M, \quad (m, n) \mapsto m + n, \quad R \times M \rightarrow M, \quad (\lambda, m) \mapsto \lambda m,$$

such that $(M, +)$ is an abelian group, and for all $\lambda, \mu \in R$ and $m, n \in M$:

$$\lambda(\mu m) = (\lambda\mu)m, \quad 1m = m, \quad (\lambda + \mu)m = (\lambda m) + (\mu m), \quad \lambda(m + n) = (\lambda m) + (\lambda n).$$

A morphism $f: M \rightarrow N$ of R -modules is an R -linear map, meaning

$$f(m + m') = f(m) + f(m') \quad \text{and} \quad f(\lambda m) = \lambda f(m)$$

for all $m, m' \in M$ and $\lambda \in R$.

Example 2.2. • If R is a field, then an R -module is exactly an R -vector space, and a morphism of R -modules is exactly a linear map.

- For any ring R and $n \in \mathbb{N}$, the set $R^n = \{(x_1, \dots, x_n) \mid x_i \in R\}$ is an R -module under componentwise addition and scalar multiplication.
- A \mathbb{Z} -module is exactly an abelian group: the scalar multiplication is given by $ng = g + \dots + g$ (n times) for $n \in \mathbb{Z}$, $g \in G$, and a morphism of \mathbb{Z} -modules is exactly a group homomorphism.

Notation 2.3. Let R be a ring. Given two R -modules M and N , the set of morphisms from M to N is denoted $\text{Hom}_R(M, N)$; it is an abelian group under pointwise addition. In the case $M = N$ we write $\text{End}_R(M) := \text{Hom}_R(M, M)$, which is in fact a ring under composition. If R is a field and M is an R -vector space of dimension n , then $\text{End}_R(M) \simeq \mathcal{M}_n(R)$, the ring of $n \times n$ matrices over R .

Definition 2.4 (Submodule). Let M be an R -module. A *submodule* of M is a nonempty subset $N \subseteq M$ that is closed under addition and under multiplication by R .

Example 2.5. Viewing R as an R -module over itself, its submodules are precisely its *ideals*.

Proposition 2.6. Let $f: M \rightarrow N$ be a morphism of R -modules. Then $\text{Ker } f$ is a submodule of M , and $\text{Im } f$ is a submodule of N .

Proof. $\text{Ker } f$ is non-empty since $f(0) = 0$. For $m, m' \in \text{Ker } f$ and $\lambda \in R$, $f(m + m') = f(m) + f(m') = 0$ and $f(\lambda m) = \lambda f(m) = 0$, so $\text{Ker } f$ is closed under addition and scalar multiplication.

$\text{Im } f$ is non-empty since $0 = f(0) \in \text{Im } f$. For $n = f(m)$ and $n' = f(m')$ in $\text{Im } f$ and $\lambda \in R$: $n + n' = f(m + m') \in \text{Im } f$ and $\lambda n = f(\lambda m) \in \text{Im } f$. \square

Definition 2.7 (Direct sum). Let M be an R -module and $(M_i)_{i \in I}$ a collection of submodules. We say that $M = \bigoplus_{i \in I} M_i$ if every element $m \in M$ can be expressed as $m = \sum_{i \in I}^{\text{finite}} m_i$ with $m_i \in M_i$ in a *unique* way.

Example 2.8. The polynomial ring $R[x] = \bigoplus_{n \geq 0} Rx^n$ as an R -module.

Remark 2.9. For two submodules, $M = M_1 \oplus M_2$ if and only if every $m \in M$ is uniquely of the form $m = m_1 + m_2$ with $m_1 \in M_1$ and $m_2 \in M_2$, which is equivalent to $M_1 + M_2 = M$ and $M_1 \cap M_2 = \{0\}$. Indeed, if $m_1 + m_2 = m'_1 + m'_2$, then $m'_1 - m_1 = m_2 - m'_2 \in M_1 \cap M_2$.

2.2 Representations as Modules

The group ring

Definition 2.10 (Group ring). Let K be a field and G a group. Recall that

$$K[G] = \left\{ \sum_{g \in G}^{\text{finite}} \lambda_g e_g \mid \lambda_g \in K \right\} = \bigoplus_{g \in G} K e_g$$

is the K -vector space with basis $\{e_g\}_{g \in G}$. When $X = G$ is a group, $K[G]$ becomes a *ring* — the *group ring* of G over K — under the multiplication rule $e_g \cdot e_h := e_{gh}$, extended bilinearly:

$$\left(\sum_{g \in G} \lambda_g e_g \right) \left(\sum_{g \in G} \mu_g e_g \right) = \sum_{g \in G} \left(\sum_{\substack{g_1, g_2 \in G \\ g_1 g_2 = g}} \lambda_{g_1} \mu_{g_2} \right) e_g.$$

Remark 2.11. The ring $K[G]$ is commutative if and only if G is abelian. It contains a copy of K as the subring $\{\lambda e_{1_G} \mid \lambda \in K\}$.

$K[G]$ -modules and representations

The key observation is that $K[G]$ -modules are exactly representations of G over K .

More precisely, let M be a $K[G]$ -module. Then M is a K -vector space via $\lambda m := (\lambda e_{1_G})m$ for $\lambda \in K, m \in M$. The representation is then

$$\rho: G \rightarrow \text{GL}(M), \quad g \mapsto (m \mapsto e_g \cdot m).$$

Conversely, given a K -vector space V and a representation $\rho: G \rightarrow \text{GL}(V)$, we make V into a $K[G]$ -module by

$$\left(\sum_{g \in G} \lambda_g e_g \right) v := \sum_{g \in G} \lambda_g \rho(g)(v) \quad (\lambda_g \in K, v \in V).$$

These two constructions are inverse to each other. Under this correspondence:

- sub- $K[G]$ -modules = subrepresentations,
- $K[G]$ -module morphisms = morphisms of representations.

In particular, if $f: V \rightarrow W$ is a morphism of representations of G , then $\text{Ker } f \subseteq V$ and $\text{Im } f \subseteq W$ are subrepresentations. Moreover, irreducible representations correspond to *simple* $K[G]$ -modules, and indecomposable representations to *indecomposable* $K[G]$ -modules.

Definition 2.12 (Simple and indecomposable modules). Let R be a ring and M an R -module.

- M is *simple* if $M \neq \{0\}$ and its only submodules are $\{0\}$ and M .
- M is *indecomposable* if it cannot be expressed non-trivially as $M = \bigoplus_{i \in I} M_i$ with all $M_i \neq \{0\}$.

2.3 Semi-simplicity

Definition 2.13 (Semi-simple module). Let R be a ring. An R -module M is *semi-simple* if it can be decomposed as

$$M = \bigoplus_{i \in I} M_i$$

with each M_i a simple R -submodule. Since the M_i are simple, this is a “complete decomposition”. A representation is semi-simple if and only if the corresponding $K[G]$ -module is semi-simple, i.e., it is completely decomposable into irreducibles.

Definition 2.14 (Supplement). Let R be a ring, M an R -module, and $N \subseteq M$ a submodule. A *supplement* to N is a submodule $N' \subseteq M$ such that $M = N \oplus N'$.

Remark 2.15. In general, a supplement need not exist. For example, take $R = \mathbb{Z}, M = \mathbb{Z}, N = 2\mathbb{Z}$. If $\mathbb{Z} = 2\mathbb{Z} \oplus N'$, then for any $n' \in N'$ we have $2n' \in N' \cap 2\mathbb{Z} = \{0\}$, so $N' = \{0\}$, but then $2\mathbb{Z} \oplus \{0\} \neq \mathbb{Z}$.

Theorem 2.16. Let R be a ring and M an R -module. Assume there is no infinite strictly descending chain $M \supsetneq M_0 \supsetneq M_1 \supsetneq M_2 \supsetneq \dots$ of submodules. Then

$$M \text{ is semi-simple} \iff \text{every submodule of } M \text{ has a supplement.}$$

Proof. (\Leftarrow): If M is simple, there is nothing to prove. Otherwise let $\{0\} \subsetneq N \subsetneq M$ be a proper nonzero submodule; by hypothesis it has a supplement N' , so $M = N \oplus N'$. We now iterate the argument on N and on N' separately. (The hypothesis transfers: if $P \subseteq N$ is a submodule, then $P \subseteq M$ has a supplement P' in M , and one checks that $N = P \oplus (P' \cap N)$, so $P' \cap N$ is a supplement of P inside N . The DCC restricts to N as well.) The process terminates, since at each step the submodules strictly decrease, and by assumption there is no infinite descending chain.

(\Rightarrow): Write $M = \bigoplus_{i \in I} M_i$ with each M_i simple. The index set I must be finite, else we would have an infinite strictly descending chain. Let $N \subseteq M$ be any submodule. Let $J \subseteq I$ be a maximal subset such that $M' := N \oplus \bigoplus_{i \in J} M_i$ is a direct sum. We claim $M' = M$, so that $\bigoplus_{i \in J} M_i$ is a supplement to N . Indeed, if $M_i \not\subseteq M'$ for some $i \in I$, then since M_i is simple we have $M' \cap M_i = \{0\}$, so we could add i to J and still have a direct sum, contradicting maximality. \square

2.4 Maschke's Theorem

We first recall a convenient characterisation of direct sum decompositions in terms of projections.

Theorem 2.17 (Projections). *Let K be a field and V a K -vector space. If $V = V_1 \oplus V_2$, the projection onto V_1 parallel to V_2 is the map*

$$\pi: V \rightarrow V, \quad v_1 + v_2 \mapsto v_1.$$

It is linear and satisfies $\text{Im } \pi = V_1$, $\text{Ker } \pi = V_2$, and $\pi^2 = \pi$. Conversely, if $\pi \in \text{End}_K(V)$ satisfies $\pi^2 = \pi$, then $V = \text{Im } \pi \oplus \text{Ker } \pi$, and π is the projection onto $\text{Im } \pi$ parallel to $\text{Ker } \pi$.

Proof. The forward direction is routine. For the converse, suppose $\pi^2 = \pi$. For any $v \in V$, write $v = \pi(v) + (v - \pi(v))$. Clearly $\pi(v) \in \text{Im } \pi$, and $\pi(v - \pi(v)) = \pi(v) - \pi^2(v) = \pi(v) - \pi(v) = 0$, so $v - \pi(v) \in \text{Ker } \pi$. Thus $V = \text{Im } \pi + \text{Ker } \pi$. If $v \in \text{Im } \pi \cap \text{Ker } \pi$, write $v = \pi(w)$; then $v = \pi(w) = \pi^2(w) = \pi(\pi(w)) = \pi(v) = 0$. So $\text{Im } \pi \cap \text{Ker } \pi = \{0\}$ and $V = \text{Im } \pi \oplus \text{Ker } \pi$. Finally, π acts as the identity on $\text{Im } \pi$ (just shown) and as zero on $\text{Ker } \pi$, so it is the projection onto $\text{Im } \pi$ parallel to $\text{Ker } \pi$. \square

Theorem 2.18 (Maschke). *Let K be a field and G a finite group of order $n = \#G$. If $n \neq 0$ in K (i.e. $\text{char } K \nmid n$), then every representation of G over K is semi-simple.*

Example 2.19. The permutation representation $V = K[\{1, 2, 3\}]$ induced by $S_3 \curvearrowright \{1, 2, 3\}$ is not semi-simple over $K = \mathbb{Z}/3\mathbb{Z}$, since $3 = 0$ in K . The subspace $W = \text{span}\{e_1 + e_2 + e_3\}$ is a subrepresentation isomorphic to $\mathbf{1}$. We claim W has no G -stable complement. Suppose otherwise; then there is a G -equivariant projection $\pi: V \rightarrow W$ with image W . By G -equivariance (since S_3 acts transitively on $\{e_1, e_2, e_3\}$), $\pi(e_1) = \pi(e_2) = \pi(e_3) = \alpha(e_1 + e_2 + e_3)$ for some $\alpha \in K$. For π to fix W we need $\pi(e_1 + e_2 + e_3) = e_1 + e_2 + e_3$, i.e. $3\alpha(e_1 + e_2 + e_3) = e_1 + e_2 + e_3$. But $3\alpha = 0$ in K for any α , contradicting $1 \neq 0$. This shows the hypothesis $n \neq 0$ in K is necessary.

Remark 2.20. The decomposition is in general not unique. For example, if V has degree $n \geq 2$ and G acts trivially, then $V \simeq \mathbf{1} \oplus \cdots \oplus \mathbf{1}$ (n copies), but the splitting into lines depends on the choice of basis.

Proof of Theorem 2.18. By Theorem 2.16, it suffices to show that every subrepresentation has a supplement. Since $\dim V < \infty$, there are no infinite descending chains of subrepresentations, so the

hypothesis of Theorem 2.16 is satisfied.

Let $V_1 \subseteq V$ be a subrepresentation. As K -vector spaces (ignoring the G -action), we can write $V = V_1 \oplus V_2$ for some subspace V_2 ; this need not be G -stable. Let $\pi: V \rightarrow V$ be the projection onto V_1 parallel to V_2 (which exists by Theorem 2.17). Define the *Reynolds operator*

$$\Pi: V \rightarrow V, \quad v \mapsto \frac{1}{\#G} \sum_{g \in G} g \pi(g^{-1}v).$$

This is well-defined since $\#G \neq 0$ in K . We verify three properties.

$\text{Im } \Pi \subseteq V_1$ and $\Pi|_{V_1} = \text{id}_{V_1}$. Since V_1 is a subrepresentation, $g^{-1}v \in V_1$ whenever $v \in V_1$, so $\pi(g^{-1}v) = g^{-1}v$, hence $g\pi(g^{-1}v) = v$, giving $\Pi(v) = v$. For general v , each term $g\pi(g^{-1}v)$ lies in $gV_1 = V_1$, so $\Pi(v) \in V_1$. Thus $\text{Im } \Pi = V_1$ and $\Pi^2 = \Pi$.

Π is a morphism of representations. For any $h \in G$ and $v \in V$:

$$h \Pi(v) = \frac{1}{\#G} \sum_{g \in G} hg \pi(g^{-1}v) = \frac{1}{\#G} \sum_{g \in G} hg \pi((hg)^{-1}(hv)) = \frac{1}{\#G} \sum_{g \in G} g \pi(g^{-1}(hv)) = \Pi(hv),$$

where the last step uses that $g \mapsto hg$ is a bijection $G \rightarrow G$.

Conclusion. By Theorem 2.17, $\Pi^2 = \Pi$ implies $V = \text{Im } \Pi \oplus \text{Ker } \Pi = V_1 \oplus \text{Ker } \Pi$. Since Π is a morphism of representations, $\text{Ker } \Pi$ is a subrepresentation, and it is a supplement to V_1 . \square

2.5 Exercises

Exercise 2.21 (Quotient modules). Let R be a ring, M an R -module, and $N \subset M$ a submodule. Since N is a normal subgroup of the abelian group $(M, +)$, the quotient group $M/N = \{m + N \mid m \in M\}$ is well-defined, and comes with a surjective projection $\pi: M \rightarrow M/N$, $m \mapsto m + N$, whose kernel is N .

1. Prove that M/N is an R -module, by showing that the scalar multiplication

$$R \times M/N \longrightarrow M/N, \quad (\lambda, m + N) \longmapsto (\lambda m) + N$$

is well-defined (and checking the module axioms).

2. (*Isomorphism theorem for modules.*) Prove that any module morphism $f: M \rightarrow M'$ induces a module isomorphism $M/\text{Ker } f \simeq \text{Im } f$.

(Solution)

Exercise 2.22 (Submodules and short exact sequences). In this exercise all modules are over a fixed ring R . We write 0 for the zero module $\{0\}$ and also for the zero morphism between any two modules.

Define an *exact sequence* as a diagram

$$\cdots \longrightarrow M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \longrightarrow \cdots$$

where the M_i are modules, the f_i are module morphisms, and $\text{Im } f_i = \text{Ker } f_{i+1}$ for all i .

1. Prove that $f_{i+1} \circ f_i = 0$ for all i .
2. Let N, M, Q be modules with morphisms $f: N \rightarrow M$ and $g: M \rightarrow Q$. Prove that $0 \xrightarrow{0} N \xrightarrow{f} M$ is exact if and only if f is injective, and that $M \xrightarrow{g} Q \xrightarrow{0} 0$ is exact if and only if g is surjective.

A *short exact sequence* is an exact sequence of the form $0 \rightarrow N \xrightarrow{f} M \xrightarrow{g} Q \rightarrow 0$. By the previous question, f is injective and g is surjective, so $\text{Im } f \simeq N$ is a submodule of M .

3. Prove that conversely, whenever M is a module and $N \subset M$ is a submodule, there exists a short exact sequence $0 \rightarrow N \xrightarrow{f} M \rightarrow Q \rightarrow 0$ with f the identity inclusion.

Hint: Use Exercise 2.21.

4. Give a counterexample showing that the existence of a short exact sequence $0 \rightarrow N \rightarrow M \rightarrow Q \rightarrow 0$ does *not* in general imply $M \simeq N \oplus Q$.

Hint: Take $R = \mathbb{Z}$ and $M = \mathbb{Z}/4\mathbb{Z}$.

We say a short exact sequence $0 \rightarrow N \xrightarrow{f} M \xrightarrow{g} Q \rightarrow 0$ is *left-split* if there exists a module morphism $f': M \rightarrow N$ with $f' \circ f = \text{id}_N$, and *right-split* if there exists $g': Q \rightarrow M$ with $g \circ g' = \text{id}_Q$.

5. Let $0 \rightarrow N \xrightarrow{f} M \xrightarrow{g} Q \rightarrow 0$ be short exact. Prove that if $\text{Im } f$ admits a supplement $M' \subset M$, then the sequence is both left-split and right-split.

Hint: Consider the restriction of g to M' .

6. Conversely, prove that if the sequence is left-split, then $\text{Im } f$ admits a supplement in M .

Hint: Consider $T = f \circ f' \in \text{End}(M)$.

7. Similarly, prove that if the sequence is right-split, then $\text{Im } f$ admits a supplement in M .

In conclusion, submodules correspond to short exact sequences, and a submodule admits a supplement if and only if the short exact sequence is left-split, if and only if it is right-split. (Solution)

Exercise 2.23 (Preservation of semi-simplicity). In this exercise all modules are over a fixed ring R and are *Artinian* (meaning there is no infinite strictly descending chain of submodules).

1. Prove that a submodule of a semi-simple module is semi-simple.
2. Prove that if $f: M \rightarrow N$ is a module morphism and M is semi-simple, then $\text{Im } f$ is also semi-simple.
3. Let G be a group, K a field, and $f: V \rightarrow W$ a morphism of representations of G over K of finite degree. Prove that if V is semi-simple, then so are $\text{Ker } f$ and $\text{Im } f$.

(Solution)

Exercise 2.24 (A non-semi-simple ring). Let K be a field and G a finite group of order $n = \#G$. We view the group ring $K[G]$ as a module over itself.

1. Let $\Sigma = \sum_{g \in G} e_g \in K[G]$. Prove that $e_h \Sigma = \Sigma$ for all $h \in G$.
2. Prove that $S = \{\lambda \Sigma \mid \lambda \in K\}$ is a sub- $K[G]$ -module of $K[G]$.
3. Identify S as a representation of G .

From now on assume that $n = 0$ in K .

4. Prove that $\Sigma^2 = 0$ in $K[G]$.

5. Deduce that $1 - \lambda\Sigma$ is invertible in $K[G]$ for all $\lambda \in K$, where $1 = e_{1_G}$ is the multiplicative identity of $K[G]$.

Note: since $K[G]$ need not be commutative, verify your inverse works on both sides.

Hint: Recall the identity $(1 - x)(1 + x + \cdots + x^m) = 1 - x^{m+1}$, valid in any ring.

6. Deduce that $K[G]$, viewed as a $K[G]$ -module, is not semi-simple.

(Solution)

Chapter 3

Character Theory

The character of a representation is a function $G \rightarrow \mathbb{C}$ that encodes an enormous amount of information about the representation in a highly compressed form. In this chapter we prove Schur's lemma, develop the inner-product structure on class functions, and show that irreducible characters form an orthonormal set that completely determines representations up to isomorphism.

Throughout this chapter and the rest of the notes, G denotes a finite group and $K = \mathbb{C}$. By Maschke's theorem, every finite-dimensional representation of G over \mathbb{C} is semi-simple.

3.1 Schur's Lemma

Theorem 3.1 (Schur's lemma). *Let R be a ring, and let M_1, M_2 be simple R -modules. Then any module morphism $f: M_1 \rightarrow M_2$ is either 0 or an isomorphism.*

Proof. Since M_1 is simple, $\text{Ker } f$ is either $\{0\}$ or M_1 . If $\text{Ker } f = M_1$ then $f = 0$. Otherwise f is injective and $\text{Im } f \subseteq M_2$ is a nonzero submodule; since M_2 is simple, $\text{Im } f = M_2$, so f is an isomorphism. \square

Corollary 3.2. *If M is a simple R -module, then $\text{End}_R(M)$ is a division ring.*

Proof. Every nonzero endomorphism is an isomorphism by Theorem 3.1, hence invertible. \square

The decisive consequence for representations over \mathbb{C} follows from the fact that \mathbb{C} is algebraically closed.

Corollary 3.3 (Schur's lemma over \mathbb{C}). *Let G be a group, and let V, W be irreducible representations of G over \mathbb{C} . Then*

$$\dim_{\mathbb{C}} \text{Hom}_G(V, W) = \begin{cases} 0 & \text{if } V \not\simeq W, \\ 1 & \text{if } V \simeq W. \end{cases}$$

In particular $\text{End}_G(V) = \{\lambda \text{ id}_V \mid \lambda \in \mathbb{C}\}$, and if $V \simeq W$ then every G -linear map $V \rightarrow W$ is a scalar multiple of any fixed isomorphism.

Proof. The case $V \not\simeq W$ follows directly from Theorem 3.1. For $V = W$, let $f \in \text{End}_G(V)$. Since \mathbb{C} is algebraically closed, f has at least one eigenvalue $\lambda \in \mathbb{C}$. Then $f - \lambda \text{ id} \in \text{End}_G(V)$ is not injective, so by Theorem 3.1 it must be 0, giving $f = \lambda \text{ id}$. The general case $V \simeq W$ reduces to this one: fix an isomorphism $\phi: V \xrightarrow{\sim} W$; then $T \mapsto \phi^{-1} \circ T$ is a \mathbb{C} -linear bijection $\text{Hom}_G(V, W) \rightarrow \text{End}_G(V)$. \square

3.2 Dot Products

Definition 3.4 (Dot product over \mathbb{R}). Let V be an \mathbb{R} -vector space. A *dot product* on V is a map $(v, w) \mapsto (v | w)$ from $V \times V$ to \mathbb{R} that is bilinear, symmetric: $(v | w) = (w | v)$, and positive definite: $(v | v) \geq 0$ with equality only when $v = 0$.

Example 3.5. On $V = \mathbb{R}^n$, the usual dot product $(v | w) = \sum_{k=1}^n v_k w_k$. On $V = \mathbb{R}[x]$, one may take $(P | Q) = \int_0^1 P(x)Q(x) dx$.

Definition 3.6 (Dot product over \mathbb{C}). Let V be a \mathbb{C} -vector space. A *dot product* (Hermitian inner product) on V is a map $(v, w) \mapsto (v | w)$ from $V \times V$ to \mathbb{C} that is sesquilinear (linear in the first argument, conjugate-linear in the second: $(v | \lambda w) = \bar{\lambda}(v | w)$), conjugate-symmetric: $(v | w) = \overline{(w | v)}$, and positive definite: $(v | v) \in \mathbb{R}_{\geq 0}$ with equality only when $v = 0$.

Example 3.7. On $V = \mathbb{C}^n$, the standard product $(v | w) = \sum_{k=1}^n v_k \bar{w}_k$. On $\mathbb{C}[x]$, one may take $(P | Q) = \int_0^1 P(x)\overline{Q(x)} dx$.

Definition 3.8 (Orthogonal, orthonormal). A family $(v_j)_{j \in J}$ in V is *orthogonal* if $(v_j | v_k) = 0$ for all $j \neq k$, and *orthonormal* if additionally $(v_j | v_j) = 1$ for all j .

Proposition 3.9. If $(e_j)_{j \in J}$ is an orthonormal basis of V , then the coordinates of any $v \in V$ are recovered as $(v | e_j)$.

Proof. Write $v = \sum_{j \in J} \lambda_j e_j$. Then $(v | e_k) = \sum_{j \in J} \lambda_j (e_j | e_k) = \lambda_k$. \square

3.3 Conjugacy and Class Functions

Definition 3.10 (Conjugacy). Two elements $g, g' \in G$ are *conjugate* if $g' = hgh^{-1}$ for some $h \in G$. The *conjugacy class* of g is the set of all its conjugates.

Definition 3.11 (Class function). A *class function* is a function $\psi: G \rightarrow \mathbb{C}$ satisfying $\psi(hgh^{-1}) = \psi(g)$ for all $g, h \in G$, i.e., a function constant on conjugacy classes.

Class functions form a \mathbb{C} -vector space of dimension equal to the number of conjugacy classes. We equip it with the inner product

$$(\phi | \psi) = \frac{1}{\#G} \sum_{g \in G} \phi(g) \overline{\psi(g)}.$$

3.4 Traces

Definition 3.12 (Trace). The *trace* of a square matrix A is the sum of its diagonal entries: $\text{tr } A = \sum_i A_{ii}$.

