Representations of Finite Groups

Andrew Baker

School of Mathematics & Statistics, University of Glasgow.
E-mail address: a.baker@maths.gla.ac.uk
URL: http://www.maths.gla.ac.uk/∼ajb

Contents

CHAPTER 1

Linear and multilinear algebra

In this chapter we will study the *linear algebra* required in representation theory. Some of this will be familiar but there will also be new material, especially that on 'multilinear' algebra.

1.1. Basic linear algebra

Throughout the remainder of these notes $\Bbbk$ will denote a *field*, i.e., a commutative ring with unity 1 in which every non-zero element has an inverse. Most of the time in representation theory we will work with the field of complex numbers $\mathbb{C}$ and occasionally the field of real numbers $\mathbb{R}$. However, a lot of what we discuss will work over more general fields, including those of *finite characteristic* such as $\mathbb{F}_p = \mathbb{Z}/p$ for a prime p. Here, the *characteristic* of the field $\Bbbk$ is defined to be the smallest natural number $p \in \mathbb{N}$ such that

$$p1 = \underbrace{1 + \cdots + 1}_{p \text{ summands}} = 0,$$

provided such a number exists, in which case $\Bbbk$ is said to have *finite* or *positive characteristic*, otherwise $\Bbbk$ is said to have characteristic 0. When the characteristic of $\Bbbk$ is finite it is actually a prime number.

1.1.1. Bases, linear transformations and matrices. Let V be a finite dimensional vector space over $\Bbbk$, i.e., a $\Bbbk$-vector space. Recall that a *basis* for V is a linearly independent spanning set for V. The *dimension* of V (over $\Bbbk$) is the number of elements in any basis, and is denoted $\dim_{\Bbbk} V$. We will often view $\Bbbk$ itself as a 1-dimensional $\Bbbk$-vector space with basis $\{1\}$ or indeed any set $\{x\}$ with $x \neq 0$.

Given two $\Bbbk$-vector spaces V, W, a *linear transformation* (or *linear mapping*) from V to W is a function $\varphi\colon V \to W$ such that

$$\begin{aligned} \varphi(v_1 + v_2) &= \varphi(v_1) + \varphi(v_2) && (v_1, v_2, v \in V), \\ \varphi(tv) &= t\varphi(v) && (t \in \Bbbk). \end{aligned}$$

We will be denote the set of all linear transformations $V \to W$ by $\mathrm{Hom}_{\Bbbk}(V, W)$. This is a $\Bbbk$-vector space with the operations of addition and scalar multiplication given by

$$\begin{aligned} (\varphi + \theta)(u) &= \varphi(u) + \theta(u) && (\varphi, \theta \in \mathrm{Hom}_{\Bbbk}(V, W)), \\ (t\varphi)(u) &= t(\varphi(u)) = \varphi(tu) && (t \in \Bbbk). \end{aligned}$$

The *extension property* in the next result is an important property of a basis.

Proposition 1.1. *Let V, W be $\Bbbk$-vector spaces with V finite dimensional, and $\{v_1, \ldots, v_m\}$ a basis for V where $m = \dim_{\Bbbk} V$. Given a function $\varphi\colon \{v_1, \ldots, v_m\} \to W$, there is a unique linear transformation $\tilde{\varphi}\colon V \to W$ such that*

$$\tilde{\varphi}(v_j) = \varphi(v_j) \quad (1 \leqslant j \leqslant m).$$

We can express this with the aid of the *commutative diagram*

$$\begin{tikzcd}
\{v_1, \ldots, v_m\} \arrow[rr, "\text{inclusion}"] \arrow[dr, "\varphi"'] & & V \arrow[dl, dotted, "\exists!\, \tilde{\varphi}"] \\
& W &
\end{tikzcd}$$

in which the dotted arrow is supposed to indicate a (unique) solution to the problem of filling in the diagram

$$\begin{tikzcd}
\{v_1, \ldots, v_m\} \arrow[rr, "\text{inclusion}"] \arrow[dr, "\varphi"'] & & V \\
& W &
\end{tikzcd}$$

with a linear transformation so that composing the functions corresponding to the horizontal and right hand sides agrees with the functions corresponding to left hand side.

Proof. The formula for $\tilde{\varphi}$ is

$$\tilde{\varphi}\left(\sum_{j=1}^{m} \lambda_j v_j\right) = \sum_{j=1}^{m} \lambda_j \varphi(v_j). \qquad \square$$

The linear transformation $\tilde{\varphi}$ is known as the *linear extension* of φ and is often just denoted by φ.

Let V, W be finite dimensional $\Bbbk$-vector spaces with the bases $\{v_1, \ldots, v_m\}$ and $\{w_1, \ldots, w_n\}$ respectively, where $m = \dim_\Bbbk V$ and $n = \dim_\Bbbk W$. By Proposition 1.1, for $1 \leqslant i \leqslant m$ and $1 \leqslant j \leqslant n$, the function

$$\varphi_{ij} \colon \{v_1, \ldots, v_m\} \to W; \quad \varphi_{ij}(v_k) = \delta_{ik} w_j \quad (1 \leqslant k \leqslant m)$$

has a unique extension to a linear transformation $\varphi_{ij} \colon V \to W$.