Example 3.13. $\operatorname{tr} \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = 1 + 4 = 5.$

Proposition 3.14. *The trace is linear: $\operatorname{tr}(A + B) = \operatorname{tr} A + \operatorname{tr} B$ and $\operatorname{tr}(\lambda A) = \lambda \operatorname{tr} A$. Furthermore $\operatorname{tr}(AB) = \operatorname{tr}(BA)$, whence $\operatorname{tr}(BAB^{-1}) = \operatorname{tr} A$.*

Corollary 3.15. *The trace of a linear map $T: V \rightarrow V$ is well-defined independently of the choice of basis: for any basis (e_1, \dots, e_d) of V ,*

$$\operatorname{tr} T = \sum_i (\text{coefficient of } e_i \text{ in } T(e_i)).$$

3.5 The Character of a Representation

Definition 3.16 (Character). The *character* of a representation $\rho: G \rightarrow \operatorname{GL}(V)$ is the function

$$\chi_\rho: G \longrightarrow \mathbb{C}, \quad g \longmapsto \operatorname{tr} \rho(g).$$

Proposition 3.17. *The character of a representation is a class function.*

Proof. $\operatorname{tr} \rho(hgh^{-1}) = \operatorname{tr}(\rho(h)\rho(g)\rho(h)^{-1}) = \operatorname{tr} \rho(g).$ □

Proposition 3.18. *Equivalent representations have the same character.*

Proof. $\operatorname{tr}(P^{-1}\rho(g)P) = \operatorname{tr} \rho(g).$ □

Proposition 3.19. *The character of the trivial representation $\mathbf{1}$ is the constant function $\mathbf{1}: G \rightarrow \mathbb{C}$.*

Proof. By definition, $\mathbf{1}: G \rightarrow \operatorname{GL}(\mathbb{C})$ sends every g to $\operatorname{id}_{\mathbb{C}}$, so $\chi_{\mathbf{1}}(g) = \operatorname{tr}(\operatorname{id}_{\mathbb{C}}) = 1$ for all g . □

Proposition 3.20. *If χ is the character of a representation of degree n , then $\chi(1_G) = n$. We write $\deg \chi := \chi(1_G)$.*

Proof. Since ρ is a group morphism, $\rho(1_G) = \operatorname{id}_V$. Hence $\chi(1_G) = \operatorname{tr}(\operatorname{id}_V) = \dim V = n$. □

Proposition 3.21. *If V_1, V_2 are representations of G with characters χ_1, χ_2 , then the character of $V_1 \oplus V_2$ is $\chi_1 + \chi_2$.*

Proof. The action of g on $V_1 \oplus V_2$ is given by the block matrix $\begin{pmatrix} \rho_1(g) & 0 \\ 0 & \rho_2(g) \end{pmatrix}$, whose trace is $\operatorname{tr} \rho_1(g) + \operatorname{tr} \rho_2(g)$. □

3.6 Characters on Inverses and Kernels

Since G is finite, every element has finite order, which forces the eigenvalues of $\rho(g)$ to be roots of unity.

Lemma 3.22. *Let ρ be a representation of a finite group G of order $n = \#G$. For all $g \in G$, the matrix $\rho(g)$ is diagonalisable over \mathbb{C} , and its eigenvalues are of the form $e^{2k\pi i/n}$, $k \in \mathbb{Z}$.*

Proof. By Lagrange's theorem $g^n = 1_G$, so $\rho(g)^n = \text{id}$. The polynomial $P(x) = x^n - 1 = \prod_{k=0}^{n-1} (x - e^{2k\pi i/n})$ satisfies $P(\rho(g)) = 0$, has all roots in \mathbb{C} , and has no repeated roots. Hence $\rho(g)$ is diagonalisable with eigenvalues among the n -th roots of unity. \square

Corollary 3.23. *Let χ be the character of ρ . For all $g \in G$, $g \in \text{Ker } \rho \iff \chi(g) = \text{deg } \rho$.*

Proof. Choose a basis diagonalising $\rho(g)$, with diagonal entries λ_j satisfying $|\lambda_j| = 1$. Then $\chi(g) = \sum_j \lambda_j$. The triangle inequality gives $|\chi(g)| \leq \sum_j |\lambda_j| = n$, with equality iff all λ_j are non-negative real multiples of a common direction; combined with $|\lambda_j| = 1$, this forces $\lambda_1 = \dots = \lambda_n$. Hence $\chi(g) = n$ iff every $\lambda_j = 1$, i.e. $\rho(g) = \text{id}$. \square

Corollary 3.24. *For all $g \in G$, $\chi(g^{-1}) = \overline{\chi(g)}$.*

Proof. With $\rho(g) = \text{diag}(\lambda_1, \dots, \lambda_n)$ as above, we have $\rho(g^{-1}) = \rho(g)^{-1} = \text{diag}(\lambda_1^{-1}, \dots, \lambda_n^{-1}) = \text{diag}(\overline{\lambda_1}, \dots, \overline{\lambda_n})$, so $\chi(g^{-1}) = \sum_j \overline{\lambda_j} = \overline{\chi(g)}$. \square

3.7 Invariants and the Character of Hom

Recall from Example 1.23 that the space of G -invariants of V is $V^G = \{v \in V \mid gv = v \text{ for all } g \in G\} = \bigcap_{g \in G} \text{Ker}(\rho(g) - \text{id})$. Recall also that $\text{Hom}(V, W)^G = \text{Hom}_G(V, W)$.

Lemma 3.25. *Let $\rho: G \rightarrow \text{GL}(V)$ be a representation. The operator $\pi = \frac{1}{\#G} \sum_{g \in G} \rho(g)$ is a projection onto V^G .*

Proof. For any $v \in V$ and $h \in G$:

$$\rho(h)(\pi(v)) = \frac{1}{\#G} \sum_{g \in G} \rho(hg)(v) = \frac{1}{\#G} \sum_{g \in G} \rho(g)(v) = \pi(v),$$

so $\text{Im } \pi \subseteq V^G$. If $v \in V^G$ then $\rho(g)(v) = v$ for all g , giving $\pi(v) = v$. Thus π is the identity on V^G and maps all of V into V^G , so $\pi^2 = \pi$. \square

Corollary 3.26. $\dim V^G = \frac{1}{\#G} \sum_{g \in G} \chi(g)$.

Proof. In a suitable basis, π has matrix $\begin{pmatrix} I_n & 0 \\ 0 & 0 \end{pmatrix}$ with $n = \dim V^G$. Hence $\dim V^G = \text{tr } \pi = \frac{1}{\#G} \sum_g \text{tr } \rho(g)$. \square

Lemma 3.27. *The character of $\text{Hom}(V_1, V_2)$ is $\overline{\chi_1} \chi_2$, where χ_i is the character of V_i .*

Proof. Fix bases (e_1, \dots, e_m) of V_1 and (f_1, \dots, f_n) of V_2 . For each pair (i, j) with $1 \leq i \leq n$, $1 \leq j \leq m$, let $T_{ij} \in \text{Hom}(V_1, V_2)$ be the map $e_j \mapsto f_i$ sending the remaining basis vectors of V_1 to 0. These T_{ij} form a basis of $\text{Hom}(V_1, V_2)$. For $g \in G$ we have $gT_{ij} = \rho_2(g) T_{ij} \rho_1(g)^{-1}$. Writing $[\rho_1(g)^{-1}]_{kl}$ and $[\rho_2(g)]_{kl}$ for the matrix entries in the chosen bases,

$$(gT_{ij})(e_l) = \rho_2(g) T_{ij} \left(\sum_k [\rho_1(g)^{-1}]_{kl} e_k \right) = [\rho_1(g)^{-1}]_{jl} \rho_2(g) f_i = \sum_k [\rho_2(g)]_{ki} [\rho_1(g)^{-1}]_{jl} f_k,$$

so $gT_{ij} = \sum_{k,l} [\rho_2(g)]_{ki} [\rho_1(g)^{-1}]_{jl} T_{kl}$. The coefficient of T_{ij} in gT_{ij} is therefore $[\rho_2(g)]_{ii} [\rho_1(g)^{-1}]_{jj}$, and the trace is

$$\chi_{\text{Hom}(V_1, V_2)}(g) = \sum_{i,j} [\rho_2(g)]_{ii} [\rho_1(g)^{-1}]_{jj} = \chi_2(g) \chi_1(g^{-1}) = \chi_2(g) \overline{\chi_1(g)},$$

where the last step uses Corollary 3.24. □

Corollary 3.28. *The character of the dual $V^\vee = \text{Hom}(V, \mathbf{1})$ is $\overline{\chi}$.*

Proof. Apply Lemma 3.27 with $V_1 = V$ and $V_2 = \mathbf{1}$: the character of V^\vee is $\overline{\chi} \cdot 1 = \overline{\chi}$. □

Corollary 3.29. *Let V_1, V_2 be representations of G with characters χ_1, χ_2 . Then*

$$(\chi_1 \mid \chi_2) = \dim \text{Hom}_G(V_1, V_2) \in \mathbb{Z}_{\geq 0}.$$

Proof. The character of $\text{Hom}(V_1, V_2)$ is $\overline{\chi_1} \chi_2$, so by Corollary 3.26,

$$\dim \text{Hom}_G(V_1, V_2) = \dim \text{Hom}(V_1, V_2)^G = \frac{1}{\#G} \sum_{g \in G} \overline{\chi_1(g)} \chi_2(g) = (\chi_1 \mid \chi_2). \quad \square$$

3.8 Tensor Products and Symmetric Powers

Proposition 3.30 (Character of a tensor product). *Let V and W be representations of G with characters χ_V and χ_W . Then*

$$\chi_{V \otimes W} = \chi_V \cdot \chi_W \quad (\text{pointwise product}).$$

Proof. By Proposition 1.21, $V \otimes W \simeq \text{Hom}(V^\vee, W)$ as G -representations. Applying Lemma 3.27 and the fact that $\chi_{V^\vee} = \overline{\chi_V}$:

$$\chi_{V \otimes W} = \chi_{\text{Hom}(V^\vee, W)} = \overline{\chi_{V^\vee}} \chi_W = \overline{\overline{\chi_V}} \chi_W = \chi_V \chi_W. \quad \square$$

Remark 3.31. Alternatively: if g acts on V by A and on W by B , the Kronecker product formula (Remark 1.20) gives $\chi_{V \otimes W}(g) = \text{tr}(A \otimes B) = \text{tr}(A) \text{tr}(B) = \chi_V(g) \chi_W(g)$, since the diagonal entries of $A \otimes B$ are $a_{ii} b_{kk}$.

Definition 3.32 (Symmetric and alternating squares). Let V be a G -representation over \mathbb{C} . The transposition $\tau: V \otimes V \rightarrow V \otimes V$, $v \otimes w \mapsto w \otimes v$, satisfies $\tau^2 = \text{id}$ and commutes with the G -action, so its ± 1 eigenspaces are G -stable. They are called the *symmetric square* and the *alternating*

square (or exterior square) of V :

$$S^2V = \text{span}\{v \otimes w + w \otimes v : v, w \in V\}, \quad \Lambda^2V = \text{span}\{v \otimes w - w \otimes v : v, w \in V\}.$$

If v_1, \dots, v_n is a basis of V then $\{v_i \otimes v_j + v_j \otimes v_i : i \leq j\}$ is a basis of S^2V and $\{v_i \otimes v_j - v_j \otimes v_i : i < j\}$ is a basis of Λ^2V , giving $\dim S^2V = \frac{n(n+1)}{2}$ and $\dim \Lambda^2V = \frac{n(n-1)}{2}$. Since the minimal polynomial of τ divides $x^2 - 1$, which has distinct roots over \mathbb{C} (or over any field of characteristic $\neq 2$), the two eigenspaces span $V \otimes V$, and we have $V \otimes V = S^2V \oplus \Lambda^2V$.

Proposition 3.33 (Characters of the symmetric and alternating squares). *Let V be a representation of G with character χ . For all $g \in G$:*

$$\chi_{S^2V}(g) = \frac{1}{2}(\chi(g)^2 + \chi(g^2)), \quad \chi_{\Lambda^2V}(g) = \frac{1}{2}(\chi(g)^2 - \chi(g^2)).$$

Proof. Since g has finite order, $\rho(g)^{|g|} = I$, so $\rho(g)$ is diagonalizable over \mathbb{C} with eigenvalues $\alpha_1, \dots, \alpha_n$ (roots of unity). The element g acts on $v_i \otimes v_j \pm v_j \otimes v_i$ with eigenvalue $\alpha_i \alpha_j$. Using the standard identity $\sum_{i \leq j} \alpha_i \alpha_j = \frac{1}{2}[(\sum_i \alpha_i)^2 + \sum_i \alpha_i^2]$ and $\sum_{i < j} \alpha_i \alpha_j = \frac{1}{2}[(\sum_i \alpha_i)^2 - \sum_i \alpha_i^2]$, together with $\sum_i \alpha_i = \chi(g)$ and $\sum_i \alpha_i^2 = \chi(g^2)$ (eigenvalues of $\rho(g^2)$ are α_i^2), the formulas follow. \square

Remark 3.34. As a consistency check, $\chi_{S^2V}(g) + \chi_{\Lambda^2V}(g) = \chi(g)^2 = \chi_V(g)^2 = \chi_{V \otimes V}(g)$, confirming the decomposition $V \otimes V = S^2V \oplus \Lambda^2V$. The formulas are practical: given the character table of G , one can decompose S^2V and Λ^2V into irreducibles using the first orthogonality relations, without constructing the representation explicitly.

3.9 First Orthogonality and the Main Theorem

Theorem 3.35 (First orthogonality of characters). *The set $\text{Irr}(G)$ is orthonormal with respect to the inner product on class functions.*

Proof. Let $\chi_1, \chi_2 \in \text{Irr}(G)$ with corresponding irreducible representations V_1, V_2 . By Corollary 3.29 and Corollary 3.3,

$$(\chi_1 | \chi_2) = \dim \text{Hom}_G(V_1, V_2) = \begin{cases} 0 & \text{if } V_1 \not\simeq V_2, \\ 1 & \text{if } V_1 \simeq V_2. \end{cases} \quad \square$$

Theorem 3.36 (Characters know everything). *Let V be a representation of G of character χ , with irreducible decomposition $V \simeq W_1^{\oplus n_1} \oplus \dots \oplus W_r^{\oplus n_r}$ (pairwise non-isomorphic W_j with characters χ_j). Then $\chi = \sum_j n_j \chi_j$ and*

$$n_j = (\chi | \chi_j) \quad \text{and} \quad (\chi | \chi) = \sum_{j=1}^r n_j^2.$$

Proof. Additivity of characters on direct sums gives $\chi = \sum_j n_j \chi_j$. Taking the inner product with χ_k and using orthonormality yields $(\chi | \chi_k) = n_k$. Then $(\chi | \chi) = \sum_{j,k} n_j n_k (\chi_j | \chi_k) = \sum_j n_j^2$. \square

Corollary 3.37. *V is irreducible if and only if $(\chi | \chi) = 1$.*

Proof. By Theorem 3.36, $(\chi | \chi) = \sum_j n_j^2$ with $n_j \in \mathbb{Z}_{\geq 0}$. This equals 1 iff exactly one $n_j = 1$ and the rest vanish, i.e. $V \simeq W_j$ for a unique irreducible W_j . \square

Corollary 3.38. *The multiplicities n_k are uniquely determined by V .*

Proof. By Theorem 3.36, $n_k = (\chi | \chi_k)$, which depends only on the character χ of V (and not on a chosen decomposition). \square

Corollary 3.39. *Two representations of G are equivalent if and only if they have the same character.*

Proof. Equivalent representations have the same character (already noted). Conversely, if $\chi_V = \chi_{V'}$, then $n_k = (\chi_V | \chi_k) = (\chi_{V'} | \chi_k) = n'_k$ for each k , so V and V' have the same decomposition into irreducibles and are therefore isomorphic. \square

Corollary 3.40. $\#\text{Irr}(G) \leq \#\{\text{conjugacy classes of } G\}$.

Proof. The elements of $\text{Irr}(G)$ are orthonormal in the space of class functions, which has dimension equal to the number of conjugacy classes. An orthonormal set cannot exceed the dimension of its ambient space. (We will prove equality in Theorem 4.21.) \square

Example 3.41 (S_3). Take $G = S_3$ with $\#G = 6$ and three conjugacy classes: $\{1_G\}$, $\{(12), (13), (23)\}$, $\{(123), (132)\}$. We already know three irreducible representations: the trivial $\mathbf{1}$, the sign ε , and the standard Δ of degree 2. The permutation representation Perm (induced by $S_3 \curvearrowright \{1, 2, 3\}$) has character $\chi_{\text{Perm}}(g) = \#\text{Fix } g$:

	$\{1_G\}$	$\{(12), (13), (23)\}$	$\{(123), (132)\}$
$\mathbf{1}$	1	1	1
ε	1	-1	1
Δ	2	0	-1
Perm	3	1	0

We compute $(\mathbf{1} | \mathbf{1}) = (\varepsilon | \varepsilon) = (\Delta | \Delta) = 1$, confirming irreducibility. Since $(\text{Perm} | \text{Perm}) = \frac{1}{6}(9 + 3 + 0) = 2$, Perm is not irreducible. Computing $(\text{Perm} | \mathbf{1}) = 1$, $(\text{Perm} | \varepsilon) = 0$, $(\text{Perm} | \Delta) = 1$ gives $\text{Perm} \simeq \mathbf{1} \oplus \Delta$.

3.10 Exercises

Exercise 3.42 (Decomposition of permutation representations). Let G be a finite group acting on a finite set X with $\#X \geq 2$. The *orbit* of $x \in X$ is $G \cdot x = \{h \cdot x \mid h \in G\}$, and the *fixed set* of $g \in G$ is $\text{Fix } g = \{x \in X \mid g \cdot x = x\}$. Orbits partition X . We admit the following *orbit-counting formula*: the number of orbits equals

$$\frac{1}{\#G} \sum_{g \in G} \#\text{Fix } g.$$

The action is *transitive* if X is a single orbit, and *doubly transitive* if for all $x \neq x'$ in X and $y \neq y'$ in X there exists $g \in G$ with $g \cdot x = y$ and $g \cdot x' = y'$. Let π be the permutation representation corresponding to $G \curvearrowright X$; recall $\chi_\pi(g) = \#\text{Fix } g$.

1. Prove that there exists a representation ρ of G such that $\pi \simeq \mathbf{1} \oplus \rho$.

2. Prove that ρ has no subrepresentation isomorphic to $\mathbf{1}$ if and only if the action of G on X is transitive.
3. Suppose the action of G on X is transitive. Prove that ρ is irreducible if and only if the action is doubly transitive.

Hint: Consider the diagonal action of G on $X \times X$ by $g \cdot (x, y) = (g \cdot x, g \cdot y)$. Note that the diagonal $\Delta = \{(x, x) \mid x \in X\}$ is a proper G -stable subset of $X \times X$.

(Solution)

Exercise 3.43 (Schur vs. class functions). Let G be a finite group, $f: G \rightarrow \mathbb{C}$ a class function (not necessarily a character), and $\rho: G \rightarrow \text{GL}(V)$ an irreducible representation of G with character χ . Define

$$T_f = \sum_{g \in G} f(g) \rho(g): V \rightarrow V.$$

1. Explain why $T_f = \lambda \text{id}_V$ for some $\lambda \in \mathbb{C}$.
2. Express λ in terms of $\deg \rho$ and an inner product of class functions.

(Solution)

Exercise 3.44 (Real-valued characters). Let G be a finite group.

1. Prove that every character of G is real-valued if and only if every $g \in G$ is conjugate to its inverse.
Hint: Recall that $\chi(g^{-1}) = \overline{\chi(g)}$ (Corollary 3.24).
2. Let $n \in \mathbb{N}$. Prove that every character of S_n is real-valued. What about A_4 ?

(Solution)

Chapter 4

Character Tables

In this chapter we determine the precise number of irreducible representations of a finite group (it equals the number of conjugacy classes), prove the Wedderburn structure theorem for $\mathbb{C}[G]$, and use these tools to compute character tables explicitly.

4.1 Decomposition of the Regular Representation

Proposition 4.1. *Let G act on a finite set X . The character of the permutation representation $\mathbb{C}[X]$ is $\chi(g) = \# \text{Fix } g$, where $\text{Fix } g = \{x \in X \mid g \cdot x = x\}$.*

Proof. In the basis $\{e_x\}_{x \in X}$, the action sends $e_x \mapsto e_{g \cdot x}$, so the diagonal entry of g at position x is 1 if $g \cdot x = x$ and 0 otherwise. \square

Applying this to the regular representation $G \curvearrowright G$ by left multiplication:

$$\chi_{\text{reg}}(g) = \# \text{Fix } g = \#\{h \in G \mid gh = h\} = \begin{cases} \#G & \text{if } g = 1_G, \\ 0 & \text{otherwise.} \end{cases}$$

Remark 4.2. The regular representation is *faithful*: if $g \cdot x = x$ for all $x \in G$, then $g \cdot 1_G = 1_G$ forces $g = 1_G$. Hence every finite group admits a faithful representation. In particular, a non-abelian group must have at least one irreducible representation of degree ≥ 2 : were every irreducible component of the (faithful) regular representation of degree 1, each would factor through the abelianisation G/G' , and the kernel of the regular representation would contain $G' \neq \{1_G\}$.

Theorem 4.3 (Decomposition of the regular representation).

$$\mathbb{C}[G] \simeq \bigoplus_{\rho \in \text{Irr}(G)} \rho^{\oplus \deg \rho}.$$

Proof. For any $\rho \in \text{Irr}(G)$ with character χ_ρ , its multiplicity in $\mathbb{C}[G]$ is

$$(\chi_{\text{reg}} \mid \chi_\rho) = \frac{1}{\#G} \sum_{g \in G} \chi_{\text{reg}}(g) \overline{\chi_\rho(g)} = \frac{1}{\#G} \cdot \#G \cdot \chi_\rho(1_G) = \deg \rho. \quad \square$$

Corollary 4.4. $\#G = \sum_{\rho \in \text{Irr}(G)} (\deg \rho)^2$.

Proof. Compare dimensions on both sides of Theorem 4.3: $\#G = \sum_{\rho} (\deg \rho) \cdot \deg \rho$. \square

Example 4.5. For $G = S_3$ with $\text{Irr}(G) = \{1, \varepsilon, \Delta\}$: $\mathbb{C}[S_3] \simeq 1 \oplus \varepsilon \oplus \Delta^{\oplus 2}$, and $6 = 1^2 + 1^2 + 2^2$. \checkmark

Corollary 4.6. For all $g \in G$,

$$\sum_{\chi \in \text{Irr}(G)} (\deg \chi) \chi(g) = \begin{cases} \#G & \text{if } g = 1_G, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. This is the statement that the character of $\bigoplus_{\rho} \rho^{\oplus \deg \rho}$ equals χ_{reg} . \square

4.2 Wedderburn on $\mathbb{C}[G]$

Definition 4.7 (K -algebra). Let K be a field. A K -algebra is a K -vector space A which is also a ring satisfying $\lambda(ab) = (\lambda a)b = a(\lambda b)$ for all $\lambda \in K$ and $a, b \in A$.

Example 4.8. The polynomial ring $K[x]$, the matrix ring $\mathcal{M}_n(K)$, and the group ring $\mathbb{C}[G]$ are all K -algebras.

Definition 4.9 (Opposite ring). The *opposite ring* R^{opp} of a ring R has the same underlying set and addition, with multiplication reversed: $x \times_{R^{\text{opp}}} y = y \times_R x$.

Example 4.10. If R is commutative, $R^{\text{opp}} = R$. Transposition gives $\mathcal{M}_n(K)^{\text{opp}} \simeq \mathcal{M}_n(K)$.

Lemma 4.11. Let $M = R$ viewed as an R -module. Then $\text{End}_R(M) \simeq R^{\text{opp}}$.

Proof. The map $r \mapsto (\mu_r : m \mapsto mr)$ from R^{opp} to $\text{End}_R(M)$ is injective (since $\mu_r(1) = r$), surjective (any $f \in \text{End}_R(M)$ satisfies $f = \mu_{f(1)}$), and a ring morphism ($\mu_r \circ \mu_s = \mu_{sr}$). \square

Lemma 4.12 (Endomorphisms of direct sums). If $M = M_1 \oplus M_2$ is an R -module, then

$$\text{End}_R(M) \simeq \begin{pmatrix} \text{End}_R(M_1) & \text{Hom}_R(M_2, M_1) \\ \text{Hom}_R(M_1, M_2) & \text{End}_R(M_2) \end{pmatrix}.$$

If $M_1 \not\cong M_2$ are both simple, this reduces to $\text{End}_R(M) \simeq \text{End}_R(M_1) \times \text{End}_R(M_2)$.

Proof. Let $\iota_i : M_i \hookrightarrow M$ be the canonical inclusions and $\pi_i : M \rightarrow M_i$ the projections, satisfying $\pi_i \iota_j = \delta_{ij} \text{id}_{M_i}$ and $\iota_1 \pi_1 + \iota_2 \pi_2 = \text{id}_M$. For $f \in \text{End}_R(M)$, define $f_{ij} = \pi_i f \iota_j \in \text{Hom}_R(M_j, M_i)$. The map $f \mapsto (f_{ij})$ is a K -linear bijection from $\text{End}_R(M)$ to the matrix space, with inverse $(f_{ij}) \mapsto \sum_{i,j} \iota_i f_{ij} \pi_j$. It is a ring morphism: if $f, g \in \text{End}_R(M)$, then

$$(fg)_{ij} = \pi_i f g \iota_j = \pi_i f (\iota_1 \pi_1 + \iota_2 \pi_2) g \iota_j = \sum_k f_{ik} g_{kj},$$

which is matrix multiplication. For the second statement: if $M_1 \not\cong M_2$ are simple, then Schur's lemma (Theorem 3.1) gives $\text{Hom}_R(M_1, M_2) = \text{Hom}_R(M_2, M_1) = 0$, so the off-diagonal entries vanish and the matrix ring becomes the product $\text{End}_R(M_1) \times \text{End}_R(M_2)$. \square

Theorem 4.13 (Wedderburn–Artin). *Let K be a field, and let A be a K -algebra that is semi-simple as an A -module. Then*

$$A \simeq \prod_{i=1}^r \mathcal{M}_{n_i}(D_i),$$

a finite product, where the D_i are division rings containing K .

Remark 4.14. We state Wedderburn–Artin as background context only: its proof in full generality requires the Jacobson density theorem and other tools from noncommutative algebra. For the case $A = \mathbb{C}[G]$ we will give a direct proof below, using only Maschke, Schur, and the decomposition of the regular representation.