Proposition 1.2. *The collection of functions* $\varphi_{ij} \colon V \to W$ $(1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant n)$ *forms a basis for* $\operatorname{Hom}_\Bbbk(V, W)$. *Hence*

$$\dim_\Bbbk \operatorname{Hom}_\Bbbk(V, W) = \dim_\Bbbk V \dim_\Bbbk W = mn.$$

A particular and important case of this is the *dual space* of V,

$$V^* = \operatorname{Hom}(V, \Bbbk).$$

Notice that $\dim_\Bbbk V^* = \dim_\Bbbk V$. Given any basis $\{v_1, \ldots, v_m\}$ of V, define elements $v_i^* \in V^*$ $(i = 1, \ldots, m)$ by

$$v_i^*(v_k) = \delta_{ik},$$

where δ_{ij} is the *Kronecker δ-function* for which

$$\delta_{ij} = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{otherwise.} \end{cases}$$

Then the set of functions $\{v_1^*, \ldots, v_m^*\}$ forms a basis of V^*. There is an associated isomorphism $V \to V^*$ under which

$$v_j \longleftrightarrow v_j^*.$$

If we set $V^{**} = (V^*)^*$, the double dual of V, then there is an isomorphism $V^* \to V^{**}$ under which

$$v_j^* \longleftrightarrow (v_j^*)^*.$$

Here we use the fact that the v_j^* form a basis for V^*. Composing these two isomorphisms we obtain a third $V \to V^{**}$ given by

$$v_j \longleftrightarrow (v_j^*)^*.$$

In fact, this does not depend on the basis of V used, although the factors do! This is sometimes called the *canonical isomorphism* $V \to V^{**}$.

The set of all ($\Bbbk$-)*endomorphisms* of V is

$$\mathrm{End}_{\Bbbk}(V) = \mathrm{Hom}_{\Bbbk}(V, V).$$

This is a ring (actually a $\Bbbk$-*algebra*, and also non-commutative if $\dim_{\Bbbk} V > 1$) with addition as above, and composition of functions as its multiplication. There is a ring monomorphism

$$\Bbbk \to \mathrm{End}_{\Bbbk}(V); \quad t \longmapsto t\,\mathrm{Id}_V,$$

which embeds $\Bbbk$ into $\mathrm{End}_{\Bbbk}(V)$ as the *subring of scalars*. We also have

$$\dim_{\Bbbk} \mathrm{End}_{\Bbbk}(V) = (\dim_{\Bbbk} V)^2.$$

Let $\mathrm{GL}_{\Bbbk}(V)$ denote the group of all invertible $\Bbbk$-linear transformations $V \to V$, i.e., the group of units in $\mathrm{End}_{\Bbbk}(V)$. This is usually called the *general linear group* of V or the *group of linear automorphisms* of V and denoted $\mathrm{GL}_{\Bbbk}(V)$ or $\mathrm{Aut}_{\Bbbk}(V)$.

Now let $\mathbf{v} = \{v_1, \ldots, v_m\}$ and $\mathbf{w} = \{w_1, \ldots, w_n\}$ be bases for V and W. Then given a linear transformation $\varphi\colon V \to W$ we may define the matrix of φ with respect to the bases $\mathbf{v}$ and $\mathbf{w}$ to be the $n \times m$ matrix with coefficients in $\Bbbk$,

$$_{\mathbf{w}}[\varphi]_{\mathbf{v}} = [a_{ij}],$$

where

$$\varphi(v_j) = \sum_{k=1}^{n} a_{kj} w_k.$$

Now suppose we have a second pair of bases for V and W, say $\mathbf{v}' = \{v'_1, \ldots, v'_m\}$ and $\mathbf{w}' = \{w'_1, \ldots, w'_n\}$. Then we can write

$$v'_j = \sum_{r=1}^{m} p_{rj} v_r, \quad w'_j = \sum_{s=1}^{n} q_{sj} w_s,$$

for some $p_{ij}, q_{ij} \in \Bbbk$. If we form the $m \times m$ and $n \times n$ matrices $P = [p_{ij}]$ and $Q = [q_{ij}]$, then we have the following standard result.

Proposition 1.3. *The matrices* $_{\mathbf{w}}[\varphi]_{\mathbf{v}}$ *and* $_{\mathbf{w}'}[\varphi]_{\mathbf{v}'}$ *are related by the formulæ*

$$_{\mathbf{w}'}[\varphi]_{\mathbf{v}'} = Q\,_{\mathbf{w}}[\varphi]_{\mathbf{v}} P^{-1} = Q[a_{ij}]P^{-1}.$$

In particular, if $W = V$, $\mathbf{w} = \mathbf{v}$ *and* $\mathbf{w}' = \mathbf{v}'$, *then*

$$_{\mathbf{v}'}[\varphi]_{\mathbf{v}'} = P\,_{\mathbf{v}}[\varphi]_{\mathbf{v}} P^{-1} = P[a_{ij}]P^{-1}.$$

1.1.2. Quotients and complements. Let $W \subseteq V$ be a vector subspace. Then we define the *quotient space* V/W to be the set of equivalence classes under the equivalence relation $\sim$ on V defined by

$$u \sim v \quad \text{if and only if} \quad v - u \in W.$$

We denote the class of v by $v + W$. This set V/W becomes a vector space with operations

$$(u + W) + (v + W) = (u + v) + W,$$
$$\lambda(v + W) = (\lambda v) + W$$

and zero element $0 + W$. There is a linear transformation, usually called the *quotient map* $q\colon V \to V/W$, defined by

$$q(v) = v + W.$$

Then q is surjective, has kernel $\ker q = W$ and has the following *universal property*.

THEOREM 1.4. *Let $f\colon V \to U$ be a linear transformation with $W \subseteq \ker f$. Then there is a unique linear transformation $\overline{f}\colon V/W \to U$ for which $f = \overline{f} \circ q$. This can be expressed in the diagram*

$$\begin{tikzcd} V \arrow[rr, "q"] \arrow[dr, "f"'] & & V/W \arrow[dl, dotted, "\exists!\,\overline{f}"] \\ & U & \end{tikzcd}$$

in which all the sides represent linear transformations.