Theorem 4.15 (Wedderburn decomposition of $\mathbb{C}[G]$).

$$\mathbb{C}[G] \simeq \prod_{\rho \in \text{Irr}(G)} \mathcal{M}_{\deg \rho}(\mathbb{C}).$$

Proof. By Lemma 4.11, $\mathbb{C}[G]^{\text{opp}} \simeq \text{End}_{\mathbb{C}[G]}(\mathbb{C}[G]) = \text{End}_G(\mathbb{C}[G])$. By Theorem 4.3, $\mathbb{C}[G] \simeq \bigoplus_{\rho \in \text{Irr}(G)} \rho^{\oplus \deg \rho}$ as G -modules. Iterated application of Lemma 4.12, together with the vanishing $\text{Hom}_G(\rho, \rho') = 0$ for $\rho \not\cong \rho'$ (Schur), gives

$$\text{End}_G(\mathbb{C}[G]) \simeq \prod_{\rho \in \text{Irr}(G)} \text{End}_G(\rho^{\oplus \deg \rho}) \simeq \prod_{\rho \in \text{Irr}(G)} \mathcal{M}_{\deg \rho}(\text{End}_G(\rho)).$$

By Corollary 3.3, $\text{End}_G(\rho) \simeq \mathbb{C}$ for every irreducible ρ over \mathbb{C} , so

$$\mathbb{C}[G]^{\text{opp}} \simeq \prod_{\rho \in \text{Irr}(G)} \mathcal{M}_{\deg \rho}(\mathbb{C}).$$

Taking opposites on both sides and using $\mathcal{M}_n(\mathbb{C})^{\text{opp}} \simeq \mathcal{M}_n(\mathbb{C})$ (via transposition) yields the claim. \square

Fourier inversion formula

The Wedderburn isomorphism is given concretely by $x \mapsto (\rho(x))_{\rho \in \text{Irr}(G)}$. Its inverse sends the element $(0, \dots, 0, \text{id}, 0, \dots, 0) \in \prod_{\rho} \mathcal{M}_{\deg \rho}(\mathbb{C})$ (identity in the ρ -slot, zero elsewhere) to the idempotent

$$\pi_{\rho} = \frac{\deg \rho}{\#G} \sum_{g \in G} \overline{\chi_{\rho}(g)} e_g \in \mathbb{C}[G].$$

This *Fourier inversion formula* provides the projections onto isotypic components, as we discuss in Section 4.4.

4.3 The Number of Irreducible Representations

Definition 4.16 (Centre). The *centre* of a ring R is $Z(R) = \{z \in R \mid zr = rz \text{ for all } r \in R\}$.

Theorem 4.17. For every field K and $n \in \mathbb{N}$, $Z(\mathcal{M}_n(K)) = \{\lambda I_n \mid \lambda \in K\} \simeq K$.

Proof. Clearly every scalar matrix λI_n commutes with all of $\mathcal{M}_n(K)$. Conversely, let $A = (a_{ij}) \in Z(\mathcal{M}_n(K))$ and let E_{kl} denote the matrix with a 1 in position (k, l) and zeros elsewhere. Then

$$[AE_{kl}]_{ij} = a_{ik} \delta_{jl}, \quad [E_{kl}A]_{ij} = \delta_{ik} a_{lj},$$

so $AE_{kl} = E_{kl}A$ for all k, l gives $a_{ik} \delta_{jl} = \delta_{ik} a_{lj}$ for all i, j, k, l . Setting $i \neq k$ and $j = l$ yields $a_{ik} = 0$: all off-diagonal entries of A vanish. Setting $i = k$ and $j = l$ gives $a_{kk} = a_{ll}$: all diagonal entries are equal. Hence $A = \lambda I_n$ for some $\lambda \in K$. The map $\lambda \mapsto \lambda I_n$ is a ring isomorphism $K \rightarrow Z(\mathcal{M}_n(K))$. \square

Proposition 4.18. An element $x = \sum_{g \in G} \lambda_g e_g \in \mathbb{C}[G]$ lies in $Z(\mathbb{C}[G])$ if and only if the function $g \mapsto \lambda_g$ is a class function.

Proof. $x \in Z(\mathbb{C}[G])$ iff $x e_h = e_h x$ for all $h \in G$, which amounts to $\lambda_g = \lambda_{hgh^{-1}}$ for all $g, h \in G$. \square

Corollary 4.19. The class sums $e_C = \sum_{g \in C} e_g$, as C ranges over conjugacy classes, form a \mathbb{C} -basis of $Z(\mathbb{C}[G])$. In particular, $\dim_{\mathbb{C}} Z(\mathbb{C}[G]) = \#\{\text{conjugacy classes in } G\}$.

Proof. By Proposition 4.18, $x = \sum_g \lambda_g e_g \in Z(\mathbb{C}[G])$ iff the function $g \mapsto \lambda_g$ is constant on conjugacy classes. Thus every $x \in Z(\mathbb{C}[G])$ may be written uniquely as $x = \sum_C c_C e_C$ with $c_C \in \mathbb{C}$, so the class sums $\{e_C\}$ span $Z(\mathbb{C}[G])$. They are linearly independent because the $\{e_g\}_{g \in G}$ are a basis of $\mathbb{C}[G]$ and distinct conjugacy classes are disjoint. \square

Lemma 4.20. If M is any R -module, then every $z \in Z(R)$ acts on M as an R -module endomorphism via $m \mapsto zm$. In particular, if $f: G \rightarrow \mathbb{C}$ is a class function, then $T_f = \sum_{g \in G} f(g) \rho(g)$ lies in $\text{End}_G(V)$ for every representation V .

Proof. For $r \in R$ and $z \in Z(R)$: $z(rm) = (zr)m = (rz)m = r(zm)$, so $m \mapsto zm$ is R -linear. Applied to $R = \mathbb{C}[G]$: by Proposition 4.18, $T_f = \sum_g f(g) e_g$ lies in $Z(\mathbb{C}[G])$ when f is a class function; its action on V is $\sum_g f(g) \rho(g)$. \square

Theorem 4.21 (Number of irreducible representations). Let G be a finite group. Then

$$\#\text{Irr}(G) = \#\{\text{conjugacy classes in } G\}.$$

Proof. Using Theorem 4.15 and Theorem 4.17:

$$\#\{\text{conj. classes}\} = \dim Z(\mathbb{C}[G]) = \dim Z\left(\prod_{\rho \in \text{Irr } G} \mathcal{M}_{\deg \rho}(\mathbb{C})\right) = \sum_{\rho \in \text{Irr } G} \dim Z(\mathcal{M}_{\deg \rho}(\mathbb{C})) = \#\text{Irr}(G). \quad \square$$

Corollary 4.22. The irreducible characters form an orthonormal basis of the space of class functions.

Proof. They are orthonormal by Theorem 3.35. The space of class functions has dimension equal to the number of conjugacy classes, which by Theorem 4.21 equals $\# \text{Irr}(G)$. An orthonormal set of the right cardinality is a basis. \square

Corollary 4.23. *G is abelian if and only if all irreducible representations of G have degree 1.*

Proof. G abelian \iff every conjugacy class is a singleton $\iff \# \text{Irr}(G) = \#G$. Combined with $\sum_{\rho} (\deg \rho)^2 = \#G$ (Corollary 4.4), this gives $\sum_{\rho} (\deg \rho)^2 = \sum_{\rho} 1$, which forces $\deg \rho = 1$ for all ρ . \square

4.4 Isotypic Components

Theorem 4.24 (Projection onto isotypic component). *Let $V = \bigoplus_{\chi \in \text{Irr}(G)} W_{\chi}^{\oplus n_{\chi}}$ be the complete decomposition of a representation of G . For each $\chi \in \text{Irr}(G)$, the projection π_{χ} onto the χ -isotypic component $W_{\chi}^{\oplus n_{\chi}}$ is given by the operator*

$$\pi_{\chi} = \frac{\deg \chi}{\#G} \sum_{g \in G} \overline{\chi(g)} \rho(g) \in \text{End}(V).$$

Proof. Let $T = \frac{\deg \chi}{\#G} \sum_{g \in G} \overline{\chi(g)} \rho(g)$. By Lemma 4.20, $T \in \text{End}_G(V)$, and by Schur's lemma it acts on each irreducible summand W_{ψ} by a scalar λ . Taking traces, $\lambda = \frac{\deg \chi}{\#G} \cdot \frac{\#G}{\deg \psi} \cdot (\psi | \chi) = \begin{cases} 1 & \text{if } \psi = \chi, \\ 0 & \text{if } \psi \neq \chi. \end{cases}$ So T is the identity on $W_{\chi}^{\oplus n_{\chi}}$ and zero on all other isotypic components. \square

Corollary 4.25 (Isotypic components are canonical). *For each χ , the isotypic component $W_{\chi}^{\oplus n_{\chi}}$ does not depend on the chosen decomposition of V . It is called the χ -isotypic component of V .*

Proof. By Theorem 4.24, the projection π_{χ} onto the χ -isotypic component is given by the explicit formula $\pi_{\chi} = \frac{\deg \chi}{\#G} \sum_g \overline{\chi(g)} \rho(g)$, which involves only V , the representation ρ , and the character χ — not any chosen decomposition. Hence $W_{\chi}^{\oplus n_{\chi}} = \text{Im } \pi_{\chi}$ is canonically defined. \square

4.5 The Character Table

Definition 4.26 (Character table). The *character table* of a finite group G is the square matrix whose rows are indexed by $\text{Irr}(G)$, whose columns are indexed by the conjugacy classes of G , and whose (i, j) entry is the value $\chi_i(g_j)$ of the i -th irreducible character on any element g_j of the j -th conjugacy class. It is a square matrix of size $\# \text{Irr}(G) = \#\{\text{conj. classes}\}$.

Example 4.27 (Character table of S_3). From Example 3.41, with conjugacy classes represented by Id , (12) , (123) :

	Id	(12)	(123)
# elements	1	3	2
$\mathbf{1}$	1	1	1
ε	1	-1	1
Δ	2	0	-1

Theorem 4.28 (Second orthogonality of characters). *Let C, C' be conjugacy classes of G , and let $g \in C, h \in C'$. Then*

$$\sum_{\chi \in \text{Irr}(G)} \overline{\chi(g)} \chi(h) = \begin{cases} \#G / \#C & \text{if } C = C', \\ 0 & \text{if } C \neq C'. \end{cases}$$

In particular, the columns of the character table are pairwise orthogonal.

Proof. By Theorem 4.21, $\text{Irr}(G)$ is an orthonormal basis of the space of class functions. The class indicator $\delta_C: G \rightarrow \{0, 1\}$ (equal to 1 on C and 0 elsewhere) is a class function, so it expands as

$$\delta_C = \sum_{\chi \in \text{Irr}(G)} (\delta_C | \chi) \chi.$$

The coefficient is $(\delta_C | \chi) = \frac{1}{\#G} \sum_{x \in C} \overline{\chi(x)} = \frac{\#C}{\#G} \overline{\chi(g)}$. Evaluating at h :

$$\delta_C(h) = \frac{\#C}{\#G} \sum_{\chi \in \text{Irr}(G)} \overline{\chi(g)} \chi(h).$$

Since $\delta_C(h) = 1$ if $h \in C$ (i.e. $C = C'$) and 0 otherwise, dividing by $\#C/\#G$ gives the result. □

4.6 The Conjugacy Principle and Conjugacy Classes in S_n

Remark 4.29 (Conjugacy principle). In a group G of “transformations” acting on objects with “parameters” x, y, \dots , conjugation by $h \in G$ replaces parameters by their images under h : hgh^{-1} is the transformation of the same type as g but applied to the parameters $h \cdot x, h \cdot y, \dots$

Example 4.30. In $G = \text{SO}_3(\mathbb{R})$, if g is the rotation of axis ℓ and angle θ , then hgh^{-1} is the rotation of axis $h(\ell)$ and the same angle θ .

Applying the conjugacy principle to $G = S_n$ gives a complete description of conjugacy classes.

Proposition 4.31. *Two permutations $\sigma, \sigma' \in S_n$ are conjugate if and only if they have the same cycle type. Hence conjugacy classes of S_n are in bijection with partitions of n .*

Proof. If $\sigma = (i_1 \cdots i_k)(j_1 \cdots j_l) \cdots$, then $\tau\sigma\tau^{-1} = (\tau(i_1) \cdots \tau(i_k))(\tau(j_1) \cdots \tau(j_l)) \cdots$, which has the same cycle shape. Conversely, any two permutations of the same cycle shape are conjugate via an explicit permutation of the labels. □

Example 4.32. The conjugacy classes of S_5 correspond to partitions of 5:

{Id}	$5 = 1 + 1 + 1 + 1 + 1$
{(**)}	$5 = 2 + 1 + 1 + 1$
{(***)}	$5 = 3 + 1 + 1$
{(****)}	$5 = 4 + 1$
{(*****)}	$5 = 5$
{(**)(**)}	$5 = 2 + 2 + 1$
{(***)(**)}	$5 = 3 + 2$

giving 7 conjugacy classes and hence 7 irreducible representations.

4.7 Example: Character Table of S_4

The conjugacy classes of S_4 correspond to partitions of 4, giving 5 classes, represented by Id, (12), (123), (1234), (12)(34) with class sizes 1, 6, 8, 6, 3 respectively.

There are thus 5 irreducible representations of degrees $n_1 \leq n_2 \leq n_3 \leq n_4 \leq n_5$. Since $\mathbf{1}$ is always irreducible, $n_1 = 1$. The constraint $\sum_i n_i^2 = \#S_4 = 24$ forces $n_2^2 + n_3^2 + n_4^2 + n_5^2 = 23$, so $n_5 \leq 4$. If $n_5 = 4$, the remaining sum is 7, and no choice of three positive squares from $\{1, 4, 9, 16\}$ sums to 7. Hence $n_5 = 3$, leaving $n_2^2 + n_3^2 + n_4^2 = 14$ with each $n_i \leq 3$. The inequality $3n_4^2 \geq 14$ forces $n_4 \geq 2$, so $n_4 = 2$; then $n_2^2 + n_3^2 = 5 = 1 + 4$, so $n_2 = 1$ and $n_3 = 2$. The five degrees are therefore $(1, 1, 2, 3, 3)$.

We build the table using known representations:

- $\mathbf{1}$: trivial representation (row of all 1s).
- ε : sign representation (+1 on even permutations, -1 on odd).
- Perm: permutation representation on $\{1, 2, 3, 4\}$, with $\chi(g) = \# \text{Fix } g$. One computes $(\text{Perm} \mid \text{Perm}) = 2$ and $(\text{Perm} \mid \mathbf{1}) = 1$, so $\text{Perm} \simeq \mathbf{1} \oplus \chi$ where χ is the irreducible of degree 3 with values $(3, 1, 0, -1, -1)$.
- $\chi\varepsilon$: tensor product of χ with the sign, giving another irreducible of degree 3 with values $(3, -1, 0, 1, -1)$.
- The degree-2 representation ψ : found by subtracting. The character of $\text{Hom}(\chi, \chi)$ is $\overline{\chi} \cdot \chi$, which equals χ^2 here because χ takes only real values; the pointwise product has values $(9, 1, 0, 1, 1)$. Since $(\chi^2 \mid \chi^2) = 4$, $(\chi^2 \mid \mathbf{1}) = 1$, $(\chi^2 \mid \chi) = 1$, $(\chi^2 \mid \chi\varepsilon) = 1$, we get $\chi^2 \simeq \mathbf{1} \oplus \chi \oplus \chi\varepsilon \oplus \psi$ where ψ is the remaining irreducible of degree 2 with values $(2, 0, -1, 0, 2)$.

The complete character table of S_4 is:

	Id	(12)	(123)	(1234)	(12)(34)
# elements	1	6	8	6	3
$\mathbf{1}$	1	1	1	1	1
ε	1	-1	1	-1	1
ψ	2	0	-1	0	2
χ	3	1	0	-1	-1
$\chi\varepsilon$	3	-1	0	1	-1

One may verify: each row has inner product 1 with itself and 0 with all other rows; Corollary 4.4 gives $1 + 1 + 4 + 9 + 9 = 24 = \#S_4$. \checkmark

4.8 Representations of Abelian Groups

Since every finite abelian group is a direct product of cyclic groups, it suffices to understand the irreducible characters of \mathbb{Z}_n and how characters behave under direct products. Because all irreducible representations of an abelian group have degree 1, they are simply group homomorphisms $G \rightarrow \mathbb{C}^\times$.

Definition 4.33. Let $n \in \mathbb{N}$ and $\omega_n = e^{2\pi i/n}$. For each $k = 0, 1, \dots, n - 1$ define

$$\chi_k: \mathbb{Z}_n \longrightarrow \mathbb{C}^\times, \quad \chi_k(\bar{m}) = \omega_n^{km}.$$

Proposition 4.34. The characters $\chi_0, \dots, \chi_{n-1}$ are exactly the irreducible representations of \mathbb{Z}_n .

Proof. Each χ_k is a group homomorphism (hence an irreducible degree-1 representation). They are pairwise distinct since $\chi_k(\bar{1}) = \omega_n^k$ takes n different values. Since \mathbb{Z}_n is abelian, $\#\text{Irr}(\mathbb{Z}_n) = n$, so these are all. \square

Example 4.35. The character table of \mathbb{Z}_4 (with $\omega = e^{2\pi i/4} = i$):

	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
χ_0	1	1	1	1
χ_1	1	i	-1	$-i$
χ_2	1	-1	1	-1
χ_3	1	$-i$	-1	i

Both orthogonality relations can be verified directly.

Proposition 4.36 (Characters of direct products). Let G_1, G_2 be finite abelian groups with $\text{Irr}(G_1) = \{\chi_1, \dots, \chi_m\}$ and $\text{Irr}(G_2) = \{\varphi_1, \dots, \varphi_n\}$ (where $m = \#G_1, n = \#G_2$). The functions $\alpha_{ij}: G_1 \times G_2 \rightarrow \mathbb{C}^\times$ defined by

$$\alpha_{ij}(g_1, g_2) = \chi_i(g_1) \varphi_j(g_2)$$

form a complete set of $mn = \#(G_1 \times G_2)$ irreducible representations of $G_1 \times G_2$.

Proof. Each α_{ij} is a group homomorphism, hence irreducible. They are pairwise distinct: $\alpha_{ij} = \alpha_{kl}$ implies $\chi_i = \chi_k$ (restrict to $G_1 \times \{1\}$) and $\varphi_j = \varphi_l$. Since $G_1 \times G_2$ is abelian of order mn , it has exactly mn irreducible representations. \square

Example 4.37. The character table of the Klein four-group $\mathbb{Z}_2 \times \mathbb{Z}_2$, with $\text{Irr}(\mathbb{Z}_2) = \{\chi_0 \equiv 1, \chi_1(\bar{m}) = (-1)^m\}$:

	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{1})$
α_{00}	1	1	1	1
α_{01}	1	-1	1	-1
α_{10}	1	1	-1	-1
α_{11}	1	-1	-1	1

4.9 Exercises

Exercise 4.38 (An enigmatic group). A finite group G has 11 conjugacy classes C_1, \dots, C_{11} , and two representations ϕ and ψ (not necessarily irreducible) whose characters are given by:

	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8	C_9	C_{10}	C_{11}
Size	1	15	40	90	45	120	144	120	90	15	40
ϕ	6	2	0	0	2	2	1	1	0	-2	3
ψ	21	1	-3	-1	1	1	1	0	-1	-3	0

1. Which conjugacy class contains the identity 1_G ?
2. Determine $\deg \phi$ and $\deg \psi$.
3. Determine $\#G$.
4. Is the representation of character ϕ irreducible? If not, determine its decomposition into a direct sum of irreducible representations, including the degree of each irreducible constituent. (*Hint: there is one irreducible character of G you can write down immediately.*)
5. Prove that G has an irreducible representation of degree 16. Write down its character. Finally, exhibit an element of $\mathbb{C}[G]$ that acts as a projector onto the corresponding isotypic component.
6. Prove that G has a representation of degree 25 that decomposes as a direct sum of 4 pairwise non-isomorphic irreducible representations.

(Solution)

Exercise 4.39 (Non-abelian groups of order 8). Let G be a non-abelian group of order 8. Prove that G has exactly 5 conjugacy classes, and that the abelianisation $G^{\text{ab}} = G/D(G)$ must have order 4.

(Solution)

Exercise 4.40 (Character table of A_4). Let $G = A_4$ be the alternating group on 4 objects. Set $\omega = e^{2\pi i/3}$; note that $\omega^2 = \bar{\omega} = -\omega - 1$.

1. Let $V_4 = \{\text{Id}, (12)(34), (13)(24), (14)(23)\}$ be the Klein four-subgroup of A_4 . Prove that V_4 is normal in A_4 , and that A_4/V_4 is cyclic.
2. Prove that (123) and (132) are *not* conjugate in A_4 .
3. Determine the character table of A_4 .
4. Deduce that $V_4 = D(A_4)$.
5. Determine the decomposition into irreducible representations of the restriction to A_4 of each of the five irreducible representations of S_4 .
6. (Bonus) The group of rotations of \mathbb{R}^3 preserving a regular tetrahedron is isomorphic to A_4 via the induced permutations on the 4 vertices, giving a faithful representation of A_4 of degree 3. Decompose it over \mathbb{C} into irreducible representations.

(Solution)

Exercise 4.41 (Character table of $C_2 \times C_2$). Write $C_2 = \mathbb{Z}/2\mathbb{Z}$ and let $G = C_2 \times C_2$.

1. Let χ be an irreducible character of G . Prove that $\chi(g) \in \{+1, -1\}$ for all $g \in G$.
2. Write down the character table of G .
3. Is any irreducible representation of G faithful?
4. Do faithful representations of G exist? If so, what is the smallest possible degree?

(Solution)

Exercise 4.42 (Character table of D_8). Let $G = D_8$ be the group of symmetries of the square with elements Id, rotations ρ (by 90°), ρ^2 (by 180°), ρ^3 (by 270°), reflections σ, σ' about the two diagonals, and reflections τ, τ' about the axes through midpoints of opposite edges.

1. Determine the derived subgroup $D(G)$ and the structure of the quotient $G/D(G)$.
2. Determine the character table of D_8 .

(Solution)

Exercise 4.43 (Character table of Q_8). Let $Q_8 = \{1, -1, I, -I, J, -J, K, -K\}$ be the quaternion group with multiplication defined by

$$(-x)y = x(-y) = -(xy), \quad x \cdot 1 = 1 \cdot x = x, \quad I^2 = J^2 = K^2 = -1,$$

$$IJ = K = -JI, \quad JK = I = -KJ, \quad KI = J = -IK.$$

1. By Exercise 4.39, Q_8 has exactly 5 conjugacy classes. Verify that these are $\{1\}$, $\{-1\}$, $\{I, -I\}$, $\{J, -J\}$, and $\{K, -K\}$.
2. Determine the centre $Z(Q_8)$.
3. Prove that $Q_8/Z(Q_8) \cong C_2 \times C_2$.
4. Determine the character table of Q_8 . Compare it with the character table of D_8 (Exercise 4.42).
5. The matrices $\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, and $\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ satisfy the defining relations of Q_8 , giving a faithful representation of Q_8 of degree 2. Interpret this in terms of the character table.

(Solution)

Chapter 5

Induced Representations

The previous chapters developed character theory for a fixed finite group G . In many situations one encounters a group G together with a distinguished subgroup H , and it is natural to ask how the representation theories of the two groups are related. The operation of passing from G -representations to H -representations is called *restriction*; the reverse operation, building a G -representation from an H -representation, is called *induction*. The main result of this chapter, Frobenius reciprocity, expresses a clean adjointness relation between the two.

5.1 Restriction and Induction

Throughout this chapter, G denotes a finite group and $H \leq G$ a subgroup.

Definition 5.1 (Restriction). Let $\rho: G \rightarrow \text{GL}(V)$ be a representation with character χ . Composing with the inclusion $H \hookrightarrow G$ yields a representation $\rho|_H: H \rightarrow \text{GL}(V)$, called the *restriction* of ρ to H . We denote it $\text{Res}_H^G \rho$, and its character $\text{Res}_H^G \chi$.

Remark 5.2. Even if ρ is irreducible as a G -representation, $\text{Res}_H^G \rho$ may be reducible: a subgroup need not detect all of the symmetry that G sees.

Restriction goes from G -representations to H -representations. We now want the reverse: given $\rho: H \rightarrow \text{GL}(W)$, we wish to build a G -representation $\text{Ind}_H^G \rho$ from W .

Remark 5.3 (Induction \neq inflation). Do not confuse induction with *inflation*. Inflation views a representation of a quotient G/N as a representation of G via the projection $G \rightarrow G/N \rightarrow \text{GL}(V)$. Induction goes from a *subgroup* H up to G , not from a quotient.

5.2 Definition(s) of the Induced Representation

Definition 5.4 (Right transversal). A *right transversal* of H in G is a subset $T \subseteq G$ such that

$$G = \bigsqcup_{t \in T} Ht.$$

In other words, T is a system of representatives for the right cosets of H : every $g \in G$ decomposes uniquely as $g = h_g t_g$ with $h_g \in H$ and $t_g \in T$. We may and do assume $1_G \in T$, so that the

decomposition of any $h \in H$ is $h = h \cdot 1_G$, giving $t_h = 1_G$. In particular, $t_g = 1_G$ if and only if $g \in H$.

Explicit construction

Let W be a representation of H and fix a right transversal T . The idea is to build $\text{Ind}_H^G W$ as a product of copies of W indexed by T , and to let G permute these copies while applying the H -action.

Definition 5.5 (Induced representation, first version).

$$\text{Ind}_H^G W = \prod_{t \in T} W_t = \bigoplus_{t \in T} W_t,$$

where $W_t = W$ for all $t \in T$.

Given $g \in G$ and $t \in T$, write $tg = h_{tg} t'$ with $h_{tg} \in H$ and $t' = t_{tg} \in T$.

Theorem 5.6. *The formula*

$$g \cdot w_t \underset{tg=ht'}{=} h \cdot w_{t'} \quad (h \in H; t, t' \in T)$$

makes $\text{Ind}_H^G W$ a representation of G . The isomorphism class of $\text{Ind}_H^G W$ is independent of the choice of right transversal T .

Proof. The basis-free second construction (Definition 5.7 and Theorem 5.8 below) yields a G -representation that does not depend on any choice of transversal. The bijection Φ of Theorem 5.9 transports its G -action to the formula above, simultaneously proving that the formula defines a G -action and that the resulting representation is the same (up to isomorphism) for every choice of T . \square

Abstract construction

Definition 5.7 (Induced representation, second version).

$$\text{Ind}_H^G W = \{f: G \rightarrow W \mid f(hx) = h \cdot f(x) \text{ for all } h \in H, x \in G\},$$

with the G -action $(g \cdot f)(x) = f(xg)$ for $g, x \in G$.