PROOF. We define $\overline{f}$ by

$$\overline{f}(v + W) = f(v),$$

which makes sense since if $v' \sim v$, then $v' - v \in W$, hence

$$f(v') = f((v' - v) + v) = f(v' - v) + f(v) = f(v).$$

The uniqueness follows from the fact that q is surjective. $\square$

Notice also that

$$\dim_{\Bbbk} V/W = \dim_{\Bbbk} V - \dim_{\Bbbk} W. \tag{1.1}$$

A *linear complement* (in V) of a subspace $W \subseteq V$ is a subspace $W' \subseteq V$ such that the restriction $q_{|_{W'}}\colon W' \to V/W$ is a linear isomorphism. The next result sums up properties of linear complements and we leave the proofs as exercises.

THEOREM 1.5. *Let $W \subseteq V$ and $W' \subseteq V$ be vector subspaces of the $\Bbbk$-vector space V with $\dim_{\Bbbk} V = n$. Then the following conditions are equivalent.*

(a) *W' is a linear complement of W in V.*

(b) *Let $\{w_1, \ldots, w_r\}$ be a basis for W, and $\{w_{r+1}, \ldots, w_n\}$ a basis for W'. Then*

$$\{w_1, \ldots, w_n\} = \{w_1, \ldots, w_r\} \cup \{w_{r+1}, \ldots, w_n\}$$

is a basis for V.

(c) *Every $v \in V$ has a unique expression of the form*

$$v = v_1 + v_2$$

for some elements $v_1 \in W$, $v_2 \in W'$. In particular, $W \cap W' = \{0\}$.

(d) *Every linear transformation $h\colon W' \to U$ has a unique extension to a linear transformation $H\colon V \to U$ with $W \subseteq \ker H$.*

(e) *W is a linear complement of W' in V.*

(f) *There is a linear isomorphism $J\colon V \xrightarrow{\cong} W \times W'$ for which $\operatorname{im} J_{|_W} = W \times \{0\}$ and $\operatorname{im} J_{|_{W'}} = \{0\} \times W'$.*

(g) *There are unique linear transformations $p\colon V \to V$ and $p'\colon V \to V$ having images $\operatorname{im} p = W$, $\operatorname{im} p' = W'$ and which satisfy*

$$p^2 = p \circ p = p, \quad {p'}^2 = p' \circ p' = p', \quad \mathrm{Id}_V = p + p'.$$

We often write $V = W \oplus W'$ whenever W' is a linear complement of W. The maps p, p' of Theorem 1.5(g) are often called the (*linear*) *projections onto W and W'*.

This situation just discussed can be extended to the case of r subspaces $V_1, \ldots, V_r \subseteq V$ for which

$$V = V_1 + \cdots + V_r = \Big\{ \sum_{j=1}^{r} v_j : v_j \in V_j \Big\},$$

and inductively we have that V_k is a linear complement of $(V_1 \oplus \cdots \oplus V_{k-1})$ in $(V_1 + \cdots + V_k)$.

A linear complement for a subspace $W \subseteq V$ always exists since each basis $\{w_1, \ldots, w_r\}$ of W extends to a basis $\{w_1, \ldots, w_r, w_{r+1}, \ldots, w_n\}$ of V, and on taking W' to be the subspace spanned by $\{w_{r+1}, \ldots, w_n\}$, Theorem 1.5(b) implies that W' *is* a linear complement.

1.2. Class functions and the Cayley-Hamilton Theorem

In this section $\Bbbk$ can be any field. Let $A = [a_{ij}]$ be an $n \times n$ matrix over $\Bbbk$.

Definition 1.6. The *characteristic polynomial* of A is the polynomial (in the variable X)

$$\operatorname{char}_A(X) = \det(XI_n - [a_{ij}]) = \sum_{k=0}^{n} c_k(A) X^k \in \Bbbk[X],$$

where I_n is the $n \times n$ identity matrix.

Notice that $c_n(A) = 1$, so this polynomial in X is monic and has degree n. The coefficients $c_k(A) \in \Bbbk$ are polynomial functions of the entries a_{ij}. The following is an important result about the characteristic polynomial.

Theorem 1.7 (**Cayley-Hamilton Theorem: matrix version**). *The matrix A satisfies the polynomial identity*

$$\operatorname{char}_A(A) = \sum_{k=0}^{n} c_k(A) A^k = 0.$$

Example 1.8. Let

$$A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \in \mathbb{R}[X].$$

Then

$$\operatorname{char}_A(X) = \det \begin{bmatrix} X & 1 \\ -1 & X \end{bmatrix} = X^2 + 1.$$

By calculation we find that $A^2 + I_2 = O_2$ as claimed.

LEMMA 1.9. *Let $A = [a_{ij}]$ and P be an $n \times n$ matrix with coefficients in $\Bbbk$. Then if P is invertible,*

$$\operatorname{char}_{PAP^{-1}}(X) = \operatorname{char}_A(X).$$

Thus each of the coefficients $c_k(A)$ $(0 \leqslant k \leqslant n)$ satisfies

$$c_k(PAP^{-1}) = c_k(A).$$

PROOF. We have

$$\begin{aligned}
\operatorname{char}_{PAP^{-1}}(X) &= \det(XI_n - PAP^{-1}) \\
&= \det(P(XI_n)P^{-1} - PAP^{-1}) \\
&= \det(P(XI_n - A)P^{-1}) \\
&= \det P \det(XI_n - A) \det P^{-1} \\
&= \det P \operatorname{char}_A(X)(\det P)^{-1} \\
&= \operatorname{char}_A(X).
\end{aligned}$$

Comparing coefficients we obtain the result. □

This result shows that as functions of A (and hence of the a_{ij}), the coefficients $c_k(A)$ are *invariant* or *class functions* in the sense that they are invariant under conjugation,

$$c_r(PAP^{-1}) = c_r(A).$$

Recall that for an $n \times n$ matrix $A = [a_{ij}]$, the *trace* of A, $\operatorname{tr} A \in \Bbbk$, is defined by

$$\operatorname{tr} A = \sum_{j=1}^{n} a_{jj}.$$

PROPOSITION 1.10. *For any $n \times n$ matrix over $\Bbbk$ we have*

$$c_{n-1}(A) = -\operatorname{tr} A \quad \textit{and} \quad c_n(A) = (-1)^n \det A.$$

PROOF. The coefficient of X^{n-1} in $\det(XI_n - [a_{ij}])$ is

$$-\sum_{r=1}^{n} a_{rr} = -\operatorname{tr}[a_{ij}] = -\operatorname{tr} A,$$

giving the formula for $c_{n-1}(A)$. Putting $X = 0$ in $\det(XI_n - [a_{ij}])$ gives

$$c_n(A) = \det([-a_{ij}]) = (-1)^n \det[a_{ij}] = (-1)^n \det A. \qquad \square$$

Now let $\varphi\colon V \to V$ be a linear transformation on a finite dimensional $\Bbbk$-vector space with a basis $\mathbf{v} = \{v_1, \ldots, v_n\}$. Consider the matrix of φ relative to $\mathbf{v}$,

$$[\varphi]_{\mathbf{v}} = [a_{ij}],$$

where

$$\varphi(v_j) = \sum_{r=1}^{n} a_{rj} v_r.$$

Then the *trace of φ with respect to the basis* $\mathbf{v}$ is

$$\operatorname{tr}_{\mathbf{v}} \varphi = \operatorname{tr}[\varphi]_{\mathbf{v}}.$$

If we change to a second basis $\mathbf{w}$ say, there is an invertible $n \times n$ matrix $P = [p_{ij}]$ such that

$$w_j = \sum_{r=1}^{n} p_{rj} v_r,$$

and then

$$[\varphi]_{\mathbf{w}} = P[\varphi]_{\mathbf{v}} P^{-1}.$$

Hence,

$$\operatorname{tr}_{\mathbf{w}} \varphi = \operatorname{tr}\left(P[\varphi]_{\mathbf{v}} P^{-1}\right) = \operatorname{tr}_{\mathbf{v}} \varphi.$$

Thus we see that the quantity

$$\operatorname{tr} \varphi = \operatorname{tr}_{\mathbf{v}} \varphi$$

only depends on φ, not the basis $\mathbf{v}$. We call this the *trace* of φ. Similarly, we can define $\det \varphi = \det A$.

More generally, we can consider the polynomial

$$\operatorname{char}_{\varphi}(X) = \operatorname{char}_{[\varphi]_{\mathbf{v}}}(X)$$

which by Lemma 1.9 is independent of the basis $\mathbf{v}$. Thus all of the coefficients $c_k(A)$ are functions of φ and do not depend on the basis used, so we may write $c_k(\varphi)$ in place of $c_k(A)$. In particular, an alternative way to define $\operatorname{tr} \varphi$ and $\det \varphi$ is by setting

$$\operatorname{tr} \varphi = -c_{n-1}(\varphi) = \operatorname{tr} A, \quad \det \varphi = (-1)^n c_0(\varphi) = \det A.$$

We also call $\operatorname{char}_{\varphi}(X)$ the *characteristic polynomial* of φ. The following is a formulation of the Cayley-Hamilton Theorem for a linear transformation.

Theorem 1.11 (**Cayley-Hamilton Theorem: linear transformation version**). *If $\varphi\colon V \to V$ is a $\Bbbk$-linear transformation on the finite dimensional $\Bbbk$-vector space V, then φ satisfies the polynomial identity*

$$\operatorname{char}_{\varphi}(\varphi) = 0.$$

More explicitly, if

$$\operatorname{char}_{\varphi}(X) = \sum_{r=0}^{n} c_r(\varphi) X^r,$$

then writing $\varphi^0 = \mathrm{Id}_V$, we have

$$\sum_{r=0}^{n} c_r(\varphi)\varphi^r = 0.$$

There is an important connection between class functions of matrices (such as the trace and determinant) and eigenvalues. Recall that if $\Bbbk$ is an algebraically closed field then any non-constant monic polynomial with coefficients in $\Bbbk$ factors into d linear factors over $\Bbbk$, where d is the degree of the polynomial.

Proposition 1.12. *Let $\Bbbk$ be an algebraically closed field and let A be an $n \times n$ matrix with entries in $\Bbbk$. Then the eigenvalues of A in $\Bbbk$ are the roots of the characteristic polynomial $\operatorname{char}_A(X)$ in $\Bbbk$. In particular, A has at most n distinct eigenvalues in $\Bbbk$.*

On factoring $\mathrm{char}_A(X)$ into linear factors over $\Bbbk$ we may find some repeated linear factors corresponding to 'repeated' or 'multiple' roots. If a linear factor $(X - \lambda)$ appears to degree m say, we say that λ is an eigenvalue of *multiplicity* m. If every eigenvalue of A has multiplicity 1, then A is diagonalisable in the sense that there is an invertible matrix P satisfying

$$PAP^{-1} = \mathrm{diag}(\lambda_1, \dots, \lambda_n),$$

the diagonal matrix with the n distinct diagonal entries λ_k down the leading diagonal. More generally, let

$$\mathrm{char}_A(X) = (X - \lambda_1) \cdots (X - \lambda_n), \tag{1.2}$$

where now we allow some of the λ_j to be repeated. Then we can describe $\operatorname{tr} A$ and $\det A$ in terms of the eigenvalues λ_j.

PROPOSITION 1.13. *The following identities hold:*

$$\operatorname{tr} A = \sum_{j=1}^{n} \lambda_j = \lambda_1 + \cdots + \lambda_n, \quad \det A = \lambda_1 \cdots \lambda_n.$$

PROOF. These can be verified by considering the degree $(n-1)$ and constant terms in Equation (1.2) and using Proposition 1.10. $\square$

REMARK 1.14. More generally, the coefficient $(-1)^{n-k} c_k(A)$ can be expressed as the k-th elementary symmetric function in $\lambda_1, \dots, \lambda_n$.