Theorem 5.8. *The formula $(g \cdot f)(x) = f(xg)$ makes $\text{Ind}_H^G W$ a representation of G .*

Proof. If $f \in \text{Ind}_H^G W$, then for all $g \in G, h \in H, x \in G$:

$$(g \cdot f)(hx) = f(hxg) = h \cdot f(xg) = h \cdot (g \cdot f)(x),$$

so $g \cdot f \in \text{Ind}_H^G W$. This defines a G -action: $1_G \cdot f = f$ is clear, and for $g_1, g_2 \in G$,

$$(g_1 \cdot (g_2 \cdot f))(x) = (g_2 \cdot f)(xg_1) = f(xg_1g_2) = ((g_1g_2) \cdot f)(x).$$

Linearity is immediate: $g \cdot (f_1 + f_2) = g \cdot f_1 + g \cdot f_2$ and $g \cdot (\lambda f) = \lambda(g \cdot f)$. \square

Equivalence and basic properties

Theorem 5.9 ($\text{Ind}_H^G W$ well-defined up to isomorphism). *The two constructions of $\text{Ind}_H^G W$ yield equivalent representations.*

Proof. The maps

$$\Phi: \{f: G \rightarrow W \mid f(hx) = h \cdot f(x)\} \longrightarrow \bigoplus_{t \in T} W_t, \quad f \longmapsto (f(t))_{t \in T},$$

$$\Psi: \bigoplus_{t \in T} W_t \longrightarrow \{f: G \rightarrow W \mid f(hx) = h \cdot f(x)\}, \quad (w_t)_{t \in T} \longmapsto (x \mapsto h_x \cdot w_{t_x}),$$

are well-defined, \mathbb{C} -linear, and inverses of each other. To check that Φ intertwines the G -actions, note that for $t \in T$ and $g \in G$, writing $tg = ht'$ with $h \in H, t' \in T$:

$$\Phi(g \cdot f)_t = (g \cdot f)(t) = f(tg) = h_{tg} \cdot f(t_{tg}) = h \cdot f(t'),$$

which matches the formula of Theorem 5.6 for the first-construction action. \square

Remark 5.10. The degree of the induced representation is

$$\deg \text{Ind}_H^G W = (\#T) \deg W = [G : H] \deg W.$$

Moreover, $\text{Res}_H^G \text{Ind}_H^G W$ contains a copy of W : in the first construction, the component W_{1_G} is H -stable with the original H -action.

5.3 Example: Permutation Representations

Every transitive permutation representation arises as an induced representation of the trivial character.

Let G act transitively on a non-empty finite set X . Fix a base point $x_0 \in X$ and let $H = \{g \in G \mid g \cdot x_0 = x_0\}$ be its stabiliser. For each $x \in X$, choose $g_x \in G$ with $g_x \cdot x_0 = x$ and $g_{x_0} = 1_G$. Setting $t_x = g_x^{-1}$, the elements $(t_x)_{x \in X}$ form a right transversal of H in G :

$$G = \bigsqcup_{x \in X} Ht_x,$$

since the right cosets Hg of H in G biject with X via $Hg \mapsto g^{-1} \cdot x_0$.

Proposition 5.11. $\text{Ind}_H^G \mathbf{1}_H \simeq \mathbb{C}[X]$, where $\mathbf{1}_H$ is the trivial representation of H and $\mathbb{C}[X] = \bigoplus_{x \in X} \mathbb{C}e_x$ is the permutation representation attached to $G \curvearrowright X$.

Proof. Using the second definition (Definition 5.7), $\text{Ind}_H^G \mathbf{1}_H$ consists of functions $f: G \rightarrow \mathbb{C}$ with $f(hg) = f(g)$ for all $h \in H$, i.e., functions constant on the right H -cosets $\{Hg\}_{g \in G}$. For each $x \in X$, let $\delta_x \in \text{Ind}_H^G \mathbf{1}_H$ be the indicator of the coset Ht_x :

$$\delta_x(g) = \begin{cases} 1 & \text{if } g \in Ht_x, \\ 0 & \text{otherwise.} \end{cases}$$

The set $\{\delta_x\}_{x \in X}$ is a \mathbb{C} -basis of $\text{Ind}_H^G \mathbf{1}_H$. For $g \in G$ and $z \in X$:

$$(g \cdot \delta_x)(t_z) = \delta_x(t_z g).$$

Now $t_z g = g_z^{-1} g \in H t_y$ for the unique $y \in X$ satisfying $g_z^{-1} g \in H g_y^{-1}$. This holds iff $g_y g_z^{-1} g \in H$, i.e. $g_y g_z^{-1} g \cdot x_0 = x_0$, i.e. $g \cdot z = y$ (using $g_z \cdot x_0 = z$ and $g_y \cdot x_0 = y$). Hence

$$(g \cdot \delta_x)(t_z) = \delta_x(t_z g) = [x = g \cdot z],$$

so $g \cdot \delta_x = \delta_{g \cdot x}$. The map $\delta_x \mapsto e_x$ is therefore a G -equivariant isomorphism $\text{Ind}_H^G \mathbf{1}_H \xrightarrow{\sim} \mathbb{C}[X]$. \square

5.4 Induced Characters

We compute the character of $\text{Ind}_H^G W$ in terms of the character of W .

Definition 5.12 (Extension by zero). Let $\chi: H \rightarrow \mathbb{C}$ be a class function on H . Its *extension by zero* is the function $\chi^0: G \rightarrow \mathbb{C}$ defined by

$$\chi^0(g) = \begin{cases} \chi(g) & \text{if } g \in H, \\ 0 & \text{otherwise.} \end{cases}$$

Remark 5.13. In general χ^0 is *not* a class function on G , since conjugation by elements of G can move elements into or out of H . However, it does satisfy the following partial invariance.

Lemma 5.14. For all $g \in G$ and $h \in H$, $\chi^0(hgh^{-1}) = \chi^0(g)$.

Proof. If $g \notin H$ then $hgh^{-1} \notin H$ (since H is a subgroup), so both sides equal 0. If $g \in H$ then $\chi^0(hgh^{-1}) = \chi(hgh^{-1}) = \chi(g) = \chi^0(g)$ since χ is a class function on H . \square

Remark 5.15. Lemma 5.14 fails if we conjugate by an arbitrary $g' \in G$: $g' g g'^{-1}$ may lie in H even when $g \notin H$.

First formula

Lemma 5.16 (First formula for induced characters). Let χ be the character of a representation W of H . For all $g \in G$,

$$\text{Ind}_H^G \chi(g) = \frac{1}{\#H} \sum_{x \in G} \chi^0(xgx^{-1}).$$

Proof. Let $(e_i)_{i \in I}$ be a basis of W . Then $(e_{i,t})_{i \in I, t \in T}$ is a basis of $\text{Ind}_H^G W = \bigoplus_{t \in T} W_t$. For $g \in G$, the action sends $g \cdot e_{i,t} = h \cdot e_{i,t'}$ where $tg = ht'$. The diagonal term at (i, t) is nonzero only if $t' = t$, i.e. $tgt^{-1} \in H$, in which case it contributes $\chi(tgt^{-1}) = \chi^0(tgt^{-1})$. Hence

$$\text{Ind}_H^G \chi(g) = \sum_{t \in T} \chi^0(tgt^{-1}).$$

Since $G = \bigsqcup_{t \in T} Ht$, every $x \in G$ writes as $x = ht$ for unique $h \in H, t \in T$, and by Lemma 5.14, $\chi^0(xgx^{-1}) = \chi^0(htgt^{-1}h^{-1}) = \chi^0(tgt^{-1})$. Summing over $x \in G$ gives $\#H$ copies of each term $\chi^0(tgt^{-1})$, so

$$\frac{1}{\#H} \sum_{x \in G} \chi^0(xgx^{-1}) = \sum_{t \in T} \chi^0(tgt^{-1}) = \text{Ind}_H^G \chi(g). \quad \square$$

Second formula

To state the second formula we introduce notation. For a group K and $g \in K$, let

$$cc_K(g) = \{kgk^{-1} \mid k \in K\} \subseteq K, \quad C_K(g) = \{k \in K \mid kg = gk\} \leq K$$

denote the K -conjugacy class of g and the centraliser of g in K , respectively. By the orbit-stabiliser theorem, $\#K = \#C_K(g) \cdot \#cc_K(g)$.

For $H \leq G$, the intersection $cc_G(g) \cap H$ is a (possibly empty) union of H -conjugacy classes; write $cc_G(g) \cap H = \bigsqcup_j cc_H(h_j)$ for representatives $h_j \in H$.

Theorem 5.17 (Second formula for induced characters). *Let χ be a character on $H \leq G$. For all $g \in G$,*

$$\text{Ind}_H^G \chi(g) = \#C_G(g) \sum_j \frac{\chi(h_j)}{\#C_H(h_j)} = \frac{[G : H]}{\#cc_G(g)} \sum_j \#cc_H(h_j) \chi(h_j),$$

where $cc_G(g) \cap H = \bigsqcup_j cc_H(h_j)$. (An empty intersection gives $\text{Ind}_H^G \chi(g) = 0$.)

Proof. Starting from Lemma 5.16:

$$\text{Ind}_H^G \chi(g) = \frac{1}{\#H} \sum_{x \in G} \chi^0(xgx^{-1}) = \frac{\#C_G(g)}{\#H} \sum_{g' \in cc_G(g)} \chi^0(g'),$$

since each element $g' \in cc_G(g)$ is achieved by exactly $\#C_G(g)$ choices of x . Since χ^0 vanishes outside H , the sum reduces to $cc_G(g) \cap H = \bigsqcup_j cc_H(h_j)$:

$$\text{Ind}_H^G \chi(g) = \frac{\#C_G(g)}{\#H} \sum_j \#cc_H(h_j) \chi(h_j).$$

Substituting $\#cc_H(h_j) = \#H/\#C_H(h_j)$ gives the first form. For the second form, observe

$$\frac{\#C_G(g)}{\#H} = \frac{\#G/\#cc_G(g)}{\#G/[G : H]} = \frac{[G : H]}{\#cc_G(g)}. \quad \square$$

Example 5.18. Take $G = S_3$, $H = \{\text{Id}, \tau\}$ with $\tau = (12)$, and $\chi \in \text{Irr}(H)$ the sign: $\chi(\text{Id}) = 1$, $\chi(\tau) = -1$.

- $g = \sigma = (123)$: $cc_G(\sigma) = \{(123), (132)\}$ and $cc_G(\sigma) \cap H = \emptyset$, so $\text{Ind}_H^G \chi(\sigma) = 0$.
- $g = \tau' = (23)$: $cc_G(\tau') = \{(12), (13), (23)\}$, $cc_G(\tau') \cap H = \{(12)\} = cc_H(\tau)$. Thus $j = 1$, $h_1 = \tau$, $[G : H] = 3$, $\#cc_G(\tau') = 3$, $\#cc_H(\tau) = 1$, so $\text{Ind}_H^G \chi(\tau') = \frac{3}{3} \cdot 1 \cdot (-1) = -1$.

Together with $\text{Ind}_H^G \chi(\text{Id}) = [G : H] \chi(\text{Id}) = 3$, the full character of $\text{Ind}_H^G \chi$ on the three conjugacy classes of S_3 is $(3, -1, 0)$, which equals $\varepsilon + \Delta$ as we will confirm using Frobenius reciprocity below.

5.5 Frobenius Reciprocity

The most important formal property of induction is that it is adjoint to restriction with respect to the inner product of characters.

Theorem 5.19 (Frobenius reciprocity). *Let ϕ be a character on H and ψ a character on G . Then*

$$(\text{Ind}_H^G \phi \mid \psi)_G = (\phi \mid \text{Res}_H^G \psi)_H.$$

Proof. Expanding the left-hand side using Lemma 5.16:

$$\begin{aligned} (\text{Ind}_H^G \phi \mid \psi)_G &= \frac{1}{\#G} \sum_{g \in G} \text{Ind}_H^G \phi(g) \overline{\psi(g)} = \frac{1}{\#G} \sum_{g \in G} \left(\frac{1}{\#H} \sum_{x \in G} \phi^0(xgx^{-1}) \right) \overline{\psi(g)} \\ &= \frac{1}{\#G \cdot \#H} \sum_{x \in G} \sum_{g \in G} \phi^0(xgx^{-1}) \overline{\psi(g)}. \end{aligned}$$

Substituting $y = xgx^{-1}$ (so $g = x^{-1}yx$) and using that ψ is a class function ($\psi(x^{-1}yx) = \psi(y)$):

$$= \frac{1}{\#G \cdot \#H} \sum_{x \in G} \sum_{y \in G} \phi^0(y) \overline{\psi(y)} = \frac{1}{\#H} \sum_{y \in G} \phi^0(y) \overline{\psi(y)} = \frac{1}{\#H} \sum_{y \in H} \phi(y) \overline{\psi(y)} = (\phi \mid \text{Res}_H^G \psi)_H.$$

□

Example 5.20. Take $G = S_3$ and $H = \{\text{Id}, \tau\}$ where $\tau = (12)$, with character table of H :

H	Id	τ
$\mathbf{1}_H$	1	1
ψ	1	-1

and character table of $G = S_3$ (with # class sizes 1, 3, 2):

G	Id	(12)	(123)
#	1	3	2
$\mathbf{1}_G$	1	1	1
ε	1	-1	1
Δ	2	0	-1

For any character χ of H , Frobenius reciprocity gives

$$(\text{Ind}_H^G \chi \mid \mathbf{1}_G)_G = (\chi \mid \text{Res}_H^G \mathbf{1}_G)_H = \frac{\chi(\text{Id}) + \chi(\tau)}{2},$$

$$(\text{Ind}_H^G \chi \mid \varepsilon)_G = (\chi \mid \text{Res}_H^G \varepsilon)_H = \frac{\chi(\text{Id}) - \chi(\tau)}{2},$$

$$(\text{Ind}_H^G \chi \mid \Delta)_G = (\chi \mid \text{Res}_H^G \Delta)_H = \frac{2\chi(\text{Id}) + 0 \cdot \chi(\tau)}{2} = \chi(\text{Id}) = \text{deg } \chi.$$

Applying this to $\chi = \mathbf{1}_H$ and $\chi = \psi$:

$$\text{Ind}_H^G \mathbf{1}_H \simeq \mathbf{1}_G \oplus \Delta, \quad \text{Ind}_H^G \psi \simeq \varepsilon \oplus \Delta.$$

In particular, every irreducible representation of G appears in some $\text{Ind}_H^G \chi$, $\chi \in \text{Irr}(H)$.

Corollary 5.21 (All representations from induction). *Let G be a finite group and $\chi \in \text{Irr}(G)$. For any $H \leq G$, there exists $\psi \in \text{Irr}(H)$ such that $\text{Ind}_H^G \psi$ contains χ as an irreducible component.*

Proof. Let ψ be any irreducible component of $\text{Res}_H^G \chi$. By Frobenius reciprocity,

$$(\text{Ind}_H^G \psi \mid \chi)_G = (\psi \mid \text{Res}_H^G \chi)_H \geq 1. \quad \square$$

Example 5.22. Take $G = S_4$ and $H = S_3 \leq S_4$ (permuting the first three elements). Recall the character tables:

S_3	Id	(12)	(123)	S_4	Id	(12)	(123)	(1234)	(12)(34)
#	1	3	2	#	1	6	8	6	3
$\mathbf{1}_{S_3}$	1	1	1	$\mathbf{1}_{S_4}$	1	1	1	1	1
ε_{S_3}	1	-1	1	ε_{S_4}	1	-1	1	-1	1
Δ	2	0	-1	ψ	2	0	-1	0	2
				χ	3	1	0	-1	-1
				$\chi \varepsilon_{S_4}$	3	-1	0	1	-1

Applying Frobenius reciprocity one finds:

$$\begin{aligned} \text{Ind}_{S_3}^{S_4} \mathbf{1}_{S_3} &\simeq \mathbf{1}_{S_4} \oplus \chi, \\ \text{Ind}_{S_3}^{S_4} \varepsilon_{S_3} &\simeq \varepsilon_{S_4} \oplus \chi \varepsilon_{S_4}, \\ \text{Ind}_{S_3}^{S_4} \Delta &\simeq \psi \oplus \chi \oplus \chi \varepsilon_{S_4}. \end{aligned}$$

Every irreducible representation of S_4 appears, confirming Corollary 5.21.

5.6 Exercises

Exercise 5.23 (Character table of D_{2n} , n odd). Fix an odd integer $n = 2m + 1 \geq 3$ and let $G = D_{2n}$ be the dihedral group of symmetries of a regular n -gon, with ρ the rotation of angle $2\pi/n$ and τ one axial symmetry. Set $H = \langle \rho \rangle \cong \mathbb{Z}/n\mathbb{Z}$; since $\tau\rho\tau^{-1} = \rho^{-1}$, H is normal in G with index $[G : H] = 2$ and $G/H \cong \mathbb{Z}/2\mathbb{Z}$. The irreducible characters of H are $\chi_y: \rho^x \mapsto e^{2\pi ixy/n}$, $y \in \mathbb{Z}/n\mathbb{Z}$; note that $\mathbb{Z}/n\mathbb{Z} = \{-m, \dots, 0, \dots, m\}$ without repetition.

1. Show that the conjugacy classes of G are $\{\text{Id}\}$, $\{\rho^k, \rho^{-k}\}$ for $k = 1, \dots, m$, and one class consisting of all n axial symmetries.
2. Use $G/H \cong \mathbb{Z}/2\mathbb{Z}$ to write down two irreducible characters of G of degree 1. (*Hint:* inflate the characters of the quotient to G via the projection $G \rightarrow G/H$; see Remark 5.3.)
3. For $y \in \mathbb{Z}/n\mathbb{Z}$ let $\psi_y = \text{Ind}_H^G \chi_y$.
 - (a) Compute the character values of ψ_y using the induced-character formula (Section 5.4). (*Hint:* $e^{it} + e^{-it} = 2 \cos t$.)
 - (b) Determine the decomposition of $\text{Res}_H^G \psi_y$ into irreducible characters of H .
 - (c) Use Frobenius reciprocity (Section 5.5) to determine for which values of y the character ψ_y is irreducible.
4. Write down the full character table of G .
5. Determine the centre $Z(G)$ and the derived subgroup $D(G)$.

(Solution)

Exercise 5.24 (Character table of D_{2n} , n even). Carry out the same programme as in Exercise 5.23 for $G = D_{2n}$ with $n = 2m$ even. Note that the axial symmetries now fall into two conjugacy classes; you may find Exercise 4.41 useful. ([Solution](#))

Chapter 6

Fourier Analysis on Finite Groups

Classical Fourier analysis decomposes a periodic function on \mathbb{R} as a sum of pure exponentials $e^{2\pi i n x}$. The same idea applies to finite groups: every function $G \rightarrow \mathbb{C}$ expands uniquely in terms of *matrix coefficients* of irreducible representations. For abelian groups this specialises to the classical discrete Fourier transform; for non-abelian groups it yields a ring isomorphism $\mathbb{C}[G] \simeq \prod_{\rho} \mathcal{M}_{\deg \rho}(\mathbb{C})$, recovering the Wedderburn theorem from a Fourier-analytic viewpoint.

6.1 The Function Algebra $L(G)$

Definition 6.1. The *function space* $L(G) = \text{Map}(G, \mathbb{C})$ is the \mathbb{C} -vector space of all functions $G \rightarrow \mathbb{C}$. It has dimension $\#G$, with basis the *delta functions* δ_g ($g \in G$), where

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

The space $L(G)$ carries the inner product $(a | b) = \frac{1}{\#G} \sum_{g \in G} a(g) \overline{b(g)}$.

Definition 6.2 (Convolution). For $a, b \in L(G)$, the *convolution* $a * b \in L(G)$ is defined by

$$(a * b)(x) = \sum_{y \in G} a(xy^{-1}) b(y).$$

The formula is forced by the requirement that $\delta_g * \delta_h = \delta_{gh}$: convolution is the unique bilinear extension to $L(G)$ of the multiplication on $\mathbb{C}[G]$.

Proposition 6.3. For all $g, h \in G$, $\delta_g * \delta_h = \delta_{gh}$.

Proof. $(\delta_g * \delta_h)(x) = \sum_y \delta_g(xy^{-1}) \delta_h(y)$; the only non-zero term is $y = h$, which contributes $\delta_g(xh^{-1}) = 1$ iff $x = gh$. \square

Theorem 6.4. $(L(G), +, *)$ is a unital ring with identity δ_{1_G} , isomorphic to $\mathbb{C}[G]$ via $e_g \mapsto \delta_g$. Class functions on G are exactly the elements of the centre $Z(L(G))$.

Proof. Since $\delta_g * \delta_h = \delta_{gh}$, the assignment $e_g \mapsto \delta_g$ extends linearly to a ring isomorphism $\mathbb{C}[G] \xrightarrow{\sim} L(G)$. The characterisation of $Z(L(G))$ then follows from Proposition 4.18. \square

Remark 6.5. Under the isomorphism $\mathbb{C}[G] \simeq L(G)$, the element $\sum_g \lambda_g e_g$ corresponds to the function $a : g \mapsto \lambda_g$, and the group ring multiplication corresponds to convolution. We will freely switch between the two viewpoints.

6.2 Matrix Coefficients

Definition 6.6 (Matrix coefficients). Fix unitary representatives $\rho^{(1)}, \dots, \rho^{(s)}$ of all isomorphism classes in $\text{Irr}(G)$, with $d_k = \deg \rho^{(k)}$. The *matrix coefficients* of $\rho^{(k)}$ are the d_k^2 functions

$$\varphi_{ij}^{(k)} : G \longrightarrow \mathbb{C}, \quad g \longmapsto \rho^{(k)}(g)_{ij}, \quad 1 \leq i, j \leq d_k.$$

In particular, $\chi_k = \sum_i \varphi_{ii}^{(k)}$.

Theorem 6.7 (Schur orthogonality of matrix coefficients). *For all k, l and all index pairs $(a, b), (c, d)$,*

$$(\varphi_{ab}^{(k)} \mid \varphi_{cd}^{(l)}) = \frac{\delta_{kl} \delta_{ac} \delta_{bd}}{d_k}.$$

Equivalently, $\{\sqrt{d_k} \varphi_{ij}^{(k)}\}_{k,i,j}$ is an orthonormal set in $L(G)$.

Proof. For any linear map $A : V_l \rightarrow V_k$, the average

$$\tilde{A} = \frac{1}{\#G} \sum_{g \in G} \rho^{(k)}(g) \circ A \circ \rho^{(l)}(g)^{-1}$$

is G -equivariant, so by Corollary 3.3: $\tilde{A} = 0$ when $k \neq l$, and $\tilde{A} = \frac{\text{tr } A}{d_k} \text{id}$ when $k = l$.

Apply this with $A = E_{bd}$, the matrix with 1 in row b , column d , and zero elsewhere; note $\text{tr } E_{bd} = \delta_{bd}$. Since $\rho^{(l)}$ is unitary, $(\rho^{(l)}(g)^{-1})_{dc} = \overline{\rho_{cd}^{(l)}(g)}$, and the (a, c) -entry of $\rho^{(k)}(g) E_{bd} \rho^{(l)}(g)^{-1}$ is $\rho_{ab}^{(k)}(g) \overline{\rho_{cd}^{(l)}(g)}$. Reading off the (a, c) -entry of \tilde{A} therefore yields

$$(\varphi_{ab}^{(k)} \mid \varphi_{cd}^{(l)}) = \frac{1}{\#G} \sum_{g \in G} \rho_{ab}^{(k)}(g) \overline{\rho_{cd}^{(l)}(g)} = \begin{cases} 0 & k \neq l, \\ \frac{\delta_{bd} \delta_{ac}}{d_k} & k = l, \end{cases}$$

which is the claimed identity. □

Theorem 6.8 (Peter–Weyl theorem for finite groups). *The functions $\{\sqrt{d_k} \varphi_{ij}^{(k)}\}_{k,i,j}$ form an orthonormal basis of $L(G)$.*

Proof. Orthonormality is Theorem 6.7. By Corollary 4.4, the total count is $\sum_k d_k^2 = \#G = \dim L(G)$, so they span. □

Corollary 6.9. *Restricting to class functions (i.e. to $\varphi_{11}^{(k)} + \dots + \varphi_{d_k d_k}^{(k)} = \chi_k$) recovers the orthonormal basis $\text{Irr}(G)$ of the space of class functions.*

6.3 Fourier Analysis on Abelian Groups

For the rest of this section let $G = \{g_1, \dots, g_n\}$ be a finite abelian group of order n . All irreducible representations are 1-dimensional, so $\text{Irr}(G) = \{\chi_1, \dots, \chi_n\}$ with each $\chi_i: G \rightarrow \mathbb{C}^\times$ a group homomorphism. The Peter–Weyl basis of $L(G)$ reduces to $\text{Irr}(G)$ itself.

Definition 6.10 (Fourier transform). The *Fourier transform* of $f \in L(G)$ is the function $\hat{f}: G \rightarrow \mathbb{C}$ defined by

$$\hat{f}(g_i) = n(\chi_i | f) = \sum_{g \in G} \overline{\chi_i(g)} f(g).$$

Theorem 6.11 (Fourier inversion). For any $f \in L(G)$,

$$f = \frac{1}{n} \sum_{i=1}^n \hat{f}(g_i) \chi_i.$$

Proof. Expand f in the orthonormal basis $\{\chi_i\}$: $f = \sum_i (\chi_i | f) \chi_i = \frac{1}{n} \sum_i \hat{f}(g_i) \chi_i$. □

Theorem 6.12 (Convolution theorem). The *Fourier transform satisfies $\widehat{a * b} = \hat{a} \cdot \hat{b}$ (pointwise product). Consequently, it is a ring isomorphism*

$$(L(G), +, *) \xrightarrow{\cong} (L(G), +, \cdot),$$

or equivalently $\mathbb{C}[G] \simeq \mathbb{C}^n$ as \mathbb{C} -algebras.