We can also apply the above discussion to a linear transformation $\varphi\colon V \to V$, where an *eigenvector* for the *eigenvalue* $\lambda \in \mathbb{C}$ is a non-zero vector $v \in V$ satisfying $\varphi(v) = \lambda v$.

The characteristic polynomial may not be the polynomial of smallest degree satisfied by a matrix or a linear transformation. By definition, a *minimal polynomial* of an $n \times n$ matrix A or linear transformation $\varphi\colon V \to V$ is a (non-zero) monic polynomial $f(X)$ of smallest possible degree for which $f(A) = 0$ or $f(\varphi) = 0$.

LEMMA 1.15. *For an $n \times n$ matrix A or a linear transformation $\varphi\colon V \to V$, let $f(X)$ be a minimal polynomial and $g(X)$ be any other polynomial for which $g(A) = 0$ or $g(\varphi) = 0$. Then $f(X) \mid g(X)$. Hence $f(X)$ is the unique minimal polynomial.*

PROOF. We only give the proof for matrices, the proof for a linear transformation is similar.

Suppose that $f(X) \nmid g(X)$. Then we have

$$g(X) = q(X)f(X) + r(X),$$

where $\deg r(X) < \deg f(X)$. Since $r(A) = 0$ and $r(X)$ has degree less than $f(X)$, we have a contradiction. Hence $f(X) \mid g(X)$. In particular, if $g(X)$ has the same degree as $f(X)$, the minimality of $g(X)$ also gives $g(X) \mid f(X)$. As these are both monic polynomials, this implies $f(X) = g(X)$. $\square$

We write $\min_A(X)$ or $\min_\varphi(X)$ for the minimal polynomial of A or φ. Note also that $\min_A(X) \mid \mathrm{char}_A(X)$ and $\min_\varphi(X) \mid \mathrm{char}_\varphi(X)$.

1.3. Separability

LEMMA 1.16. *Let V be a finite dimensional vector space over $\mathbb{C}$ and let $\varphi\colon V \to V$ be a linear transformation. Suppose that*

$$0 \neq f(X) = \sum_{r=0}^{m} c_r X^r \in \mathbb{C}[X]$$

is a polynomial with no repeated linear factors over $\mathbb{C}$ and that φ satisfies the relation

$$\sum_{r=0}^{m} c_r \varphi^r = 0,$$

i.e., for every $v \in V$,

$$\sum_{r=0}^{m} c_r \varphi^r(v) = 0.$$

Then V has a basis $\mathbf{v} = \{v_1, \ldots, v_n\}$ consisting of eigenvectors of φ.

PROOF. By multiplying by the inverse of the leading coefficient of $f(X)$ we can replace $f(X)$ by a monic polynomial with the same properties, so we will assume that $f(X)$ is monic, i.e., $c_m = 1$. Factoring over $\mathbb{C}$, we obtain

$$f(X) = f_m(X) = (X - \lambda_1) \cdots (X - \lambda_m),$$

where the $\lambda_j \in \mathbb{C}$ are distinct. Put

$$f_{m-1}(X) = (X - \lambda_1) \cdots (X - \lambda_{m-1}).$$

Notice that $f_m(X) = f_{m-1}(X)(X - \lambda_m)$, hence $(X - \lambda_m)$ cannot divide $f_{m-1}(X)$, since this would lead to a contradiction to the assumption that $f_m(X)$ has no repeated linear factors.

Using *long division* of $(X - \lambda_m)$ into $f_{m-1}(X)$, we see that

$$f_{m-1}(X) = q_m(X)(X - \lambda_m) + r_m,$$

where the remainder $r_m \in \mathbb{C}$ cannot be 0 since if it were then $(X - \lambda_m)$ would divide $f_{m-1}(X)$. Dividing by r_m if necessary, we see that for some non-zero $s_m \in \mathbb{C}$,

$$s_m f_{m-1}(X) - q_m(X)(X - \lambda_m) = 1.$$

Substituting $X = \varphi$, we have for any $v \in V$,

$$s_m f_{m-1}(\varphi)(v) - q_m(\varphi)(\varphi - \lambda_m \operatorname{Id}_V)(v) = v.$$

Notice that we have

$$(\varphi - \lambda_m \operatorname{Id}_V)\,(s_m f_{m-1}(\varphi)(v)) = s_m f_m(\varphi)(v) = 0$$

and

$$f_{m-1}(\varphi)\,(q_m(\varphi)(\varphi - \lambda_m \operatorname{Id}_V)(v)) = q_m(\varphi) f_m(\varphi)(v) = 0.$$

Thus we can decompose v into a sum $v = v_m + v'_m$, where

$$(\varphi - \lambda_m \operatorname{Id}_V)(v_m) = 0 = f_{m-1}(\varphi)(v'_m).$$

Consider the following two subspaces of V:

$$V_m = \{v \in V : (\varphi - \lambda_m \operatorname{Id}_V)(v) = 0\},$$
$$V'_m = \{v \in V : f_{m-1}(\varphi)(v) = 0\}.$$

We have shown that $V = V_m + V'_m$. If $v \in V_m \cap V'_m$, then from above we would have

$$v = s_m f_{m-1}(\varphi)(v) - q_m(\varphi)(\varphi - \lambda_m \operatorname{Id}_V)(v) = 0.$$

So $V_m \cap V'_m = \{0\}$, hence $V = V_m \oplus V'_m$. We can now consider V'_m in place of V, noticing that for $v \in V'_m$, $\varphi(v) \in V'_m$, since

$$f_{m-1}(\varphi)(\varphi(v)) = \varphi\left(f_{m-1}(\varphi)(v)\right) = 0.$$

Continuing in this fashion, we eventually see that

$$V = V_1 \oplus \cdots \oplus V_m$$

where for $v \in V_k$,

$$(\varphi - \lambda_k)(v) = 0.$$

If we choose a basis $\mathbf{v}_{(k)}$ of V_k, then the (disjoint) union

$$\mathbf{v} = \mathbf{v}_{(1)} \cup \cdots \cup \mathbf{v}_{(m)}$$

is a basis for V, consisting of eigenvectors of φ. $\square$

The condition on φ in this result is sometimes referred to as the *separability* or *semisimplicity* of φ. We will make use of this when discussing *characters* of representations.