Proof. Setting $z = xy^{-1}$ and using that χ_i is a homomorphism:

$$\begin{aligned} \widehat{a * b}(g_i) &= \sum_{x \in G} \overline{\chi_i(x)} \sum_{y \in G} a(xy^{-1})b(y) = \sum_{y \in G} b(y) \sum_{z \in G} \overline{\chi_i(z)} a(z) \\ &= \sum_{y \in G} \overline{\chi_i(y)} b(y) \sum_{z \in G} \overline{\chi_i(z)} a(z) = \hat{b}(g_i) \hat{a}(g_i). \end{aligned}$$

The Fourier transform is a vector space isomorphism by Fourier inversion, and it sends $*$ to \cdot , so it is a ring isomorphism. The target ring (\mathbb{C}^n, \cdot) is the product ring $\mathbb{C} \times \dots \times \mathbb{C}$, recovering the abelian case of the Wedderburn decomposition. □

Example 6.13 (Discrete Fourier transform on \mathbb{Z}_n). Take $G = \mathbb{Z}_n$ with $\omega = e^{2\pi i/n}$ and $\chi_k(\bar{m}) = \omega^{km}$ (Proposition 4.34). For $f: \mathbb{Z}_n \rightarrow \mathbb{C}$,

$$\hat{f}(\bar{k}) = \sum_{m=0}^{n-1} \omega^{-km} f(\bar{m}), \quad f(\bar{m}) = \frac{1}{n} \sum_{k=0}^{n-1} \omega^{km} \hat{f}(\bar{k}).$$

These are the classical *discrete Fourier transform* (DFT) and its inverse. The convolution $(a * b)(\bar{m}) = \sum_{j=0}^{n-1} a(\bar{m} - \bar{j}) b(\bar{j})$ satisfies $\widehat{a * b} = \hat{a} \cdot \hat{b}$. The fast Fourier transform (FFT) computes \hat{f} in $O(n \log n)$ operations by exploiting this algebraic structure.

6.4 Cayley Graphs and Eigenvalues

Definition 6.14 (Cayley graph). Let G be a finite group. A subset $S \subseteq G$ is *symmetric* if $1_G \notin S$ and $s \in S \Rightarrow s^{-1} \in S$. The *Cayley graph* $\Gamma(G, S)$ associated to a symmetric subset S has vertex set G and an edge $\{g, h\}$ whenever $gh^{-1} \in S$ (equivalently, $g^{-1}h \in S$).

Remark 6.15. The Cayley graph is $\#S$ -regular. It is connected if and only if S generates G .

Example 6.16. Take $G = \mathbb{Z}_4$ and $S = \{\bar{1}, \bar{3}\}$. Then $\Gamma(\mathbb{Z}_4, S)$ is the 4-cycle with adjacency matrix

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

Theorem 6.17. Let $G = \{g_1, \dots, g_n\}$ be a finite abelian group, $S \subseteq G$ symmetric, and A the adjacency matrix of $\Gamma(G, S)$ (vertices in the order g_1, \dots, g_n). Then:

1. The eigenvalues of A are the real numbers $\lambda_i = \sum_{s \in S} \chi_i(s)$, $1 \leq i \leq n$.
2. An orthonormal basis of eigenvectors is $v_i = \frac{1}{\sqrt{n}}(\chi_i(g_1), \dots, \chi_i(g_n))^T$.

Proof. Let $\delta_S = \sum_{s \in S} \delta_s \in L(G)$ and let $F: L(G) \rightarrow L(G)$, $f \mapsto \delta_S * f$, be convolution by δ_S . We compute F in two bases.

In the basis $\{\delta_{g_i}\}$. Direct calculation gives $(\delta_S * \delta_{g_j})(g_i) = \sum_{s \in S} \delta_{sg_j}(g_i) = \mathbf{1}[g_i g_j^{-1} \in S] = A_{ij}$, so the matrix of F is exactly the adjacency matrix A .

In the basis $\{\chi_j\}$. Since each χ_j is a homomorphism,

$$(\delta_S * \chi_j)(x) = \sum_{s \in S} \chi_j(s^{-1}x) = \left(\sum_{s \in S} \chi_j(s^{-1}) \right) \chi_j(x).$$

Using $\chi_j(s^{-1}) = \overline{\chi_j(s)}$ and $S = S^{-1}$, the parenthesised sum equals $\lambda_j := \sum_{s \in S} \chi_j(s)$, which is real because $\overline{\lambda_j} = \sum_s \overline{\chi_j(s)} = \sum_s \chi_j(s^{-1}) = \lambda_j$. Hence $F\chi_j = \lambda_j \chi_j$.

Combining the two pictures: A has eigenvectors χ_j with eigenvalues λ_j . Expressing χ_j in the $\{\delta_{g_i}\}$ -basis gives the coordinate vector $(\chi_j(g_1), \dots, \chi_j(g_n))^T$, which is orthonormal up to the factor \sqrt{n} by Peter–Weyl (Theorem 6.8). \square

Corollary 6.18 (Circulant matrices). If A is the adjacency matrix of $\Gamma(\mathbb{Z}_n, S)$, then with $\omega = e^{2\pi i/n}$ its eigenvalues are $\lambda_k = \sum_{s \in S} \omega^{ks}$ for $k = 0, \dots, n-1$, with eigenvector $v_k = \frac{1}{\sqrt{n}}(1, \omega^k, \omega^{2k}, \dots, \omega^{(n-1)k})^T$.

Example 6.19. Take $G = \mathbb{Z}_6$ and $S = \{\pm\bar{1}, \pm\bar{2}\}$ with $\omega = e^{2\pi i/6}$. The eigenvalues of the adjacency matrix are

$$\lambda_k = 2 \cos \frac{\pi k}{3} + 2 \cos \frac{2\pi k}{3}, \quad k = 0, 1, \dots, 5.$$

6.5 Fourier Analysis on Non-Abelian Groups

For a non-abelian group G , the irreducible representations have degrees $d_k \geq 1$ and the Fourier transform takes values in a product of matrix algebras.

Definition 6.20 (Non-abelian Fourier transform). Let $\rho^{(1)}, \dots, \rho^{(s)}$ be unitary representatives of $\text{Irr}(G)$ with $d_k = \deg \rho^{(k)}$, and let $n = \#G$. The *Fourier transform* of $f \in L(G)$ is the s -tuple

$$T(f) = (\hat{f}(\rho^{(1)}), \dots, \hat{f}(\rho^{(s)})) \in \prod_{k=1}^s \mathcal{M}_{d_k}(\mathbb{C}),$$

where $\hat{f}(\rho^{(k)})$ is the $d_k \times d_k$ matrix with (i, j) -entry $\sum_{g \in G} \overline{\rho_{ij}^{(k)}(g)} f(g)$.

Remark 6.21. For abelian G , all $d_k = 1$ and $\hat{f}(\rho^{(k)}) = \hat{f}(g_k) \in \mathbb{C}$, recovering Definition 6.10.

Remark 6.22 (Fourier transform of a delta function). For the delta function δ_g , the definition gives

$$\hat{\delta}_g(\rho^{(k)})_{ij} = \sum_{x \in G} \overline{\rho_{ij}^{(k)}(x)} \delta_g(x) = \overline{\rho_{ij}^{(k)}(g)},$$

so $\hat{\delta}_g(\rho^{(k)}) = \overline{\rho^{(k)}(g)}$ (entry-wise conjugate of the matrix $\rho^{(k)}(g)$). Thus

$$T(\delta_g) = (\overline{\rho^{(1)}(g)}, \dots, \overline{\rho^{(s)}(g)}).$$

The tuple $T(\delta_g)$ packages the images of g under every irreducible representation; taking traces gives $\text{tr}(\hat{\delta}_g(\rho^{(k)})) = \overline{\chi_k(g)}$, i.e. the complex conjugates of the column of the character table at g .

Theorem 6.23 (Fourier inversion). For any $f \in L(G)$ and $g \in G$,

$$f(g) = \frac{1}{n} \sum_{k=1}^s d_k \sum_{i,j} \hat{f}(\rho^{(k)})_{ij} \varphi_{ij}^{(k)}(g).$$

Proof. Expand f in the Peter–Weyl basis (Theorem 6.8):

$$f = \sum_{k,i,j} (f | \sqrt{d_k} \varphi_{ij}^{(k)}) \sqrt{d_k} \varphi_{ij}^{(k)} = \sum_{k,i,j} d_k (f | \varphi_{ij}^{(k)}) \varphi_{ij}^{(k)}.$$

The coefficient is $(f | \varphi_{ij}^{(k)}) = \frac{1}{n} \sum_g f(g) \overline{\rho_{ij}^{(k)}(g)} = \frac{1}{n} \hat{f}(\rho^{(k)})_{ij}$. Evaluating at g gives the result. \square

Example 6.24 (Fourier transform on S_3). Let $G = S_3$, $n = 6$. There are three irreducible unitary representations:

- $\rho^{(1)}$: trivial representation, $d_1 = 1$;
- $\rho^{(2)}$: sign representation, $d_2 = 1$, with $\rho^{(2)}(\sigma) = \text{sgn}(\sigma)$;
- $\rho^{(3)}$: standard representation, $d_3 = 2$, acting on the subspace $V = \{x_1 + x_2 + x_3 = 0\} \subset \mathbb{C}^3$

by permuting coordinates. In the orthonormal basis $u_1 = \frac{1}{\sqrt{2}}(e_1 - e_2)$, $u_2 = \frac{1}{\sqrt{6}}(e_1 + e_2 - 2e_3)$ the matrices at three representative elements are

$$\rho^{(3)}(e) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \rho^{(3)}((12)) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \rho^{(3)}((123)) = \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}.$$

Take $f = \delta_{(12)} \in L(S_3)$. Since all entries of $\rho^{(3)}$ are real, Remark 6.22 gives

$$T(f) = \left(\underbrace{1}_{\hat{f}(\rho^{(1)})}, \quad \underbrace{-1}_{\hat{f}(\rho^{(2)})}, \quad \underbrace{\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}}_{\hat{f}(\rho^{(3)})} \right).$$

The degree-2 component is a non-scalar matrix – a feature impossible for abelian groups.

We verify Fourier inversion (Theorem 6.23) at two points. At $g = (12)$ (using only the diagonal entries of $\hat{f}(\rho^{(3)})$, since off-diagonal entries are zero):

$$\frac{1}{6} [1 \cdot (1)(1) + 1 \cdot (-1)(-1) + 2((-1)(-1) + (1)(1))] = \frac{1}{6}(1 + 1 + 4) = 1 = f((12)). \quad \checkmark$$

At $g = (123)$ (where $\text{sgn}((123)) = +1$ and $\rho_{11}^{(3)}((123)) = \rho_{22}^{(3)}((123)) = -\frac{1}{2}$):

$$\frac{1}{6} [1 \cdot 1 + (-1) \cdot 1 + 2((-1)(-\frac{1}{2}) + (1)(-\frac{1}{2}))] = \frac{1}{6}(1 - 1 + 0) = 0 = f((123)). \quad \checkmark$$

Theorem 6.25 (Wedderburn via Fourier). *The Fourier transform $T: L(G) \rightarrow \prod_{k=1}^s \mathcal{M}_{d_k}(\mathbb{C})$ is a ring isomorphism (with pointwise matrix multiplication on the right).*

Proof. T is a vector space isomorphism by Fourier inversion (it is injective and both spaces have dimension $\sum_k d_k^2 = n$). It remains to check $T(a * b) = T(a) \cdot T(b)$, i.e., $\widehat{a * b}(\rho^{(k)}) = \hat{a}(\rho^{(k)}) \hat{b}(\rho^{(k)})$ for each k . Setting $z = xy^{-1}$ and using that $\rho^{(k)}$ is a homomorphism:

$$\begin{aligned} \widehat{a * b}(\rho^{(k)})_{ij} &= \sum_x \overline{\rho_{ij}^{(k)}(x)} \sum_y a(xy^{-1})b(y) = \sum_y b(y) \sum_z \overline{\rho_{ij}^{(k)}(zy)} a(z) \\ &= \sum_y b(y) \sum_z \sum_m \overline{\rho_{im}^{(k)}(z)\rho_{mj}^{(k)}(y)} a(z) = \sum_m \hat{a}(\rho^{(k)})_{im} \hat{b}(\rho^{(k)})_{mj}. \end{aligned}$$

This is the (i, j) -entry of $\hat{a}(\rho^{(k)}) \hat{b}(\rho^{(k)})$, as required. □

Remark 6.26. This is the Wedderburn decomposition $\mathbb{C}[G] \simeq \prod_{\rho \in \text{Irr } G} \mathcal{M}_{\text{deg } \rho}(\mathbb{C})$ from Theorem 4.15, now proved via Fourier analysis rather than module theory. The Fourier inversion formula also recovers the isotypic projections of Theorem 4.24: the element $\pi_\rho = \frac{\text{deg } \rho}{\#G} \sum_g \overline{\chi_\rho(g)} e_g$ in $\mathbb{C}[G]$ corresponds to the tuple with the identity matrix in the ρ -slot and zero elsewhere.

6.6 Exercises

Exercise 6.27 (DFT on \mathbb{Z}_3). Let $f: \mathbb{Z}_3 \rightarrow \mathbb{C}$ be defined by $f(\bar{k}) = \sin(2\pi k/3)$ for $k = 0, 1, 2$. Compute the Fourier transform $\hat{f}: \mathbb{Z}_3 \rightarrow \mathbb{C}$ explicitly using Definition 6.10.

(Solution)

Exercise 6.28 (Cayley graph of \mathbb{Z}_6). Let $S = \{\pm\bar{2}, \pm\bar{3}\} \subseteq \mathbb{Z}_6$ (where $\pm\bar{3} = \{\bar{3}\}$ and $\pm\bar{2} = \{\bar{2}, \bar{4}\}$, so $S = \{\bar{2}, \bar{3}, \bar{4}\}$). Draw the Cayley graph $\Gamma(\mathbb{Z}_6, S)$ and compute the eigenvalues of its adjacency matrix using Corollary 6.18.

(Solution)

Exercise 6.29 (Plancherel formula). Let G be a finite abelian group of order n with irreducible characters χ_1, \dots, χ_n , and let \hat{f} denote the Fourier transform of Definition 6.10. Prove the *Plancherel formula*

$$(a | b) = \frac{1}{n}(\hat{a} | \hat{b})$$

for all $a, b \in L(G)$, where the inner product on the right is $(\hat{a} | \hat{b}) = \frac{1}{n} \sum_{i=1}^n \hat{a}(g_i) \overline{\hat{b}(g_i)}$.

(Solution)

Exercise 6.30 (Central idempotents). Let G be a finite group of order n , with unitary irreducible representations $\rho^{(1)}, \dots, \rho^{(s)}$ (degrees d_k , characters χ_k). Define $e_k \in L(G)$ by $e_k(g) = \frac{d_k}{n} \chi_k(g)$.

1. Show that if $f \in Z(L(G))$, then $\hat{f}(\rho^{(k)}) = \frac{n}{d_k} (f | \chi_k) I_{d_k}$. (*Hint*: f is a class function, so $\hat{f}(\rho^{(k)})$ commutes with all $\rho^{(k)}(g)$; apply Corollary 3.3 and take the trace.)

2. Deduce that

$$\hat{e}_i(\rho^{(k)}) = \begin{cases} I_{d_k} & i = k, \\ 0 & i \neq k. \end{cases}$$

3. Deduce that $e_i * e_j = \begin{cases} e_i & i = j, \\ 0 & i \neq j, \end{cases}$ and that each e_k is a central idempotent in $(L(G), *)$.

4. Deduce that $e_1 + \dots + e_s = \delta_{1G}$. (*Hint*: apply the Fourier inversion formula Theorem 6.23.)

(Solution)

Exercise 6.31 (Eigenvalues of Cayley graphs of non-abelian groups). Let G be a finite group of order n , with unitary irreducible representations $\rho^{(1)}, \dots, \rho^{(s)}$ (degrees d_k , characters χ_k). Let $a \in Z(L(G))$ and define $F: L(G) \rightarrow L(G)$ by $F(b) = a * b$.

1. Show that each matrix coefficient $\varphi_{ij}^{(k)}$ is an eigenvector of F with eigenvalue $\frac{n}{d_k} (a | \chi_k)$. (*Hint*: use Exercise 6.30(1) and the Fourier inversion formula.)

2. Conclude that F is diagonalizable.

3. Let $S \subseteq G$ be a symmetric subset satisfying $gSg^{-1} = S$ for all $g \in G$ (so that $\delta_S \in Z(L(G))$), and let A be the adjacency matrix of the Cayley graph $\Gamma(G, S)$. Show that the eigenvalues of A are

$$\lambda_k = \frac{1}{d_k} \sum_{s \in S} \chi_k(s), \quad k = 1, \dots, s,$$

each with multiplicity d_k^2 .

4. Compute the eigenvalues (and multiplicities) of the adjacency matrix of the Cayley graph of S_3 with $S = \{(12), (13), (23)\}$.

(Solution)

Exercise 6.32 (Convolution and random variables). Let G be a finite group and let X, Y be independent G -valued random variables with probability distributions $\mu, \nu \in L(G)$, i.e. $\Pr[X = g] = \mu(g)$ and $\Pr[Y = g] = \nu(g)$ for all $g \in G$. Show that the product XY has distribution $\mu * \nu$.

(Solution)

Chapter 7

Burnside's Theorem

In this chapter we prove one of the first major applications of representation theory: Burnside's pq -theorem, which states that a group of order $p^a q^b$ (with p, q prime) is never simple unless it is cyclic of prime order. The proof requires a brief excursion into algebraic number theory, specifically the arithmetic of algebraic integers and a touch of Galois theory of cyclotomic fields.

7.1 A Little Number Theory

Definition 7.1 (Algebraic integer). A complex number α is called an *algebraic integer* if it is a root of a monic polynomial with integer coefficients: there exists $p(z) = z^n + a_{n-1}z^{n-1} + \cdots + a_0$ with $a_0, \dots, a_{n-1} \in \mathbb{Z}$ and $p(\alpha) = 0$.

Example 7.2 (n th roots). Let $m \in \mathbb{Z}$. The polynomial $z^n - m$ is monic with integer coefficients, so every n th root of m is an algebraic integer. In particular $\sqrt{2}$ is an algebraic integer, as is $e^{2\pi i/n}$; in fact every n th root of unity is an algebraic integer.

Example 7.3 (Eigenvalues of integer matrices). Let $A = (a_{ij})$ be an $n \times n$ matrix with integer entries $a_{ij} \in \mathbb{Z}$. The characteristic polynomial $p_A(z) = \det(zI - A)$ is monic with integer coefficients, so every eigenvalue of A is an algebraic integer.

A rational number such as $1/2$ satisfies $2z - 1 = 0$, a polynomial with integer coefficients but non-unit leading coefficient, yet $1/2$ is *not* an algebraic integer. The requirement that the leading coefficient be 1 is essential.

Proposition 7.4. A rational number r is an algebraic integer if and only if $r \in \mathbb{Z}$.

Proof. Every integer r satisfies $z - r = 0$, so integers are algebraic integers. Conversely, write $r = m/n$ with $m, n \in \mathbb{Z}$, $n > 0$, and $\gcd(m, n) = 1$. Suppose r satisfies $z^k + a_{k-1}z^{k-1} + \cdots + a_0 = 0$ with $a_i \in \mathbb{Z}$. Multiplying through by n^k :

$$m^k + a_{k-1}m^{k-1}n + \cdots + a_1mn^{k-1} + a_0n^k = 0.$$

Hence $m^k = -n(a_{k-1}m^{k-1} + \cdots + a_0n^{k-1})$, so $n \mid m^k$. Since $\gcd(m, n) = 1$, we conclude $n = 1$ and $r = m \in \mathbb{Z}$. \square

A useful strategy for showing that an integer d divides an integer n is to show that n/d is an algebraic integer; Proposition 7.4 then forces $n/d \in \mathbb{Z}$. For this to work, we need algebraic integers to be closed under arithmetic operations, which we prove via the following characterisation.

Lemma 7.5. *An element $y \in \mathbb{C}$ is an algebraic integer if and only if there exist $y_1, \dots, y_t \in \mathbb{C}$, not all zero, such that*

$$yy_i = \sum_{j=1}^t a_{ij} y_j \quad \text{for all } 1 \leq i \leq t,$$

with $a_{ij} \in \mathbb{Z}$ (i.e. yy_i is an integral linear combination of y_1, \dots, y_t for each i).

Proof. Suppose y is an algebraic integer, a root of $p(z) = z^n + a_{n-1}z^{n-1} + \dots + a_0$. Take $y_i = y^{i-1}$ for $1 \leq i \leq n$. Then $yy_i = y^i = y_{i+1}$ for $1 \leq i \leq n-1$, and $yy_n = y^n = -a_0y_1 - a_1y_2 - \dots - a_{n-1}y_n$ (since y satisfies p). Since $y_1 = 1 \neq 0$, the elements are not all zero.

Conversely, suppose such y_1, \dots, y_t exist. Let $A = (a_{ij})$ and $Y = (y_1, \dots, y_t)^\top \in \mathbb{C}^t$. The condition reads $[AY]_i = \sum_j a_{ij} y_j = yy_i = y[Y]_i$, so $AY = yY$. Since $Y \neq 0$, y is an eigenvalue of the $t \times t$ integer matrix A , hence an algebraic integer by Example 7.3. \square

Corollary 7.6. *The set \mathbb{A} of algebraic integers is a subring of \mathbb{C} . In particular, sums and products of algebraic integers are algebraic integers. Moreover, the complex conjugate of an algebraic integer is an algebraic integer.*

Proof. If $p(z)$ is monic with integer coefficients and $p(\alpha) = 0$, then $(-1)^n p(-z)$ is a monic polynomial with integer coefficients vanishing at $-\alpha$, so $-\alpha \in \mathbb{A}$.

Let $y, y' \in \mathbb{A}$ and choose witnesses y_1, \dots, y_t and y'_1, \dots, y'_s as in Lemma 7.5. The products $\{y_i y'_k : 1 \leq i \leq t, 1 \leq k \leq s\}$ are not all zero. For the sum:

$$(y + y') y_i y'_k = yy_i \cdot y'_k + y' y'_k \cdot y_i = \sum_j a_{ij} y_j y'_k + \sum_\ell b_{k\ell} y'_\ell y_i,$$

an integral linear combination of the products $y_j y'_\ell$, so $y + y' \in \mathbb{A}$ by Lemma 7.5. For the product:

$$yy' \cdot y_i y'_k = (yy_i)(y' y'_k) = \left(\sum_j a_{ij} y_j \right) \left(\sum_\ell b_{k\ell} y'_\ell \right) = \sum_{j,\ell} a_{ij} b_{k\ell} y_j y'_\ell,$$

so $yy' \in \mathbb{A}$. For conjugation: if $p(\alpha) = 0$ with $p(z) = z^n + a_{n-1}z^{n-1} + \dots + a_0$ and $a_i \in \mathbb{Z} \subseteq \mathbb{R}$, then $p(\bar{\alpha}) = \overline{p(\alpha)} = 0$. \square

7.2 The Dimension Theorem

The connection between algebraic integers and representation theory begins with the following observation.

Corollary 7.7. *Let χ be a character of a finite group G . Then $\chi(g)$ is an algebraic integer for all $g \in G$.*

Proof. Let $\varphi: G \rightarrow \text{GL}_m(\mathbb{C})$ be a representation with character χ . By Lemma 3.22, φ_g is diagonalizable with eigenvalues $\lambda_1, \dots, \lambda_m$ that are n th roots of unity (where $n = \#G$). Roots of unity are algebraic integers (Example 7.2), and \mathbb{A} is closed under addition (Corollary 7.6), so $\chi(g) = \lambda_1 + \dots + \lambda_m \in \mathbb{A}$. \square

Remark 7.8. The proof shows that $\chi_\varphi(g)$ is a sum of exactly $\deg \varphi$ roots of unity of order dividing $\#G$. We shall use this precision later.

The key algebraic fact needed for the dimension theorem is:

Theorem 7.9. *Let φ be an irreducible representation of G of degree d , let $g \in G$, and let $h = \#C$ where C is the conjugacy class of g . Then $(h/d)\chi_\varphi(g)$ is an algebraic integer.*

Proof. Let C_1, \dots, C_s be the conjugacy classes of G with sizes $h_i = \#C_i$, and let χ_i denote the value of χ_φ on C_i . For each i define the class sum

$$T_i = \sum_{x \in C_i} \varphi_x \in \text{End}(V).$$

We establish two claims.

Claim 1. $T_i = \frac{h_i \chi_i}{d} I$.

For any $g \in G$, $\varphi_g T_i \varphi_g^{-1} = \sum_{x \in C_i} \varphi_{gxg^{-1}} = \sum_{y \in C_i} \varphi_y = T_i$ (since C_i is stable under conjugation). Thus T_i commutes with all φ_g , so by Corollary 3.3 we have $T_i = \lambda I$ for some $\lambda \in \mathbb{C}$. Taking traces: $d\lambda = \text{tr}(T_i) = \sum_{x \in C_i} \chi_i = h_i \chi_i$, giving $\lambda = h_i \chi_i / d$.

Claim 2. $T_i T_j = \sum_{k=1}^s a_{ijk} T_k$ for non-negative integers a_{ijk} .

Direct computation gives $T_i T_j = \sum_{g \in G} a_{ijg} \varphi_g$ where $a_{ijg} = \#\{(x, y) \in C_i \times C_j : xy = g\}$. If $g' = k g k^{-1}$, the map $(x, y) \mapsto (k x k^{-1}, k y k^{-1})$ is a bijection from $\{xy = g\}$ to $\{xy = g'\}$ inside $C_i \times C_j$, so a_{ijg} depends only on the conjugacy class of g . Writing a_{ijk} for the common value on C_k gives $T_i T_j = \sum_k a_{ijk} T_k$.