1.4. Basic notions of multilinear algebra

In this section we will describe the *tensor product* of r vector spaces. We will most often consider the case where $r = 2$, but give the general case for completeness. Multilinear algebra is important in differential geometry, relativity, electromagnetism, fluid mechanics and indeed much of advanced applied mathematics where tensors play a rôle.

Let $V_1, \ldots, V_r$ and W be $\Bbbk$-vector spaces. A function

$$F \colon V_1 \times \cdots \times V_r \to W$$

is $\Bbbk$-*multilinear* if it satisfies

(ML-1)
$$F(v_1, \ldots, v_{k-1}, v_k + v'_k, v_{k+1}, \ldots, v_r) = F(v_1, \ldots, v_k, \ldots, v_r) + F(v_1, \ldots, v_{k-1}, v'_k, v_{k+1}, \ldots, v_r),$$

(ML-2)
$$F(v_1, \ldots, v_{k-1}, t v_k, v_{k+1}, \ldots, v_r) = t F(v_1, \ldots, v_{k-1}, v_k, v_{k+1}, \ldots, v_r)$$

for $v_j, v'_j \in V$ and $t \in \Bbbk$. It is *symmetric* if for any permutation $\sigma \in S_r$ (the permutation group on r objects),

(ML-S) $$F(v_{\sigma(1)}, \ldots, v_{\sigma(k)}, \ldots, v_{\sigma(r)}) = F(v_1, \ldots, v_k, \ldots, v_r),$$

and is *alternating* or *skew-symmetric* if

(ML-A) $$F(v_{\sigma(1)}, \ldots, v_{\sigma(k)}, \ldots, v_{\sigma(r)}) = \operatorname{sign}(\sigma) F(v_1, \ldots, v_k, \ldots, v_r),$$

where $\operatorname{sign}(\sigma) \in \{\pm 1\}$ is the sign of σ.

The *tensor product* of $V_1, \dots, V_r$ is a $\Bbbk$-vector space $V_1 \otimes V_2 \otimes \cdots \otimes V_r$ together with a function $\tau\colon V_1 \times \cdots \times V_r \to V_1 \otimes V_2 \otimes \cdots \otimes V_r$ satisfying the following *universal property*.

UP-TP: *For any $\Bbbk$-vector space W and multilinear map $F\colon V_1 \times \cdots \times V_r \to W$, there is a unique linear transformation $F'\colon V_1 \otimes \cdots \otimes V_r \to W$ for which $F' \circ \tau = F$.*

In diagram form this becomes

$$\begin{tikzcd} V_1 \times \cdots \times V_r \arrow[rr, "\tau"] \arrow[dr, "F"'] & & V_1 \otimes \cdots \otimes V_r \arrow[dl, dotted, "\exists!\, F'"] \\ & W & \end{tikzcd}$$

where the dotted arrow represents a unique linear transformation making the diagram commute.

When $V_1 = V_2 = \cdots = V_r = V$, we call $V \otimes \cdots \otimes V$ the rth tensor power and write $\mathrm{T}^r V$.

Our next result provides an explicit description of a tensor product.

Proposition 1.17. *If the finite dimensional $\Bbbk$-vector space V_k $(1 \leqslant k \leqslant r)$ has a basis*

$$\mathbf{v}_k = \{v_{k,1}, \dots, v_{k,n_k}\}$$

where $\dim_{\Bbbk} V_k = n_k$, then $V_1 \otimes \cdots \otimes V_r$ has a basis consisting of the vectors

$$v_{1,i_1} \otimes \cdots \otimes v_{r,i_r} = \tau(v_{1,i_1}, \dots, v_{r,i_r}),$$

where $1 \leqslant i_k \leqslant n_k$. Hence we have

$$\dim_{\Bbbk} V_1 \otimes \cdots \otimes V_r = n_1 \cdots n_r.$$

More generally, for any sequence $w_1 \in V_1, \dots w_r \in V_r$, we set

$$w_1 \otimes \cdots \otimes w_r = \tau(w_1, \dots, w_r).$$

These satisfy the *multilinearity formulæ*

(MLF-1) $$w_1 \otimes \cdots \otimes w_{k-1} \otimes (w_k + w_k') \otimes w_{k+1} \otimes \cdots \otimes w_r = \\ w_1 \otimes \cdots \otimes w_k \otimes \cdots \otimes w_r + w_1 \otimes \cdots \otimes w_{k-1} \otimes w_k' \otimes w_{k+1} \otimes \cdots \otimes w_r,$$

(MLF-2) $$w_1 \otimes \cdots \otimes w_{k-1} \otimes t w_k \otimes w_{k+1} \otimes \cdots \otimes w_r = \\ t(w_1 \otimes \cdots \otimes w_{k-1} \otimes w_k \otimes w_{k+1} \otimes \cdots \otimes w_r).$$

We will see later that the tensor power $\mathrm{T}^r V$ can be decomposed as a direct sum $\mathrm{T}^r V = \mathrm{Sym}^r V \oplus \mathrm{Alt}^r V$ consisting of the *symmetric* and *antisymmetric* or *alternating* tensors $\mathrm{Sym}^r V$ and $\mathrm{Alt}^r V$.

We end with some useful results.

Proposition 1.18. *Let $V_1, \dots, V_r, V$ be finite dimensional $\Bbbk$-vector spaces. Then there is a linear isomorphism*

$$V_1^* \otimes \cdots \otimes V_r^* \cong (V_1 \otimes \cdots \otimes V_r)^*.$$

In particular,

$$\mathrm{T}^r(V^*) \cong (\mathrm{T}^r V)^*.$$

PROOF. Use the universal property to construct a linear transformation with suitable properties. $\square$

PROPOSITION 1.19. *Let V, W be finite dimensional $\Bbbk$-vector spaces. Then there is a $\Bbbk$-linear isomorphism*

$$W \otimes V^* \cong \operatorname{Hom}_{\Bbbk}(V, W)$$

under which for $\alpha \in V^*$ and $w \in W$,

$$w \otimes \alpha \longleftrightarrow w\alpha$$

where by definition, $w\alpha\colon V \to W$ is the function determined by $w\alpha(v) = \alpha(v)w$ for $v \in V$.

PROOF. The function $W \times V^* \to \operatorname{Hom}_{\Bbbk}(V, W)$ given by $(w, \alpha) \mapsto w\alpha$ is bilinear, and hence factors uniquely through a linear transformation $W \otimes V^* \to \operatorname{Hom}_{\Bbbk}(V, W)$. But for bases $\mathbf{v} = \{v_1, \ldots, v_m\}$ and $\mathbf{w} = \{w_1, \ldots, w_n\}$ of V and W, then the vectors $w_j \otimes v_i^*$ form a basis of $W \otimes V^*$. Under the above linear mapping, $w_j \otimes v_i^*$ gets sent to the function $w_j v_i^*$ which maps v_k to w_j if $k = i$ and 0 otherwise. Using Propositions 1.2 and 1.17, it is now straightforward to verify that these functions are linearly independent and span $\operatorname{Hom}_{\Bbbk}(V, W)$. $\square$

PROPOSITION 1.20. *Let $V_1, \ldots, V_r, W_1, \ldots, W_r$ be finite dimensional $\Bbbk$-vector spaces, and for each $1 \leqslant k \leqslant r$, let $\varphi_k\colon V_k \to W_k$ be a linear transformation. Then there is a unique linear transformation*

$$\varphi_1 \otimes \cdots \otimes \varphi_r\colon V_1 \otimes \cdots \otimes V_r \to W_1 \otimes \cdots \otimes W_r$$

given on each tensor $v_1 \otimes \cdots \otimes v_r$ by the formula

$$\varphi_1 \otimes \cdots \otimes \varphi_r(v_1 \otimes \cdots \otimes v_r) = \varphi_1(v_1) \otimes \cdots \otimes \varphi_1(v_r).$$

PROOF. This follows from the universal property UP-TP. $\square$

Exercises on Chapter 1

1-1. Consider the 2-dimensional $\mathbb{C}$-vector space $V = \mathbb{C}^2$. Viewing V as a 4-dimensional $\mathbb{R}$-vector space, show that

$$W = \{(z, w) \in \mathbb{C}^2 : z = -\overline{w}\}$$

is an $\mathbb{R}$-vector subspace of V. Is it a $\mathbb{C}$-vector subspace?

Show that the function $\theta\colon W \to \mathbb{C}$ given by

$$\theta(z, w) = \operatorname{Re} z + \operatorname{Im} w$$

is an $\mathbb{R}$-linear transformation. Choose $\mathbb{R}$-bases for W and $\mathbb{C}$ and determine the matrix of θ with respect to these. Use these bases to extend θ to an $\mathbb{R}$-linear transformation $\Theta\colon V \to \mathbb{C}$ agreeing with θ on W. Is there an extension which is $\mathbb{C}$-linear?

1-2. Let $V = \mathbb{C}^4$ as a $\mathbb{C}$-vector space. Suppose that $\sigma\colon V \to V$ is the function defined by

$$\sigma(z_1, z_2, z_3, z_4) = (z_3, z_4, z_1, z_2).$$

Show that σ is a $\mathbb{C}$-linear transformation. Choose a basis for V and determine the matrix of σ relative to it. Hence determine the characteristic and minimal polynomials of σ and show that there is basis for V consisting of eigenvectors of σ.

1-3. For the matrix

$$A = \begin{bmatrix} 18 & 5 & 15 \\ -6 & 5 & -9 \\ -2 & -1 & 5 \end{bmatrix}$$

show that the characteristic polynomial is $\mathrm{char}_A(X) = (X-12)(X-8)^2$ and find a basis for $\mathbb{C}^3$ consisting of eigenvectors of A. Determine the minimal polynomial of A.

1-4. For each of the $\Bbbk$-vector spaces V and subspaces W, find a linear complement W'.

(i) $\Bbbk = \mathbb{R}$, $V = \mathbb{R}^3$, $W = \{(x_1, x_2, x_3) : x_2 - 2x_3 = 0\}$;

(ii) $\Bbbk = \mathbb{R}$, $V = \mathbb{R}^4$, $W = \{(x_1, x_2, x_3, x_4) : x_2 - 2x_3 = 0 = x_1 + x_4\}$;

(iii) $\Bbbk = \mathbb{C}$, $V = \mathbb{C}^3$, $W = \{(z_1, z_2, z_3, z_4) : z_2 - iz_3 = 0 = z_1 + 4iz_4\}$.

(iv) $\Bbbk = \mathbb{R}$, $V = (\mathbb{R}^3)^*$, $W = \{\alpha : \alpha(e_3) = 0\}$.

1-5. Let V be a 2-dimensional $\mathbb{C}$-vector space with basis $\{v_1, v_2\}$. Describe a basis for the tensor square $\mathrm{T}^2 V = V \otimes V$ and state the *universal property* for the natural function $\tau \colon V \times V \to \mathrm{T}^2 V$.

Let $F \colon V \times V \to \mathbb{C}$ be a non-constant $\mathbb{C}$-bilinear function for which

$$F(v, u) = -F(u, v) \quad (u, v \in V)$$

(Such a function is called *alternating* or *odd*.) Show that F factors through a linear transformation $F' \colon \mathrm{T}^2 V \to \mathbb{C}$ and find $\ker F'$.