Conclusion. Set $\beta_k = h_k \chi_k / d$ for $k = 1, \dots, s$. Substituting Claim 1 into Claim 2 gives $\beta_i \beta_k = \sum_j a_{ikj} \beta_j$ for each i, k . Fixing i , the elements β_1, \dots, β_s satisfy $\beta_i \cdot \beta_k = \sum_j a_{ikj} \beta_j$, an integral linear combination of β_1, \dots, β_s . Since $\beta_1 = h_1 \chi_1 / d = 1 \cdot d / d = 1 \neq 0$, the β_j are not all zero. By Lemma 7.5, each $\beta_i = h_i \chi_i / d$ is an algebraic integer. \square

Theorem 7.10 (Dimension theorem). *Let φ be an irreducible representation of a finite group G of degree d . Then d divides $\#G$.*

Proof. Write $n = \#G$. By the first orthogonality relations (Theorem 3.35), $\langle \chi_\varphi, \chi_\varphi \rangle = 1$, i.e.

$$\frac{n}{d} = \sum_{g \in G} \overline{\chi_\varphi(g)} \cdot \frac{\chi_\varphi(g)}{d}.$$

Grouping by conjugacy classes C_1, \dots, C_s with sizes h_i and character values χ_i :

$$\frac{n}{d} = \sum_{i=1}^s \overline{\chi_i} \cdot \frac{h_i \chi_i}{d}.$$

Each $h_i \chi_i / d$ is an algebraic integer by Theorem 7.9; each $\overline{\chi_i}$ is an algebraic integer by Corollary 7.7 and Corollary 7.6. Since \mathbb{A} is a ring, each summand is algebraic, and so is the sum n/d . Being rational, Proposition 7.4 gives $n/d \in \mathbb{Z}$, i.e. $d \mid n$. \square

Corollary 7.11. *If $\#G = p^2$ for a prime p , then G is abelian.*

Proof. Each irreducible degree d_i divides p^2 , so $d_i \in \{1, p, p^2\}$. If $d_i \geq p$ for some i , then $d_i^2 \geq p^2 = \#G$, leaving $\sum_{j \neq i} d_j^2 = 0$ (impossible since the trivial representation contributes $d_j = 1$). Hence all $d_i = 1$. Then $\# \text{Irr}(G) = \sum_i 1 = \sum_i d_i^2 = p^2 = \#G$, so by Theorem 4.21 there are p^2 conjugacy classes and p^2 elements; every conjugacy class is a singleton, meaning every element is central. Thus $G = Z(G)$ is abelian. \square

Recall that the *commutator subgroup* G' of G is the subgroup generated by all commutators $g^{-1}h^{-1}gh$ with $g, h \in G$. It is normal, G/G' is abelian, and if $N \triangleleft G$ with G/N abelian then $G' \subseteq N$.

Lemma 7.12. *The number of degree-one irreducible representations of G equals $[G : G']$, and this number divides $\#G$.*

Proof. A degree-one representation $\rho: G \rightarrow \mathbb{C}^*$ has abelian image, so $G' \subseteq \ker \rho$ and ρ factors as $\rho = \psi \circ \pi$, where $\pi: G \rightarrow G/G'$ is the quotient map and ψ is a degree-one representation of G/G' . Conversely, every degree-one representation of G/G' pulls back to one of G this way. Since G/G' is abelian, by Corollary 4.23 all of its irreducible representations have degree one, and by Theorem 4.21 there are $\#(G/G') = [G : G']$ of them. Finally, $[G : G']$ divides $\#G$ by Lagrange's theorem. \square

Corollary 7.13. *Let $p < q$ be primes with $q \not\equiv 1 \pmod{p}$. Then every group of order pq is abelian (hence cyclic).*

Proof. Let d_1, \dots, d_s be the irreducible degrees. Each d_i divides pq and satisfies $d_i^2 \leq pq$; since $p < q$, both $q^2 > pq$ and $(pq)^2 > pq$, so $d_i \in \{1, p\}$. Let m be the number of degree-1 representations and r the number of degree- p representations. Then $m + p^2r = pq$, so $p \mid m$. By Lemma 7.12, $m \mid pq$; combined with $p \mid m$, we get $m \in \{p, pq\}$. If $m = p$, then $p^2r = p(q - 1)$, giving $pr = q - 1$, i.e. $p \mid q - 1$, meaning $q \equiv 1 \pmod{p}$, contrary to hypothesis. Hence $m = pq$ and G is abelian. \square

7.3 Burnside's Theorem

The proof of Burnside's theorem uses Galois theory of cyclotomic fields. We develop what we need from scratch.

Recall from Remark 7.8 that $\chi_\varphi(g)$ is a sum of $d = \deg \varphi$ roots of unity of order dividing $n = \#G$. The following elementary lemma controls the absolute value of such sums.

Lemma 7.14. *Let $\lambda_1, \dots, \lambda_d$ be roots of unity. Then $|\lambda_1 + \dots + \lambda_d| \leq d$, with equality if and only if $\lambda_1 = \dots = \lambda_d$.*

Proof. The triangle inequality gives $|\lambda_1 + \dots + \lambda_d| \leq |\lambda_1| + \dots + |\lambda_d| = d$. Equality holds if and only if all non-zero summands point in the same direction, i.e. all λ_i are non-negative real multiples of the same complex number. Since $|\lambda_i| = 1$, this forces $\lambda_1 = \dots = \lambda_d$. \square

Let $\omega = e^{2\pi i/n}$ and let $\Gamma = \text{Gal}(\mathbb{Q}[\omega]/\mathbb{Q})$ be the group of all field automorphisms $\sigma: \mathbb{Q}[\omega] \rightarrow \mathbb{Q}[\omega]$ that fix \mathbb{Q} pointwise. By the fundamental theorem of Galois theory, $|\Gamma| = \phi(n)$ (Euler's totient function) and $\Gamma \cong \mathbb{Z}_n^*$.

Lemma 7.15. *Let $p(z)$ be a polynomial with rational coefficients and let $\alpha \in \mathbb{Q}[\omega]$ be a root of p . Then $\sigma(\alpha)$ is also a root of p for every $\sigma \in \Gamma$.*

Proof. Write $p(z) = \sum a_k z^k$ with $a_k \in \mathbb{Q}$. Then $p(\sigma(\alpha)) = \sum a_k \sigma(\alpha)^k = \sigma(\sum a_k \alpha^k) = \sigma(p(\alpha)) = \sigma(0) = 0$, using $\sigma(a_k) = a_k$ since $a_k \in \mathbb{Q}$. \square

Corollary 7.16. *If α is an n th root of unity then $\sigma(\alpha)$ is an n th root of unity for every $\sigma \in \Gamma$.*

Proof. Apply Lemma 7.15 to $p(z) = z^n - 1$. \square

Corollary 7.17. *If $\alpha \in \mathbb{Q}[\omega]$ is an algebraic integer and $\sigma \in \Gamma$, then $\sigma(\alpha)$ is an algebraic integer.*

Proof. α is a root of a monic polynomial p with integer coefficients; $\sigma(\alpha)$ is also a root by Lemma 7.15. \square

We use the following two standard results from Galois theory without proof.

Theorem 7.18. *Let $\alpha \in \mathbb{Q}[\omega]$. Then $\sigma(\alpha) = \alpha$ for all $\sigma \in \Gamma$ if and only if $\alpha \in \mathbb{Q}$.*

Corollary 7.19. *For any $\alpha \in \mathbb{Q}[\omega]$, the product $\prod_{\sigma \in \Gamma} \sigma(\alpha)$ lies in \mathbb{Q} .*

Proof. For any $\tau \in \Gamma$, applying τ permutes the factors: $\tau(\prod_{\sigma} \sigma(\alpha)) = \prod_{\sigma} \tau\sigma(\alpha) = \prod_{\rho} \rho(\alpha)$. Hence the product is fixed by all $\tau \in \Gamma$ and belongs to \mathbb{Q} by Theorem 7.18. \square

The following theorem is the key technical engine of Burnside's argument.

Theorem 7.20. *Let G have order n , let C be a conjugacy class of G , and let $\varphi: G \rightarrow \text{GL}_d(\mathbb{C})$ be an irreducible representation with $\gcd(\#C, d) = 1$. Then for every $g \in C$, either $\varphi_g = \lambda I$ for some $\lambda \in \mathbb{C}^*$, or $\chi_\varphi(g) = 0$.*

Proof. Set $\chi = \chi_\varphi$ and $h = \#C$. Since $\gcd(h, d) = 1$, choose integers k, j with $kh + jd = 1$. Define

$$\alpha = k \cdot \frac{h}{d} \chi(g) + j \chi(g) = \frac{\chi(g)}{d}.$$

This is an algebraic integer: $(h/d)\chi(g)$ is algebraic by Theorem 7.9, $\chi(g)$ is algebraic by Corollary 7.7, and \mathbb{A} is a ring (Corollary 7.6).

Since χ is a class function, it is either zero on all of C or on none. It therefore suffices to show: if φ_g is not a scalar matrix, then $\chi(g) = 0$.

Assume $\varphi_g \neq \lambda I$ for all λ . By Lemma 3.22, φ_g is diagonalizable with eigenvalues $\lambda_1, \dots, \lambda_d$ that are n th roots of unity, hence in $\mathbb{Q}[\omega]$. Since φ_g is not scalar, the λ_i are not all equal, so Lemma 7.14 gives $|\chi(g)| < d$, hence $|\alpha| < 1$.

For any $\sigma \in \Gamma$: $\sigma(\alpha) = \sigma(\chi(g))/d = (\sigma(\lambda_1) + \dots + \sigma(\lambda_d))/d$. By Corollary 7.16, each $\sigma(\lambda_i)$ is an n th root of unity. Since σ is injective and the λ_i are not all equal, neither are the $\sigma(\lambda_i)$; another application of Lemma 7.14 gives $|\sigma(\alpha)| < 1$. By Corollary 7.17, $\sigma(\alpha)$ is an algebraic integer.

Therefore $q = \prod_{\sigma \in \Gamma} \sigma(\alpha)$ is a product of algebraic integers each of modulus < 1 , so q is an algebraic integer with $|q| < 1$. By Corollary 7.19, $q \in \mathbb{Q}$, and by Proposition 7.4, $q \in \mathbb{Z}$. Since $|q| < 1$, we get $q = 0$, hence $\sigma(\alpha) = 0$ for some σ . Since σ is a field automorphism, $\alpha = 0$, i.e. $\chi(g) = 0$. \square

Lemma 7.21. *Let G be a finite non-abelian group. If G has a conjugacy class $C \neq \{1\}$ with $\#C$ a power of a prime p , then G is not simple.*

Proof. Suppose for contradiction that G is simple. Let $\varphi^{(1)}, \dots, \varphi^{(s)}$ be the irreducible representations of G with $\varphi^{(1)}$ trivial, characters χ_1, \dots, χ_s , and degrees $d_1 = 1, d_2, \dots, d_s$. For $k \geq 2$, the kernel $\ker \varphi^{(k)}$ is normal in G . By simplicity it is $\{1\}$ or G ; since $\varphi^{(k)}$ is non-trivial, $\ker \varphi^{(k)} = \{1\}$, so $\varphi^{(k)}$ is injective. Since G is non-abelian and \mathbb{C}^* is abelian, $d_k > 1$ for all $k \geq 2$. Since G is simple and non-abelian, $Z(G) = \{1\}$, so $\#C = p^t$ with $t \geq 1$.

Fix $g \in C$, so in particular $g \neq 1$. We claim that for every $k \geq 2$ with $p \nmid d_k$, $\chi_k(g) = 0$.

Indeed, $\gcd(\#C, d_k) = \gcd(p^t, d_k) = 1$, so Theorem 7.20 applies: either $\varphi_g^{(k)} = \lambda I$ or $\chi_k(g) = 0$. In the first case, the set $Z_k = \{x \in G : \varphi_x^{(k)} \text{ is scalar}\}$ is the preimage of $Z(\text{GL}_{d_k}(\mathbb{C}))$ under $\varphi^{(k)}$, hence a normal subgroup of G . Since $\varphi^{(k)}$ is irreducible of degree $d_k > 1$, it cannot have scalar image, so $Z_k \neq G$; by simplicity, $Z_k = \{1\}$. But $\varphi_g^{(k)}$ scalar means $g \in Z_k = \{1\}$, contradicting $g \neq 1$. So the second case must hold, i.e. $\chi_k(g) = 0$.

The character of the regular representation (Theorem 4.3) satisfies $\chi_L(g) = 0$ for $g \neq 1$:

$$0 = 1 + \sum_{k=2}^s d_k \chi_k(g) = 1 + \sum_{\substack{k \geq 2 \\ p \nmid d_k}} d_k \chi_k(g).$$

Dividing by p :

$$\sum_{\substack{k \geq 2 \\ p \nmid d_k}} \frac{d_k}{p} \chi_k(g) = -\frac{1}{p}.$$

The left side is a sum of integer multiples of algebraic integers, hence an algebraic integer. Being rational, Proposition 7.4 forces it to be an integer. But $-1/p \notin \mathbb{Z}$ – a contradiction. \square

Theorem 7.22 (Burnside's pq -theorem). *Let G be a group of order $p^a q^b$ with p, q prime. Then G is not simple unless it is cyclic of prime order.*

Proof. An abelian group is simple if and only if it is cyclic of prime order. So we may assume G is non-abelian.

If $a = 0$ (or $b = 0$), then G is a p -group (or q -group). A non-trivial p -group has non-trivial centre $Z(G)$, which is a proper non-trivial normal subgroup when G is non-abelian, so G is not simple.

Suppose $a, b \geq 1$. By Sylow's theorem, G has a Sylow q -subgroup H of order q^b . Choose $1 \neq g \in Z(H)$ (possible since $Z(H) \neq \{1\}$ as H is a non-trivial q -group). Every element of H commutes with g , so $H \subseteq C_G(g)$, and by orbit-stabiliser for the conjugation action,

$$\#C_g = [G : C_G(g)] \mid [G : H] = p^a.$$

Thus $\#C_g = p^t$ for some $0 \leq t \leq a$. Since $g \neq 1$, we have $C_g \neq \{1\}$. By Lemma 7.21, G is not simple. \square

Remark 7.23. Burnside's theorem is often stated in the equivalent form: every group of order $p^a q^b$ is solvable. This follows by induction: a non-simple group has a proper normal subgroup N , and both N and G/N have orders of the form $p^{a'} q^{b'}$ with $a' \leq a, b' \leq b$, and $\#N < \#G$, so they are solvable by induction, and hence so is G .

7.4 Exercises

Exercise 7.24 (Group of order 39). Let G be a non-abelian group of order $39 = 3 \cdot 13$.

1. Determine the degree of every irreducible representation of G and how many irreducible representations of each degree G possesses. (*Hint*: note that $13 \equiv 1 \pmod{3}$, so Corollary 7.13 does not rule out a non-abelian group of this order. Use Theorem 7.10 and Corollary 4.4 to constrain the possible degrees.)
2. Determine the number of conjugacy classes of G .

(Solution)

Exercise 7.25 (Non-solvable groups of order $p^a q^b$). Prove that if there exists a non-solvable group of order $p^a q^b$ (with p, q prime), then there exists a simple non-abelian group of order $p^{a'} q^{b'}$ for some $a' \leq a, b' \leq b$.

(Solution)

Exercise 7.26 (Kernel via characters). Let $\varphi: G \rightarrow \mathrm{GL}_d(\mathbb{C})$ be a representation with character χ . Prove that $g \in \ker \varphi$ if and only if $\chi(g) = d$. (*Hint*: use Lemma 3.22 and Lemma 7.14.)

(Solution)

Appendix A

Solutions to Exercises

A.1 Chapter 1

Solution to Exercise 1.29.

1. Since $\dim V = 1$, the only subspaces of V are $\{0\}$ and V itself, so ρ has no proper nonzero subrepresentations; hence ρ is irreducible. Every irreducible representation is indecomposable.
2. (\Rightarrow) If W is a subrepresentation it is stable under every $\rho(g)$, so $\rho(g)(v) \in W = Kv$, hence $\rho(g)(v) = \mu_g v$ for some $\mu_g \in K$. Thus v is an eigenvector of every $\rho(g)$.
(\Leftarrow) Suppose $\rho(g)(v) = \mu_g v$ for all $g \in G$. For any $w = \lambda v \in W$ and $g \in G$, $\rho(g)(w) = \lambda \rho(g)(v) = \lambda \mu_g v \in W$. So W is stable under all $\rho(g)$.
3. We induct on $\dim V$. If $\dim V = 1$, take V itself. Suppose $\dim V > 1$.

If every $\rho(g)$ acts as a scalar, then any nonzero $v \in V$ is a common eigenvector of all $\rho(g)$, and Kv is a degree-1 subrepresentation.

Otherwise pick $g_0 \in G$ such that $\rho(g_0)$ is not scalar. Over \mathbb{C} its characteristic polynomial has a root λ ; let $W = \text{Ker}(\rho(g_0) - \lambda \text{id}_V)$. Then $0 < \dim W < \dim V$. For any $g \in G$ and $v \in W$:

$$\rho(g_0)(\rho(g)(v)) = \rho(g_0 g)(v) = \rho(g g_0)(v) = \rho(g)(\rho(g_0)(v)) = \lambda \rho(g)(v),$$

using that G is abelian. So $\rho(g)(v) \in W$, making W a subrepresentation. By the induction hypothesis, W contains a degree-1 subrepresentation of V .

Remark A.1. This shows that over \mathbb{C} , every representation of an abelian group of degree > 1 is reducible. We will see later that if G is finite, every such representation decomposes as a direct sum of degree-1 representations.

Solution to Exercise 1.30.

1. Using the standard basis (e_1 pointing right, e_2 pointing up):

$$\begin{aligned} \rho(\text{id}) &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, & \rho(r) &= \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, & \rho(r^2) &= \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, & \rho(r^3) &= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \\ \rho(t) &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, & \rho(t') &= \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, & \rho(s) &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, & \rho(s') &= \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}. \end{aligned}$$

2. All eight matrices are distinct, so ρ is injective, i.e. faithful.
3. Since $\deg \rho = 2$, any proper nonzero subrepresentation has degree 1, and by part (2) of Exercise 1.29 this requires a common eigenvector of all $\rho(g)$. But the characteristic polynomial of $\rho(r) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ is $x^2 + 1$, with no real roots. So no common eigenvector exists, and ρ is irreducible (and indecomposable).
4. Over \mathbb{C} the previous argument fails since $\rho(r)$ now has eigenvalues $\pm i$. However, any common eigenline for all $\rho(g)$ would also have to be an eigenspace of $\rho(t) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, whose only eigenspaces are the coordinate axes. Neither coordinate axis is an eigenline of $\rho(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ (whose eigenvectors are proportional to $(1, \pm 1)^\top$). So $\rho_{\mathbb{C}}$ is still irreducible.

Remark A.2. This shows that the commutativity hypothesis in part (3) of Exercise 1.29 is necessary: D_8 is non-abelian, yet $\rho_{\mathbb{C}}$ is an irreducible complex representation of degree 2.

Solution to Exercise 1.31.

Let $T, U \in \text{Hom}_G(V_1, V_2)$, $\lambda \in K$, $g \in G$, $v_1 \in V_1$. Then

$$(T + U)(\rho_1(g)(v_1)) = T(\rho_1(g)(v_1)) + U(\rho_1(g)(v_1)) = \rho_2(g)(T(v_1)) + \rho_2(g)(U(v_1)) = \rho_2(g)((T + U)(v_1)),$$

and $(\lambda T)(\rho_1(g)(v_1)) = \lambda T(\rho_1(g)(v_1)) = \lambda \rho_2(g)(T(v_1)) = \rho_2(g)((\lambda T)(v_1))$. So $T + U$ and λT both lie in $\text{Hom}_G(V_1, V_2)$.

Solution to Exercise 1.32.

1. Since $\deg \Delta = 2$, if reducible it would have a degree-1 subrepresentation spanned by a common eigenvector. The matrix of (123) has characteristic polynomial $x^2 + x + 1$, which has negative discriminant, so (123) has no eigenvectors over \mathbb{R} . Hence Δ is irreducible and therefore indecomposable.

Remark A.3. In fact Δ is irreducible even over \mathbb{C} : the matrix of (12) has eigenvalues ± 1 with eigenvectors $v_+ = (1, 0)^\top$ and $v_- = (1, -2)^\top$, but neither is an eigenvector of the matrix of (123).

2. Let $\sigma = (123)$, $\tau = (12)$, and let u span $\mathbf{1}$ while (e_1, e_2) is the standard basis of Δ . Define $f: \mathbf{1} \oplus \Delta \rightarrow \text{Perm}$ by

$$f(u) = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \quad f(e_1) = \begin{pmatrix} 1 \\ 1 \\ -2 \end{pmatrix}, \quad f(e_2) = \begin{pmatrix} -1 \\ 2 \\ -1 \end{pmatrix}.$$

The change-of-basis determinant equals $9 \neq 0$, so f is invertible. One verifies equivariance on generators σ, τ and basis vectors:

- $f(\sigma u) = f(u) = \sigma f(u)$, since (123) fixes $(1, 1, 1)^\top$.
- $f(\tau e_1) = f(e_1) = \tau f(e_1)$, since (12) fixes $(1, 1, -2)^\top$.
- $f(\sigma e_1) = f(-e_1 + e_2) = (-2, 1, 1)^\top = \sigma(1, 1, -2)^\top$.
- $f(\tau e_2) = f(e_1 - e_2) = (2, -1, -1)^\top = \tau(-1, 2, -1)^\top$.
- $f(\sigma e_2) = f(-e_1) = (-1, -1, 2)^\top = \sigma(-1, 2, -1)^\top$.

Thus $f: \mathbf{1} \oplus \Delta \xrightarrow{\sim} \text{Perm}$ is an isomorphism of representations.

Solution to Exercise 1.33.

Let $S = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$ be the matrix of (123) and $T = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$ the matrix of (12).

Irreducibility of Δ .

Case $p = 2$: The only eigenvalue of T is $1 = -1$, with eigenspace spanned by $v_+ = (1, 0)^\top$. Since $sv_+ = (-1, 1)^\top$ is not a scalar multiple of v_+ , no common eigenvector exists and Δ is irreducible.

Case $p \neq 2$: T has distinct eigenvalues ± 1 , with eigenvectors $v_+ = (1, 0)^\top$ and $v_- = (1, -2)^\top$.

- $sv_+ = (-1, 1)^\top$: not collinear to v_+ for any p (second coordinate is $1 \neq 0$).
- $sv_- = (1, 1)^\top$: collinear to $v_- = (1, -2)^\top$ iff $-2 = 1$ in $\mathbb{Z}/p\mathbb{Z}$, i.e. $p = 3$.

Thus:

- $p \geq 5$: no common eigenvector; Δ is irreducible (and indecomposable).
- $p = 3$: v_- spans the unique degree-1 subrepresentation, so Δ is reducible. Since there is only one such subrepresentation, Δ cannot split as a sum of two degree-1 pieces and is indecomposable.
- $p = 2$: Δ is irreducible (and indecomposable).

Isomorphism $\text{Perm} \simeq \mathbf{1} \oplus \Delta$.

The map f from Section A.1 is a morphism of representations over any field (the equivariance checks are purely algebraic). It is an isomorphism iff $\det f = 9 \neq 0$ in K , i.e. $p \neq 3$.

For $p = 3$: Perm is indecomposable, so $\text{Perm} \not\simeq \mathbf{1} \oplus \Delta$. To see this, let M denote the permutation matrix of (123). Its characteristic polynomial is $x^3 - 1 = (x - 1)^3$ over \mathbb{F}_3 , so 1 is the only eigenvalue and the eigenspace is the line $L = \text{span}\{(1, 1, 1)^\top\}$ (one checks $\dim \text{Ker}(M - I) = 1$). Any degree-2 subrepresentation P complementary to L would be a (123)-stable hyperplane. Dually, $P = \text{Ker } \phi$ for some linear functional ϕ with $\phi \circ M = \phi$, i.e. ϕ is an eigenvector of M^\top for eigenvalue 1. The same eigenvalue analysis applied to M^\top gives $\phi \in \text{span}\{(1, 1, 1)\}$, so $P = \{x + y + z = 0\}$. But $1 + 1 + 1 = 0$ in $\mathbb{Z}/3\mathbb{Z}$, so $(1, 1, 1)^\top \in P$, giving $L \subset P$ and contradicting $L \cap P = \{0\}$.

A.2 Chapter 2

Solution to Exercise 2.21.

1. We must show that the formula $(\lambda, m + N) \mapsto (\lambda m) + N$ is independent of the representative of $m + N$. If $m + N = m' + N$, then $m' = m + n$ for some $n \in N$, so $\lambda m' = \lambda(m + n) = \lambda m + \lambda n$. Since N is a submodule, $\lambda n \in N$, so $(\lambda m') + N = (\lambda m) + N$. The module axioms for M/N follow immediately from those of M (they are equalities in M , hence also in M/N).
2. Let $f: M \rightarrow M'$ be a morphism. Then $\text{Ker } f$ is a submodule of M , so the quotient module $M/\text{Ker } f$ is defined by the previous part. Define

$$f': M/\text{Ker } f \longrightarrow \text{Im } f, \quad m + \text{Ker } f \longmapsto f(m).$$

This is well-defined: $f(m) \in \text{Im } f$ by definition, and if $m + \text{Ker } f = m' + \text{Ker } f$ then $m' = m + k$ for some $k \in \text{Ker } f$, so $f(m') = f(m) + f(k) = f(m)$. It is a morphism (since f is) and surjective (by definition of $\text{Im } f$). It is injective: if $f'(m + \text{Ker } f) = f(m) = 0$ then $m \in \text{Ker } f$, so $m + \text{Ker } f = 0$ in $M/\text{Ker } f$. Hence f' is an isomorphism.

Solution to Exercise 2.22.

1. Let $m \in M_{i-1}$. Since the sequence is exact, $f_i(m) \in \text{Im } f_i = \text{Ker } f_{i+1}$, so $f_{i+1}(f_i(m)) = 0$.
2. The sequence $0 \xrightarrow{0} N \xrightarrow{f} M$ is exact if and only if $\text{Im}(0) = \text{Ker } f$; but $\text{Im}(0) = \{0\}$, so this holds if and only if f is injective. Similarly, $M \xrightarrow{g} Q \xrightarrow{0} 0$ is exact if and only if $\text{Im } g = \text{Ker}(0) = Q$, i.e. g is surjective.
3. Take $Q = M/N$ and $g: M \rightarrow M/N$ the projection. Then f (the inclusion) is injective, so $\text{Ker } f = \{0\} = \text{Im}(0)$; g is surjective by construction, so $\text{Im } g = Q = \text{Ker}(0)$; and $\text{Im } f = N = \text{Ker } g$ by definition of the quotient projection.
4. Take $R = \mathbb{Z}$, $M = \mathbb{Z}/4\mathbb{Z}$, $N = 2\mathbb{Z}/4\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z}$. By Section A.2, $M/N \simeq \mathbb{Z}/2\mathbb{Z}$, so the sequence $0 \rightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow \mathbb{Z}/4\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow 0$ is short exact. However, $\mathbb{Z}/4\mathbb{Z} \not\cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ as \mathbb{Z} -modules: the former has an element of order 4, while the latter does not.
5. Assume $M = \text{Im } f \oplus M'$ for some submodule $M' \subset M$. The restriction $g|_{M'}: M' \rightarrow Q$ is a morphism. Its kernel is $M' \cap \text{Ker } g = M' \cap \text{Im } f = \{0\}$ (the sum is direct and g is exact). It is surjective: for any $q \in Q$ pick $m \in M$ with $g(m) = q$ (possible since g is surjective), write $m = i + m'$ with $i \in \text{Im } f$ and $m' \in M'$; then $g(m') = g(m) - g(i) = q - 0 = q$ since $\text{Im } f \subseteq \text{Ker } g$. So $g|_{M'}: M' \xrightarrow{\sim} Q$ is an isomorphism; its inverse $g': Q \rightarrow M' \subset M$ satisfies $g \circ g' = \text{id}_Q$, giving right-splitting.
For left-splitting: since f is injective it restricts to an isomorphism $f: N \xrightarrow{\sim} \text{Im } f$. Let $\pi: M \rightarrow \text{Im } f$ be the projection onto $\text{Im } f$ along M' (i.e. $\pi(i + m') = i$ for $i \in \text{Im } f$, $m' \in M'$). Then $f' = f^{-1} \circ \pi: M \rightarrow N$ is a morphism satisfying $f' \circ f = \text{id}_N$.
6. Given $f': M \rightarrow N$ with $f' \circ f = \text{id}_N$. Let $T = f \circ f': M \rightarrow M$. Then $T^2 = f \circ f' \circ f \circ f' = f \circ \text{id}_N \circ f' = T$, so T is a projector and $M = \text{Im } T \oplus \text{Ker } T$. We show $\text{Im } T = \text{Im } f$: the inclusion $\text{Im } T \subseteq \text{Im } f$ is clear. Conversely, if $i = f(n) \in \text{Im } f$ then $T(f(n)) = f(f'(f(n))) = f(n) = i$, so $i \in \text{Im } T$. Thus $\text{Ker } T$ is a supplement of $\text{Im } f$.
7. Given $g': Q \rightarrow M$ with $g \circ g' = \text{id}_Q$. Let $U = g' \circ g: M \rightarrow M$. From $g \circ g' = \text{id}_Q$ we get $U^2 = g' \circ g \circ g' \circ g = g' \circ \text{id}_Q \circ g = U$, so $M = \text{Im } U \oplus \text{Ker } U$. We show $\text{Ker } U = \text{Im } f$: if $m \in \text{Im } f$ then $m \in \text{Ker } g$ by exactness (part 1), so $U(m) = g'(g(m)) = g'(0) = 0$, giving $\text{Im } f \subseteq \text{Ker } U$. Conversely, if $U(m) = g'(g(m)) = 0$ and g' is injective (it has left inverse g), then $g(m) = 0$, so $m \in \text{Ker } g = \text{Im } f$ by exactness. Thus $\text{Im } U$ is a supplement of $\text{Im } f = \text{Ker } U$.

Solution to Exercise 2.23.

Throughout we use: a module is semi-simple if and only if every submodule admits a supplement.

1. Let M be semi-simple and $N \subseteq M$ a submodule. Let $P \subseteq N$ be a submodule; since $P \subseteq M$ and M is semi-simple, there exists $S \subseteq M$ with $M = P \oplus S$. Set $S' = S \cap N$; this is a submodule of N . For any $n \in N \subseteq M$ write $n = p + s$ uniquely with $p \in P$ and $s \in S$. Since $P \subseteq N$, we have $s = n - p \in N$, so $s \in S \cap N = S'$. Hence $N = P \oplus S'$, showing N is semi-simple.
2. Since M is semi-simple, the submodule $\text{Ker } f \subseteq M$ admits a supplement M' , so $M = \text{Ker } f \oplus M'$. The restriction $f|_{M'}: M' \rightarrow \text{Im } f$ is an isomorphism (injective since $\text{Ker}(f|_{M'}) = M' \cap \text{Ker } f = \{0\}$; surjective by definition of $\text{Im } f$). Thus $\text{Im } f \simeq M'$, which is semi-simple by part 1.

3. View V and W as $K[G]$ -modules; they are Artinian since a strictly descending chain of submodules would be a strictly descending chain of K -subspaces, which cannot be infinite. The morphism f is a $K[G]$ -module morphism. Since V is semi-simple, $\text{Ker } f$ (a submodule of V) is semi-simple by part 1, and $\text{Im } f$ (a submodule of W , isomorphic to $V/\text{Ker } f$) is semi-simple by part 2.

Solution to Exercise 2.24.

1. For all $h \in G$,

$$e_h \Sigma = e_h \sum_{g \in G} e_g = \sum_{g \in G} e_{hg} = \sum_{g \in G} e_g = \Sigma,$$

since $g \mapsto hg$ is a bijection $G \rightarrow G$.

2. For any $\sum_{g \in G} \lambda_g e_g \in K[G]$ we compute

$$\left(\sum_{g \in G} \lambda_g e_g \right) \Sigma = \sum_{g \in G} \lambda_g (e_g \Sigma) = \sum_{g \in G} \lambda_g \Sigma = \left(\sum_{g \in G} \lambda_g \right) \Sigma \in S.$$

Since S is also an additive subgroup of $K[G]$, it is a sub- $K[G]$ -module.

3. S has K -dimension 1 and the action of any e_h on Σ is the identity (by part 1), so G acts trivially on S . Hence S is the trivial representation $\mathbf{1}$.
4. Using part 1 applied to each e_g :

$$\Sigma^2 = \left(\sum_{g \in G} e_g \right) \Sigma = \sum_{g \in G} (e_g \Sigma) = \sum_{g \in G} \Sigma = n \Sigma.$$

Since $n = 0$ in K , we get $\Sigma^2 = 0$.

5. In any ring, $(1 - x)(1 + x) = 1 - x^2$. Applying this with $x = \lambda \Sigma$:

$$(1 - \lambda \Sigma)(1 + \lambda \Sigma) = 1 - \lambda^2 \Sigma^2 = 1 - 0 = 1,$$

and similarly $(1 + \lambda \Sigma)(1 - \lambda \Sigma) = 1$. So $1 - \lambda \Sigma$ is invertible with inverse $1 + \lambda \Sigma$.

6. Suppose for contradiction that $K[G]$ is semi-simple (as a $K[G]$ -module). Since $K[G]$ is finite-dimensional over K , it is Artinian, so the submodule S admits a supplement: $K[G] = S \oplus T$ for some submodule T . Write $1 = m + t$ uniquely with $m = \lambda \Sigma \in S$ and $t = 1 - \lambda \Sigma \in T$. By part 5, t is invertible, so there exists $u \in K[G]$ with $ut = 1$. Then $\Sigma = \Sigma \cdot 1 = \Sigma(ut) = (\Sigma u)t$. Since T is a submodule and $t \in T$, we have $(\Sigma u)t \in T$, so $\Sigma \in T$. But $\Sigma = 1 \cdot \Sigma \in S$, contradicting $S \cap T = \{0\}$ (as $\Sigma \neq 0$).

A.3 Chapter 3

Solution to Exercise 3.42.

1. We compute

$$(\chi_\pi | \mathbf{1}) = \frac{1}{\#G} \sum_{g \in G} \chi_\pi(g) \cdot 1 = \frac{1}{\#G} \sum_{g \in G} \# \text{Fix } g > 0,$$

so π contains at least one copy of $\mathbf{1}$. By Maschke's theorem there exists a complementary subrepresentation ρ with $\pi \simeq \mathbf{1} \oplus \rho$.

Remark A.4. Concretely, since G permutes the elements of X , the vector $\sum_{x \in X} e_x \in \mathbb{C}[X]$ is fixed by every $g \in G$ and spans a copy of $\mathbf{1}$ inside π .

2. Write $\chi_\rho = \chi_\pi - \mathbf{1}$. Since $\mathbf{1}$ is irreducible,

$$(\chi_\rho | \mathbf{1}) = (\chi_\pi | \mathbf{1}) - (\mathbf{1} | \mathbf{1}) = -1 + \frac{1}{\#G} \sum_{g \in G} \# \text{Fix } g,$$

which equals one less than the number of orbits (by the orbit-counting formula). Hence $(\chi_\rho | \mathbf{1}) = 0$ if and only if there is exactly one orbit, i.e. the action is transitive.

3. We have ρ irreducible iff $(\chi_\rho | \chi_\rho) = 1$. By sesquilinearity, using transitivity (so $(\chi_\pi | \mathbf{1}) = 1$):

$$(\chi_\rho | \chi_\rho) = (\chi_\pi - \mathbf{1} | \chi_\pi - \mathbf{1}) = (\chi_\pi | \chi_\pi) - 2(\chi_\pi | \mathbf{1}) + 1 = -1 + \frac{1}{\#G} \sum_{g \in G} (\# \text{Fix } g)^2.$$

Consider the diagonal action of G on $X \times X$ by $g \cdot (x, y) = (g \cdot x, g \cdot y)$. An element g fixes (x, y) iff it fixes both x and y , so $\# \text{Fix}_{X \times X} g = (\# \text{Fix}_X g)^2$. By the orbit-counting formula, $(\chi_\rho | \chi_\rho)$ equals the number of orbits of G on $X \times X$ minus 1.

The diagonal $\Delta = \{(x, x) | x \in X\}$ is G -stable and, since G acts transitively on X , forms a single orbit. Its complement $X \times X \setminus \Delta$ consists of pairs (x, y) with $x \neq y$. The action of G on $X \times X \setminus \Delta$ is transitive if and only if the original action is doubly transitive. Therefore: if G acts doubly transitively on X , there are exactly two orbits on $X \times X$, giving $(\chi_\rho | \chi_\rho) = 1$ and ρ irreducible; conversely, if not doubly transitive, there are more than two orbits and ρ is not irreducible.

Remark A.5. This shows in particular that for $n \geq 2$ the symmetric group S_n has an irreducible character of degree $n - 1$: the complement of $\mathbf{1}$ in the permutation representation of S_n on $\{1, \dots, n\}$ is irreducible, since S_n acts doubly transitively on $\{1, \dots, n\}$.

Solution to Exercise 3.43.

1. The map T_f is the action of the element $\sum_{g \in G} f(g) e_g \in \mathbb{C}[G]$ on the $\mathbb{C}[G]$ -module V . Since f is a class function, this element lies in the centre of $\mathbb{C}[G]$, so T_f commutes with every $\rho(h)$ ($h \in G$), i.e. $T_f \in \text{End}_G(V)$. Since V is irreducible, Schur's lemma (Corollary 3.3) gives $\text{End}_G(V) = \{\lambda \text{ id}_V | \lambda \in \mathbb{C}\}$, so $T_f = \lambda \text{ id}_V$ for some $\lambda \in \mathbb{C}$.
2. Taking traces on both sides: $\text{tr } T_f = \lambda \dim V = \lambda \deg \rho$. On the other hand, by linearity of the trace,

$$\text{tr } T_f = \sum_{g \in G} f(g) \text{tr } \rho(g) = \sum_{g \in G} f(g) \chi(g) = \#G (f | \bar{\chi}),$$

where $\bar{\chi}(g) = \overline{\chi(g)}$ is the pointwise complex conjugate (the character of the contragredient of ρ), and we used the definition $(f | \bar{\chi}) = \frac{1}{\#G} \sum_{g \in G} f(g) \overline{\chi(g)} = \frac{1}{\#G} \sum_{g \in G} f(g) \chi(g)$. Therefore

$$\lambda = \frac{\#G}{\deg \rho} (f | \bar{\chi}).$$

Solution to Exercise 3.44.

1. By Corollary 3.24, $\chi(g^{-1}) = \overline{\chi(g)}$ for every character χ and every $g \in G$.

(\Leftarrow) Suppose every $g \in G$ is conjugate to g^{-1} . Since χ is a class function,

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

so $\chi(g) \in \mathbb{R}$ for all g .

(\Rightarrow) Suppose every character of G is real-valued, and let $g \in G$. Since all characters are real, $\chi(g^{-1}) = \overline{\chi(g)} = \chi(g)$ for all $\chi \in \text{Irr}(G)$. Therefore

$$\sum_{\chi \in \text{Irr}(G)} \overline{\chi(g)} \chi(g^{-1}) = \sum_{\chi \in \text{Irr}(G)} \chi(g)^2 \geq 1^2 = 1 > 0,$$

where the last inequality uses the trivial character. By Theorem 4.28, the left-hand side equals $\#G/\#C_g$ if g and g^{-1} lie in the same conjugacy class C_g , and 0 otherwise. Since the sum is positive, g must be conjugate to g^{-1} .

2. For any $g \in S_n$, the permutation g^{-1} has the same cycle decomposition shape as g (with the order inside each cycle reversed), so g and g^{-1} are conjugate in S_n . By part 1, every character of S_n is real-valued.

For A_4 : by Section A.4(2), the elements (123) and $(132) = (123)^{-1}$ are not conjugate in A_4 . By part 1, A_4 therefore has characters that are not real-valued (namely ϕ and $\bar{\phi}$ from the character table of A_4).

A.4 Chapter 4

Solution to Exercise 4.38.

1. The identity 1_G is conjugate only to itself, so it lies in the unique conjugacy class of size 1. Since C_1 is the only class of size 1, we have $1_G \in C_1$.

2. The degree of a character equals its value at 1_G (the trace of the identity matrix). Hence $\deg \phi = \phi(1_G) = 6$ and $\deg \psi = \psi(1_G) = 21$.

3. Since conjugacy classes partition G :

$$\#G = 1 + 15 + 40 + 90 + 45 + 120 + 144 + 120 + 90 + 15 + 40 = 720.$$

4. We compute

$$(\phi | \phi) = \frac{1}{720} \sum_{j=1}^{11} \#C_j |\phi(C_j)|^2 = \frac{1}{720} (1 \cdot 36 + 15 \cdot 4 + 0 + 0 + 45 \cdot 4 + 120 \cdot 4 + 144 \cdot 1 + 120 \cdot 1 + 0 + 15 \cdot 4 + 40 \cdot 9) = 2.$$

Since $(\phi | \phi) \neq 1$, the representation is not irreducible. Writing $\phi \simeq \bigoplus_{i=1}^k \rho_i^{\oplus n_i}$ with the ρ_i irreducible and pairwise non-isomorphic, we get $\sum n_i^2 = 2$, so $k = 2$ and $n_1 = n_2 = 1$: ϕ is the direct sum of two non-isomorphic irreducible representations.

To identify them, observe that the trivial character $\mathbf{1}$ is an irreducible character of G , and

$$(\phi | \mathbf{1}) = \frac{1}{720} \sum_{j=1}^{11} \#C_j \phi(C_j) \cdot 1 = \frac{1}{720} (6 + 30 + 0 + 0 + 90 + 240 + 144 + 120 + 0 - 30 + 120) = 1.$$

So one of the two irreducible summands is $\mathbf{1}$. The other, call it ξ , has degree $\deg \phi - \deg \mathbf{1} = 6 - 1 = 5$, and $\xi = \phi - \mathbf{1}$ (as class functions).

5. We first show ψ is not irreducible: a similar computation gives $(\psi | \psi) = 2$, so ψ also decomposes as the direct sum of two non-isomorphic irreducibles. Computing $(\psi | \xi) = 1$ shows that one of those irreducibles is ρ_ξ ; the other is ρ_η where $\eta = \psi - \xi = \psi - \phi + \mathbf{1}$ is an irreducible character of degree $\deg \psi - \deg \xi = 21 - 5 = 16$.

The values of $\eta = \psi - \phi + \mathbf{1}$ are:

	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8	C_9	C_{10}	C_{11}
η	16	0	-2	0	0	0	1	0	0	0	-2

By Theorem 4.24, the projector onto the isotypic component of ρ_η is

$$\begin{aligned} \frac{\deg \eta}{\#G} \sum_{g \in G} \overline{\eta(g)} e_g &= \frac{16}{720} \left(16 \sum_{g \in C_1} e_g - 2 \sum_{g \in C_3} e_g + \sum_{g \in C_7} e_g - 2 \sum_{g \in C_{11}} e_g \right) \\ &= \frac{16}{45} e_{1_G} - \frac{2}{45} \sum_{g \in C_3} e_g + \frac{1}{45} \sum_{g \in C_7} e_g - \frac{2}{45} \sum_{g \in C_{11}} e_g. \end{aligned}$$

6. Since $\xi = \phi - \mathbf{1}$ is real-valued, the character of the representation $\text{Hom}(\rho_\xi, \rho_\xi)$ is $\xi \bar{\xi} = \xi^2$ (see Section 3.8). This character has degree $\xi^2(1_G) = \xi(1_G)^2 = 5^2 = 25$. Decomposing $\rho_{\xi^2} \simeq \bigoplus_{i=1}^k \rho_i^{\oplus n_i}$ with the ρ_i irreducible and pairwise non-isomorphic gives $\sum_{i=1}^k n_i^2 = (\xi^2 | \xi^2) = 4$. The only solutions in positive integers are: $(k, n_1) = (1, 2)$, or $k = 4$ with all $n_i = 1$. The first is impossible since it would require $25 = \deg \rho_{\xi^2} = 2 \deg \rho_1$, but 25 is odd. Hence $k = 4$ and $n_i = 1$ for all i : ρ_{ξ^2} is a degree-25 representation that decomposes as the direct sum of 4 pairwise non-isomorphic irreducible representations.

Solution to Exercise 4.39.

We use $\# \text{Irr}(G) = \#\{\text{conjugacy classes}\}$ and $\sum_{\chi \in \text{Irr}(G)} (\deg \chi)^2 = \#G = 8$.

Since G is non-abelian, at least one $\chi \in \text{Irr}(G)$ satisfies $\deg \chi \geq 2$; since $3^2 = 9 > 8$, this degree is exactly 2. The trivial character contributes a term $1^2 = 1$. Removing these two terms leaves $8 - 1 - 4 = 3$ to be expressed as a sum of squares; since $2^2 > 3$, the only possibility is $3 = 1^2 + 1^2 + 1^2$. Hence the unique solution is $8 = 1^2 + 1^2 + 1^2 + 1^2 + 2^2$, with five summands, so $\# \text{Irr}(G) = 5$ and G has exactly 5 conjugacy classes.

For the abelianisation: since G^{ab} is abelian, every irreducible representation of G^{ab} has degree 1, so $\#G^{\text{ab}} = \# \text{Irr}(G^{\text{ab}})$. The degree-1 irreducible representations of G^{ab} pull back (via $G \rightarrow G^{\text{ab}}$) to give exactly all degree-1 irreducible representations of G , of which there are 4 by the above. Hence $\#G^{\text{ab}} = 4$.

Solution to Exercise 4.40.

1. By the conjugacy principle, conjugation in S_n preserves cycle decomposition type, so V_4 is a union of conjugacy classes of S_4 , hence normal in S_4 and *a fortiori* in A_4 . The quotient A_4/V_4 has order $\#A_4/\#V_4 = 12/4 = 3$, which is prime, so A_4/V_4 is cyclic.
2. For $\sigma(123)\sigma^{-1} = (132)$ we need $(\sigma(1) \sigma(2) \sigma(3)) = (132)$, i.e. (up to cyclic rotation of the target) σ must map $\{1, 2, 3\}$ to itself with $1 \mapsto 1, 2 \mapsto 3, 3 \mapsto 2$ (or a cyclic shift thereof). In all cases this forces σ to restrict to a transposition on $\{1, 2, 3\}$, which is an odd permutation. In particular $\sigma \notin A_4$, so (123) and (132) are not conjugate in A_4 .

3. By part (2) and the conjugacy principle (restricting to even permutations), the conjugacy classes of A_4 are:

$$\{\text{Id}\}, \quad \{(12)(34), (13)(24), (14)(23)\}, \quad \{(123), (142), (134), (243)\}, \quad \{(132), (124), (143), (234)\}.$$

That is 4 classes, so there are 4 irreducible representations. Their degrees $n_1 \leq \dots \leq n_4$ satisfy $n_1 = 1, n_4 \geq 2$ (since A_4 is non-abelian), and $\sum n_i^2 = 12$; the only solution is $n_1 = n_2 = n_3 = 1, n_4 = 3$.

Pulling back the irreducible characters of $A_4/V_4 \cong C_3$ via the quotient gives three degree-1 characters $\mathbf{1}, \phi, \bar{\phi}$ (where $\phi((123)) = \omega$ and $\bar{\phi}((123)) = \bar{\omega}$). The remaining irreducible ρ of degree 3 is found by noting that the permutation representation of A_4 on $\{1, 2, 3, 4\}$ decomposes as $\mathbf{1} \oplus \rho$ (the action is doubly transitive, hence ρ is irreducible by Exercise 3.42). Since $\chi_{\text{Perm}}(g) = \#\text{Fix } g$, we compute $\rho = \chi_{\text{Perm}} - \mathbf{1}$:

	Id	(12)(34)	(123)	(132)
#	1	3	4	4
$\mathbf{1}$	1	1	1	1
ϕ	1	1	ω	$\bar{\omega}$
$\bar{\phi}$	1	1	$\bar{\omega}$	ω
ρ	3	-1	0	0

One can verify each row has inner product 1 with itself.

4. From part (1), $A_4/V_4 \cong C_3$ is abelian, so $D(A_4) \subseteq V_4$. The character table exhibits three degree-1 characters; since these correspond bijectively to the irreducible characters of the abelianisation A_4^{ab} , and A_4^{ab} is abelian with $\#A_4^{\text{ab}} = \#\text{Irr}(A_4^{\text{ab}})$, we get $\#A_4^{\text{ab}} = 3$, so $|D(A_4)| = 12/3 = 4 = |V_4|$. Combined with $D(A_4) \subseteq V_4$, this gives $D(A_4) = V_4$.
5. Recall from Section 4.7 the character table of S_4 (with classes Id, (12), (123), (1234), (12)(34)). Restricting to A_4 , note that elements of A_4 are even, so (12)(34) maps to the S_4 -class (12)(34), while (123) and (132) (both 3-cycles) map to the same S_4 -class (123):

	Id	(12)(34)	(123)	(132)
$\mathbf{1}_{S_4} _{A_4}$	1	1	1	1
$\varepsilon _{A_4}$	1	1	1	1
$\psi _{A_4}$	2	2	-1	-1
$\chi _{A_4}$	3	-1	0	0
$\chi\varepsilon _{A_4}$	3	-1	0	0

By inner products: $\mathbf{1}_{S_4}|_{A_4} \cong \mathbf{1}$ and $\varepsilon|_{A_4} \cong \mathbf{1}$ (the sign becomes trivial on even permutations). Using $\omega + \bar{\omega} = -1$, one computes $(\psi|_{A_4} | \phi) = 1$ and $(\psi|_{A_4} | \bar{\phi}) = 1$, so $\psi|_{A_4} \cong \phi \oplus \bar{\phi}$. Finally $\chi|_{A_4} \cong \rho$ and $\chi\varepsilon|_{A_4} \cong \rho$.

6. A double transposition (e.g. (12)(34)) permutes the vertices by swapping two pairs; geometrically this corresponds to a 180° rotation of the tetrahedron about the axis joining midpoints of two opposite edges. In a suitable basis this rotation has matrix $\text{diag}(1, -1, -1)$, with trace -1 . A 3-cycle corresponds to a 120° rotation about the axis through a vertex and the midpoint of the opposite face, with matrix of trace $1 + 2\cos(120^\circ) = 0$. Hence the character of the tetrahedron representation is $(3, -1, 0, 0) = \rho$, so this representation is isomorphic to ρ .

Alternatively, the tetrahedron representation is faithful. If it contained no copy of ρ , it would be a sum of one-dimensional characters of A_4 , each of which factors through the abelianisation $A_4/V_4 \cong C_3$; the kernel would then contain $V_4 \neq \{\text{Id}\}$, contradicting faithfulness. So ρ is a summand, and by degrees the representation equals ρ .

Solution to Exercise 4.41.

1. Since G is abelian, every irreducible representation has degree 1 (Corollary 4.23), so χ is a group homomorphism $G \rightarrow \mathbb{C}^\times$. For all $g \in G$, $g^2 = 1_G$, so $\chi(g)^2 = \chi(g^2) = \chi(1_G) = 1$, giving $\chi(g) \in \{+1, -1\}$.
2. Writing $C_2 = \{1, h\}$, the four irreducible characters of $G = C_2 \times C_2$ are obtained from the projections and the diagonal:

	$(1, 1)$	$(h, 1)$	$(1, h)$	(h, h)
$\mathbf{1}$	1	1	1	1
χ_L	1	-1	1	-1
χ_R	1	1	-1	-1
χ_D	1	-1	-1	1

where χ_L (resp. χ_R) inflates the sign of the left (resp. right) C_2 -factor, and χ_D inflates from the diagonal quotient.

3. No. From the table: $\text{Ker } \mathbf{1} = G$, $\text{Ker } \chi_L = \{1\} \times C_2$, $\text{Ker } \chi_R = C_2 \times \{1\}$, $\text{Ker } \chi_D = \{(x, x) \mid x \in C_2\}$. Every irreducible representation has non-trivial kernel.
4. Yes. The representation $\chi_L \oplus \chi_R$ has degree 2 and kernel $\text{Ker } \chi_L \cap \text{Ker } \chi_R = (\{1\} \times C_2) \cap (C_2 \times \{1\}) = \{(1, 1)\}$, so it is faithful. Since no degree-1 representation is faithful (part 3), the minimum degree of a faithful representation is 2.

Solution to Exercise 4.42.

1. By Exercise 4.39, $|D(G)| = 2$, so $D(G) = \{\text{Id}, x\}$ for some $x \neq \text{Id}$. Since reflections conjugate rotations to their inverses, $\tau\rho\tau^{-1} = \rho^{-1}$, so the commutator $\tau\rho\tau^{-1}\rho^{-1} = \rho^{-2} = \rho^2 \neq \text{Id}$. Hence $\rho^2 \in D(G)$, giving $D(G) = \{\text{Id}, \rho^2\}$.

The quotient $G/D(G)$ is abelian of order 4. Every element of $G/D(G)$ has order at most 2: the rotations ρ and ρ^{-1} satisfy $\rho^2 \in D(G)$, so they have order 2 in the quotient. Hence $G/D(G) \cong C_2 \times C_2$.

2. The conjugacy classes of D_8 are $\{\text{Id}\}$, $\{\rho^2\}$, $\{\rho, \rho^{-1}\}$, $\{\sigma, \sigma'\}$, $\{\tau, \tau'\}$ (proved in the lectures). By part (1) and Exercise 4.41, the four degree-1 characters are inflated from $G/D(G) \cong C_2 \times C_2$. The fifth irreducible character of degree 2 is found from the regular representation (character 8, 0, 0, 0, 0) via $\mathbf{1} + \phi + \psi + \phi\psi + 2\chi = 8, 0, 0, 0, 0$:

	Id	ρ^2	ρ	σ	τ
#	1	1	2	2	2
$\mathbf{1}$	1	1	1	1	1
ϕ	1	1	1	-1	-1
ψ	1	1	-1	1	-1
$\phi\psi$	1	1	-1	-1	1
χ	2	-2	0	0	0

Solution to Exercise 4.43.

1. It suffices to check that each of $-I, -J, -K$ is conjugate to I, J, K respectively. Indeed, $JIJ^{-1} = JI(-J) = (-K)(-J) = KJ = -I$, and similarly for J and K . Since we know there are exactly 5 conjugacy classes (by Exercise 4.39), and the five listed sets are disjoint with total size $\#Q_8 = 8$, they are exactly the conjugacy classes.
2. The centre consists of elements forming singleton conjugacy classes: $Z(Q_8) = \{1, -1\}$.
3. $Q_8/Z(Q_8) = \{\pm 1, \pm I, \pm J, \pm K\}$ is abelian (explicit check or: it is a quotient of order 4 of Q_8 by a central subgroup). Every nontrivial element $(\pm I)^2 = (\pm J)^2 = (\pm K)^2 = -1 = 1$ in Q_8/Z has order 2. Hence $Q_8/Z \cong C_2 \times C_2$.
4. We inflate the four degree-1 characters of $Q_8/Z \cong C_2 \times C_2$ (cf. Exercise 4.41) to Q_8 . The missing degree-2 character χ is recovered from the regular representation (as in Exercise 4.42):

	1	-1	$\pm I$	$\pm J$	$\pm K$
#	1	1	2	2	2
1	1	1	1	1	1
ϕ	1	1	1	-1	-1
ψ	1	1	-1	1	-1
$\phi\psi$	1	1	-1	-1	1
χ	2	-2	0	0	0

This is identical to the character table of D_8 (Exercise 4.42). Yet $D_8 \not\cong Q_8$: for example, D_8 has five elements of order 2 whereas Q_8 has only one (namely -1). This shows that two non-isomorphic groups can share the same character table.

5. The assignment $I \mapsto \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $J \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $K \mapsto \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ is by definition a faithful degree-2 representation of Q_8 . Computing traces: at 1 the trace is $2 = \chi(1)$; at -1 the trace is $-2 = \chi(-1)$; at $\pm I$ the trace is $i + (-i) = 0 = \chi(\pm I)$; at $\pm J$ and $\pm K$ similarly 0. Hence this representation has character χ , so it is the unique irreducible representation of Q_8 of degree 2.

A.5 Chapter 5

Solution to Exercise 5.23.

We write $n = 2m + 1$, $G = D_{2n}$, $H = \langle \rho \rangle$.

1. Since H is abelian, conjugation within H fixes every element; conjugation by τ maps $\rho^x \mapsto \rho^{-x}$, and these are all conjugations (since $G = H \cup \tau H$). Thus the G -conjugacy class of ρ^x is $\{\rho^x, \rho^{-x}\}$. For $0 < x < n$ this has size 2 unless $\rho^x = \rho^{-x}$, i.e. $n \mid 2x$; since n is odd, this forces $x = 0$. The rotation classes are therefore $\{\text{Id}\}$ and $\{\rho^k, \rho^{-k}\}$ for $k = 1, \dots, m$. By the conjugacy principle, all n axial symmetries form a single conjugacy class (any rotation carries one axis to another).
2. Inflating the trivial and sign characters of $G/H \cong \mathbb{Z}/2\mathbb{Z}$ to G :

	Id	ρ^x ($1 \leq x \leq m$)	τ
#	1	2	n
1	1	1	1
ε	1	1	-1.

Both are irreducible since they have degree 1.

3. (a) For $g = \text{Id}$: $\psi_y(\text{Id}) = [G : H] \deg \chi_y = 2$.

For a nontrivial rotation ρ^x : since H is abelian every H -conjugacy class is a singleton, and $cc_G(\rho^x) \cap H = \{\rho^x, \rho^{-x}\}$, so the induction formula gives

$$\psi_y(\rho^x) = \frac{[G:H]}{\#cc_G(\rho^x)} (\chi_y(\rho^x) + \chi_y(\rho^{-x})) = e^{2\pi ixy/n} + e^{-2\pi ixy/n} = 2 \cos\left(\frac{2\pi xy}{n}\right).$$

For any axial symmetry g : $cc_G(g)$ consists entirely of symmetries, so $cc_G(g) \cap H = \emptyset$ and $\psi_y(g) = 0$.

- (b) From (a), $\psi_y(\rho^x) = \chi_y(\rho^x) + \chi_{-y}(\rho^x)$ for all $x \in \mathbb{Z}/n\mathbb{Z}$, so

$$\text{Res}_H^G \psi_y = \chi_y + \chi_{-y}.$$

- (c) By Frobenius reciprocity and part (b),

$$(\psi_y | \psi_y)_G = (\text{Ind}_H^G \chi_y | \psi_y)_G = (\chi_y | \text{Res}_H^G \psi_y)_H = 1 + (\chi_y | \chi_{-y})_H.$$

Since the χ_y are pairwise distinct irreducible characters of H , $(\chi_y | \chi_{-y})_H = 1$ iff $y \equiv -y \pmod{n}$, i.e. $n \mid 2y$. As $n = 2m + 1$ is odd, the only solution in $\{-m, \dots, m\}$ is $y = 0$. Therefore ψ_y is irreducible for all $y \neq 0$ (while $\psi_0 = \mathbf{1} + \varepsilon$).

4. By part (1) there are $m + 2$ conjugacy classes. Parts (2) and (3c) yield $2 + m$ irreducible characters: $\mathbf{1}$, ε , and ψ_1, \dots, ψ_m (these are pairwise distinct since $\text{Res}_H^G \psi_y = \chi_y + \chi_{-y}$ for $y = 1, \dots, m$ are pairwise distinct, and $\psi_y = \psi_{-y}$). The character table of D_{2n} ($n = 2m + 1$ odd) is:

	Id	ρ^x ($1 \leq x \leq m$)	τ
#	1	2	n
$\mathbf{1}$	1	1	1
ε	1	1	-1
ψ_y ($1 \leq y \leq m$)	2	$2 \cos \frac{2\pi xy}{n}$	0

5. Only Id forms a singleton conjugacy class, so $Z(G) = \{\text{Id}\}$.

The derived subgroup satisfies $D(G) = \bigcap_{\deg \phi=1} \text{Ker } \phi = \text{Ker } \mathbf{1} \cap \text{Ker } \varepsilon = \text{Ker } \varepsilon = H$.

Solution to Exercise 5.24.

Let $n = 2m$, $G = D_{2n}$, $H = \langle \rho \rangle \cong \mathbb{Z}/n\mathbb{Z}$, with σ and τ representatives of the two conjugacy classes of axial symmetries.

Conjugacy classes. The same argument as in Section A.5 shows the G -class of ρ^x is $\{\rho^x, \rho^{-x}\}$. Since $n = 2m$ is even, $n \mid 2x$ holds for $x = 0$ and also for $x = m$: indeed $\rho^m = -\text{Id}$ is central. This gives two singleton rotation classes $\{\text{Id}\}$ and $\{-\text{Id}\}$, and $m - 1$ classes $\{\rho^k, \rho^{-k}\}$ for $k = 1, \dots, m - 1$ of size 2. The axial symmetries split into two conjugacy classes of size m (vertex-to-vertex and edge-to-edge axes). In total: $m + 3$ conjugacy classes.

Degree-1 characters. Let $K = \langle \rho^2 \rangle \cong \mathbb{Z}/m\mathbb{Z}$; since $\tau \rho^2 \tau^{-1} = \rho^{-2} \in K$, the subgroup K is normal in G with $[G : K] = 4$. Every element of G/K squares to the identity, so $G/K \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ by Exercise 4.41. The four degree-1 characters of G/K inflate to:

	Id	ρ^x ($1 \leq x \leq m-1$)	$-\text{Id}$	σ	τ
$\mathbf{1}$	1	1	1	1	1
ξ	1	$(-1)^x$	$(-1)^m$	-1	1
η	1	$(-1)^x$	$(-1)^m$	1	-1
$\xi\eta$	1	1	1	-1	-1

Degree-2 characters. For $\psi_y = \text{Ind}_H^G \chi_y$, the same computation as in Section A.5 gives $\psi_y(\rho^x) = 2 \cos(2\pi xy/n)$ and $\psi_y(g) = 0$ for any symmetry g . In particular $\text{Res}_H^G \psi_y = \chi_y + \chi_{-y}$, and Frobenius reciprocity shows ψ_y is irreducible iff $n \nmid 2y$. Since $n = 2m$, this fails for $y = 0$ and $y = m$ (and indeed $\psi_0 = \mathbf{1} + \xi\eta$ and $\psi_m = \xi + \eta$, using $\psi_y(\rho^m) = 2 \cos(\pi y) = 2(-1)^y$). For $y \in \{1, \dots, m-1\}$, the characters $\psi_y = \psi_{-y}$ are $m-1$ pairwise distinct irreducibles of degree 2. Together with the four degree-1 characters this gives $m+3$ irreducibles in total, matching the number of conjugacy classes. The character table of D_{2n} ($n = 2m$ even) is:

	Id	ρ^x ($1 \leq x \leq m-1$)	-Id	σ	τ
#	1	2	1	m	m
$\mathbf{1}$	1	1	1	1	1
ξ	1	$(-1)^x$	$(-1)^m$	-1	1
η	1	$(-1)^x$	$(-1)^m$	1	-1
$\xi\eta$	1	1	1	-1	-1
ψ_y ($1 \leq y \leq m-1$)	2	$2 \cos \frac{2\pi xy}{n}$	$2(-1)^y$	0	0

This gives $Z(G) = \{\text{Id}, -\text{Id}\}$ (the two singleton conjugacy classes) and $D(G) = K = \langle \rho^2 \rangle$ (since $D(G) = \text{Ker } \xi \cap \text{Ker } \eta = K$).

A.6 Chapter 6

Solution to Exercise 6.27.

Write $\omega = e^{2\pi i/3}$, so that the irreducible characters of \mathbb{Z}_3 are $\chi_k(\bar{m}) = \omega^{km}$ for $k = 0, 1, 2$ (Proposition 4.34). The function values are $f(\bar{0}) = 0$, $f(\bar{1}) = \sin(2\pi/3) = \frac{\sqrt{3}}{2}$, and $f(\bar{2}) = \sin(4\pi/3) = -\frac{\sqrt{3}}{2}$. By Definition 6.10,

$$\hat{f}(\bar{k}) = \sum_{m=0}^2 \omega^{-km} f(\bar{m}) = \frac{\sqrt{3}}{2} (\omega^{-k} - \omega^{-2k}).$$

Using $\omega^{-1} = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$ and $\omega^{-2} = \omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$,

$$\hat{f}(\bar{0}) = 0, \quad \hat{f}(\bar{1}) = \frac{\sqrt{3}}{2}(-i\sqrt{3}) = -\frac{3i}{2}, \quad \hat{f}(\bar{2}) = \frac{\sqrt{3}}{2}(i\sqrt{3}) = \frac{3i}{2}.$$

The fact that $\hat{f}(\bar{2}) = \overline{\hat{f}(\bar{1})}$ reflects the general identity $\hat{f}(-\bar{k}) = \overline{\hat{f}(\bar{k})}$ valid for real-valued f . Since f is odd, \hat{f} is purely imaginary – the discrete analogue of the classical fact that the Fourier transform of an odd function is imaginary.

Solution to Exercise 6.28.

The Cayley graph $\Gamma(\mathbb{Z}_6, S)$ has six vertices $\bar{0}, \dots, \bar{5}$ arranged on a hexagon; each vertex \bar{i} is joined to $\bar{i} \pm \bar{2}$ (two “diagonal” neighbours at distance 2 on the hexagon) and to $\bar{i} + \bar{3}$ (the antipodal vertex). It is therefore a 3-regular graph on six vertices: two disjoint triangles $\{\bar{0}, \bar{2}, \bar{4}\}$, $\{\bar{1}, \bar{3}, \bar{5}\}$ (from $\pm\bar{2}$) together with a perfect matching $\{\bar{0}\bar{3}, \bar{1}\bar{4}, \bar{2}\bar{5}\}$ (from $\pm\bar{3}$), i.e. the triangular prism $K_3 \square K_2$.

By Corollary 6.18 with $\omega = e^{2\pi i/6} = e^{i\pi/3}$ and $S = \{\bar{2}, \bar{3}, \bar{4}\}$,

$$\lambda_k = \omega^{2k} + \omega^{3k} + \omega^{4k} = 2 \cos\left(\frac{2\pi k}{3}\right) + (-1)^k, \quad k = 0, \dots, 5.$$

Tabulating:

$$\lambda_0 = 3, \quad \lambda_1 = -2, \quad \lambda_2 = 0, \quad \lambda_3 = 1, \quad \lambda_4 = 0, \quad \lambda_5 = -2.$$

Spectrum: $\{3, 1, 0, 0, -2, -2\}$. As a check, $\sum_k \lambda_k = 0 = \text{tr } A$ and $\sum_k \lambda_k^2 = 18 = \text{tr } A^2 = 6 \cdot 3$ (each vertex has degree 3).

Solution to Exercise 6.29.

Since G is abelian, every function on G is a class function, so $\{\chi_1, \dots, \chi_n\}$ is an orthonormal basis of $L(G)$ (Theorem 3.35, plus the fact that there are $n = \#G$ of them). Expand a, b as

$$a = \sum_{i=1}^n (\chi_i | a) \chi_i = \frac{1}{n} \sum_{i=1}^n \hat{a}(g_i) \chi_i,$$

using $\hat{a}(g_i) = n(\chi_i | a)$, and similarly for b . Then by orthonormality of the χ_i ,

$$(a | b) = \sum_{i,j} \frac{\hat{a}(g_i)}{n} \overline{\left(\frac{\hat{b}(g_j)}{n}\right)} (\chi_i | \chi_j) = \frac{1}{n^2} \sum_{i=1}^n \hat{a}(g_i) \overline{\hat{b}(g_i)} = \frac{1}{n} (\hat{a} | \hat{b}).$$

Solution to Exercise 6.30.

1. Since f is a class function, $f \in Z(L(G))$; equivalently, $f * \delta_g = \delta_g * f$ for every $g \in G$. Applying Theorem 6.25 and Remark 6.22 to both sides yields

$$\hat{f}(\rho^{(k)}) \overline{\rho^{(k)}(g)} = \overline{\rho^{(k)}(g)} \hat{f}(\rho^{(k)}) \quad \text{for all } g \in G.$$

Conjugating entry-wise, $\overline{\hat{f}(\rho^{(k)})}$ commutes with $\rho^{(k)}(g)$ for all g , hence is a G -equivariant endomorphism of the irreducible representation $\rho^{(k)}$. By Corollary 3.3, $\overline{\hat{f}(\rho^{(k)})} = \mu I_{d_k}$ for some $\mu \in \mathbb{C}$, and therefore $\hat{f}(\rho^{(k)}) = \bar{\mu} I_{d_k}$ is scalar. Taking traces:

$$d_k \cdot \bar{\mu} = \text{tr } \hat{f}(\rho^{(k)}) = \sum_i \sum_g \overline{\rho_{ii}^{(k)}(g)} f(g) = \sum_g f(g) \overline{\chi_k(g)} = n(f | \chi_k),$$

giving $\hat{f}(\rho^{(k)}) = \frac{n}{d_k} (f | \chi_k) I_{d_k}$.

2. For $f = e_i = (d_i/n)\chi_i$, $(e_i | \chi_k) = (d_i/n)(\chi_i | \chi_k) = (d_i/n)\delta_{ik}$ by orthonormality of irreducible characters. Substituting into part (1):

$$\hat{e}_i(\rho^{(k)}) = \frac{n}{d_k} \cdot \frac{d_i}{n} \delta_{ik} I_{d_k} = \delta_{ik} I_{d_k}.$$

3. By Theorem 6.25, $\widehat{e_i * e_j}(\rho^{(k)}) = \hat{e}_i(\rho^{(k)}) \hat{e}_j(\rho^{(k)}) = \delta_{ik} \delta_{jk} I_{d_k}$. If $i \neq j$, this vanishes for every k , so $e_i * e_j = 0$ by injectivity of the Fourier transform. If $i = j$, the right side equals $\delta_{ik} I_{d_k} = \hat{e}_i(\rho^{(k)})$ for every k , so $e_i * e_i = e_i$. Each e_k is a scalar multiple of a class function, hence central in $L(G)$.

4. Set $e = e_1 + \dots + e_s$. By part (2), $\hat{e}(\rho^{(k)}) = I_{d_k}$ for every k . Applying Theorem 6.23,

$$e(g) = \frac{1}{n} \sum_{k=1}^s d_k \sum_{i,j} (I_{d_k})_{ij} \varphi_{ij}^{(k)}(g) = \frac{1}{n} \sum_{k=1}^s d_k \sum_i \varphi_{ii}^{(k)}(g) = \frac{1}{n} \sum_{k=1}^s d_k \chi_k(g) = \frac{\chi_L(g)}{n},$$

where χ_L is the character of the regular representation. By Theorem 4.3, $\chi_L(g) = n$ if $g = 1_G$ and 0 otherwise, so $e = \delta_{1_G}$.

The identity $\delta_{1_G} = \sum_k e_k$ is the convolution-algebra version of the Wedderburn decomposition: the e_k are the central idempotents of $\mathbb{C}[G]$ that project onto the $\rho^{(k)}$ -isotypic component, recovering the projections of Theorem 4.24.

Solution to Exercise 6.31.

1. By Schur orthogonality (Theorem 6.7), the Fourier transform of $\varphi_{ij}^{(k)}$ is

$$\widehat{\varphi_{ij}^{(k)}}(\rho^{(l)})_{ab} = \sum_g \overline{\rho_{ab}^{(l)}(g)} \rho_{ij}^{(k)}(g) = n(\varphi_{ij}^{(k)} | \varphi_{ab}^{(l)}) = \frac{n}{d_k} \delta_{kl} \delta_{ia} \delta_{jb},$$

so $\widehat{\varphi_{ij}^{(k)}}(\rho^{(l)}) = (n/d_k) \delta_{kl} E_{ij}$, where E_{ij} is the matrix unit. By part (1) of Exercise 6.30, $\hat{a}(\rho^{(l)}) = (n/d_l)(a | \chi_l) I_{d_l}$. By Theorem 6.25,

$$a * \widehat{\varphi_{ij}^{(k)}}(\rho^{(l)}) = \hat{a}(\rho^{(l)}) \widehat{\varphi_{ij}^{(k)}}(\rho^{(l)}) = \frac{n}{d_l} (a | \chi_l) \cdot \frac{n}{d_k} \delta_{kl} E_{ij},$$

which equals 0 for $l \neq k$ and $\frac{n}{d_k} (a | \chi_k) \cdot \widehat{\varphi_{ij}^{(k)}}(\rho^{(k)})$ for $l = k$. Hence all Fourier components of $a * \varphi_{ij}^{(k)}$ agree with those of $\frac{n}{d_k} (a | \chi_k) \varphi_{ij}^{(k)}$, and by injectivity of the Fourier transform,

$$F(\varphi_{ij}^{(k)}) = a * \varphi_{ij}^{(k)} = \frac{n}{d_k} (a | \chi_k) \varphi_{ij}^{(k)}.$$

2. By Peter–Weyl (Theorem 6.8), the matrix coefficients $\{\varphi_{ij}^{(k)}\}_{k,i,j}$ form a basis of $L(G)$, and part (1) exhibits each as an eigenvector of F . Hence F is diagonalizable.
3. By the same computation as in the proof of Theorem 6.17, $(\delta_S * \delta_{g_j})(g_i) = \mathbf{1}[g_i g_j^{-1} \in S] = A_{ij}$, so the matrix of F in the delta basis is exactly A . The eigenvalues of F , and hence of A , are therefore the numbers

$$\frac{n}{d_k} (\delta_S | \chi_k) = \frac{n}{d_k} \cdot \frac{1}{n} \sum_{s \in S} \overline{\chi_k(s)} = \frac{1}{d_k} \sum_{s \in S} \chi_k(s),$$

where the last equality uses $S = S^{-1}$ together with $\chi_k(s^{-1}) = \overline{\chi_k(s)}$ to rewrite $\sum_{s \in S} \overline{\chi_k(s)} = \sum_{s \in S} \chi_k(s^{-1}) = \sum_{s \in S} \chi_k(s)$. For each fixed k there are d_k^2 matrix coefficients $\varphi_{ij}^{(k)}$ all sharing this eigenvalue, so λ_k has multiplicity d_k^2 .

4. Recall S_3 has three irreducible representations: trivial ($\mathbb{1}$), sign (ε), and the standard 2-dimensional (ρ), with $d_1 = d_2 = 1$, $d_3 = 2$ and character values on a transposition equal to 1, -1 , 0 respectively. Each $s \in S = \{(12), (13), (23)\}$ is a transposition, so

$$\lambda_1 = \frac{1}{1}(1 + 1 + 1) = 3, \quad \lambda_2 = \frac{1}{1}(-1 - 1 - 1) = -3, \quad \lambda_3 = \frac{1}{2}(0 + 0 + 0) = 0,$$

with multiplicities 1, 1, 4. The spectrum $\{3, -3, 0, 0, 0\}$ matches the well-known spectrum of $K_{3,3}$: the graph $\Gamma(S_3, S)$ is bipartite, with even and odd permutations as parts, and every transposition joins every even permutation to every odd one.

Solution to Exercise 6.32.

By independence and the law of total probability, for each $g \in G$,

$$\Pr[XY = g] = \sum_{(x,y) \in G \times G, xy=g} \Pr[X = x, Y = y] = \sum_{y \in G} \mu(gy^{-1})\nu(y) = (\mu * \nu)(g),$$

where the second equality parameterises the solutions of $xy = g$ by $y \in G$ and $x = gy^{-1}$, and the last is Definition 6.2.

Iterating, the distribution of a product $X_1 \cdots X_k$ of k independent random variables with distributions μ_1, \dots, μ_k is the convolution $\mu_1 * \cdots * \mu_k$. This is the starting point for the spectral analysis of random walks on groups: powers of the convolution operator describe the distribution of a walk, while their spectrum – computed in Exercise 6.31 above for groups via characters – controls the mixing time.

A.7 Chapter 7

Solution to Exercise 7.24.

1. By Theorem 7.10, every irreducible degree d divides $\#G = 39$, so $d \in \{1, 3, 13, 39\}$. By Corollary 4.4, $\sum_i d_i^2 = 39$, so $d_i^2 \leq 39$, ruling out $d_i = 13$ and $d_i = 39$. Hence each $d_i \in \{1, 3\}$.

Let m denote the number of degree-1 irreducibles and r the number of degree-3 irreducibles. Then $m + 9r = 39$. By Lemma 7.12, $m = [G : G']$ divides 39, so $m \in \{1, 3, 13, 39\}$. The equation $m + 9r = 39$ forces $m \equiv 39 \equiv 3 \pmod{9}$, leaving $m \in \{3, 39\}$.

If $m = 39$, every irreducible has degree 1, which (by Corollary 4.23 applied via $\sum d_i^2 = \#G = \#\text{Irr}(G)$) would force G to be abelian, contradicting the hypothesis. Hence $m = 3$ and $r = (39 - 3)/9 = 4$. Thus G has exactly 3 irreducible representations of degree 1 and 4 of degree 3.

2. By Theorem 4.21, the number of conjugacy classes equals $\#\text{Irr}(G) = 3 + 4 = 7$.

Solution to Exercise 7.25.

Suppose a non-solvable group of order $p^a q^b$ exists, and let G be one of *minimum* order. We claim G is simple non-abelian, which gives the result with $a' = a$ and $b' = b$.

First, G is non-abelian: a finite abelian group is solvable (its derived series terminates immediately at $\{1\}$).

Suppose for contradiction that G has a proper non-trivial normal subgroup N . Then $\#N = p^{a_1} q^{b_1}$ and $\#(G/N) = p^{a-a_1} q^{b-b_1}$, both strictly less than $\#G$. By minimality of G , both N and G/N are solvable. The class of solvable groups is closed under extensions: if $N \triangleleft G$ with N and G/N solvable, then G is solvable. (Indeed, the derived series of G satisfies $G^{(k)} \subseteq N$ once k is large enough that $G^{(k)} \cdot N/N = (G/N)^{(k)} = \{N\}$ in G/N ; then it terminates because N is solvable.) Hence G is solvable, contradicting our assumption.

Therefore G has no proper non-trivial normal subgroup, i.e. G is simple.

This exercise shows that to *prove* Burnside's theorem in the form "every group of order $p^a q^b$ is solvable," it suffices to rule out simple non-abelian groups of this order, which is precisely what Theorem 7.22 accomplishes (cf. the remark following its proof).

Solution to Exercise 7.26.

By Lemma 3.22, $\varphi(g)$ is diagonalizable with eigenvalues $\lambda_1, \dots, \lambda_d$ that are roots of unity, and $\chi(g) = \lambda_1 + \cdots + \lambda_d$.

If $g \in \ker \varphi$, then $\varphi(g) = I_d$, so every $\lambda_i = 1$ and $\chi(g) = d$.

Conversely, suppose $\chi(g) = d$. Then $|\lambda_1 + \cdots + \lambda_d| = d$, so by Lemma 7.14 all the λ_i are equal. Their common value λ satisfies $d\lambda = d$, i.e. $\lambda = 1$. Hence $\varphi(g)$ is diagonalizable with every eigenvalue equal to 1, which forces $\varphi(g) = I_d$, i.e. $g \in \ker \varphi$.

A useful consequence: the kernel of φ is detected purely by the character, $\ker \varphi = \{g \in G : \chi(g) = \chi(1)\}$. In particular, the character of any faithful representation distinguishes 1_G from every other element of G . This is the starting point for recovering normal subgroups of G directly from the character table: every normal subgroup is an intersection $\bigcap_{i \in I} \ker \varphi^{(i)}$ for some subset of the irreducible representations.