If $G \colon V \times V \to \mathbb{C}$ is a second such function, show that there is a $t \in \mathbb{C}$ for which $G(u, v) = tF(u, v)$ for all $u, v \in V$.

1-6. Let V be a finite dimensional $\Bbbk$-vector space where $\mathrm{char}\, \Bbbk = 0$ (e.g., $\Bbbk = \mathbb{Q}, \mathbb{R}, \mathbb{C}$) and $\dim_{\Bbbk} V = n$ where n is even.

Let $F \colon V \times V \to \Bbbk$ be an alternating $\Bbbk$-bilinear function which is *non-degenerate* in the sense that for each $v \in V$, there is a $w \in V$ such that $F(v, w) \neq 0$.

Show that there is a basis $\{v_1, \ldots, v_n\}$ for V for which

$$F(v_{2r-1}, v_{2r}) = -F(v_{2r}, v_{2r-1}) = 1, \quad (r = 1, \ldots, n/2),$$
$$F(v_i, v_j) = 0, \quad \text{whenever } |i - j| \neq 1.$$

[Hint: *Try using induction on $m = n/2$, starting with $m = 1$.*]

CHAPTER 2

Representations of finite groups

2.1. Linear representations

In discussing representations, we will be mainly interested in the situations where $\Bbbk = \mathbb{R}$ or $\Bbbk = \mathbb{C}$. However, other cases are important and unless we specifically state otherwise we will usually assume that $\Bbbk$ is an arbitrary field of characteristic 0. For fields of finite characteristic dividing the order of the group, Representation Theory becomes more subtle and the resulting theory is called *Modular Representation Theory.* Another important property of the field $\Bbbk$ required in many situations is that it is *algebraically closed* in the sense that every polynomial over $\Bbbk$ has a root in $\Bbbk$; this is true for $\mathbb{C}$ but not for $\mathbb{R}$, however, the latter case is important in many applications of the theory. Throughout this section, G will denote a finite group.

A homomorphism of groups $\rho\colon G \to \mathrm{GL}_{\Bbbk}(V)$ defines a $\Bbbk$-*linear action* of G on V by

$$g \cdot v = \rho_g v = \rho(g)(v),$$

which we call a $\Bbbk$-*representation* or $\Bbbk$-*linear representation* of G in (or on) V. Sometimes V together with ρ is called a G-*module*, although we will not use that terminology. The case where $\rho(g) = \mathrm{Id}_V$ is called the *trivial representation in* V. Notice that we have the following identities:

(Rep-1) $$(hg) \cdot v = \rho_{hg} v = \rho_h \circ \rho_g v = h \cdot (g \cdot v) \quad (h, g \in G,\ v \in V),$$

(Rep-2) $$g \cdot (v_1 + v_2) = \rho_g(v_1 + v_2) = \rho_g v_1 + \rho_g v_2 = g \cdot v_1 + g \cdot v_2 \quad (g \in G,\ v_i \in V),$$

(Rep-3) $$g \cdot (tv) = \rho_g(tv) = t\rho_g(v) = t(g \cdot v) \quad (g \in G,\ v \in V,\ t \in \Bbbk).$$

A vector subspace W of V which is closed under the action of elements of G is called a G-*submodule* or G-*subspace;* we sometimes say that W is *stable* under the action of G. It is usual to view W as being a representation in its own right, using the 'restriction' $\rho_{|_W} : G \to \mathrm{GL}_{\Bbbk}(W)$ defined by

$$\rho_{|_W}(g)(w) = \rho_g(w).$$

The pair consisting of W and $\rho_{|_W}$ is called a *subrepresentation* of the original representation.

Given a basis $\mathbf{v} = \{v_1, \ldots, v_n\}$ for V with $\dim_{\Bbbk} V = n$, for each $g \in G$ we have the associated matrix of $\rho(g)$ relative to $\mathbf{v}$, $[r_{ij}(g)]$ which is defined by

(Rep-Mat) $$\rho_g v_j = \sum_{k=1}^{n} r_{kj}(g) v_k.$$

EXAMPLE 2.1. Let $\rho\colon G \to \mathrm{GL}_{\Bbbk}(V)$ where $\dim_{\Bbbk} V = 1$. Given any non-zero element $v \in V$ (which forms a basis for V) we have for each $g \in G$ a $\lambda_g \in \Bbbk$ satisfying $g \cdot v = \lambda_g v$. By Equation (Rep-1), for $g, h \in G$ we have

$$\lambda_{hg} v = \lambda_h \lambda_g v,$$

and hence

$$\lambda_{hg} = \lambda_h \lambda_g.$$

From this it is easy to see that $\lambda_g \neq 0$. Thus there is a homomorphism $\Lambda\colon G \to \Bbbk^\times$ given by

$$\Lambda(g) = \lambda_g.$$

Although this appears to depend on the choice of v, in fact it is independent of it (we leave this as an exercise). As G is finite, every element $g \in G$ has a finite order $|g|$, and it easily follows that

$$\lambda_g^{|g|} = 1,$$

so λ_g is a $|g|$-th root of unity. Hence, given a 1-dimensional representation of a group, we can regard it as equivalent to such a homomorphism $G \to \Bbbk^\times$.

Here are two illustrations of Example 2.1.

EXAMPLE 2.2. Take $\Bbbk = \mathbb{R}$. Then the only roots of unity in $\mathbb{R}$ are ± 1, hence we can assume that for a 1-dimensional representation over $\mathbb{R}$, $\Lambda\colon G \to \{1, -1\}$, where the codomain is a group under multiplication. The sign function $\operatorname{sign}\colon S_n \to \{1, -1\}$ provides an interesting and important example of this.

EXAMPLE 2.3. Now take $\Bbbk = \mathbb{C}$. Then for each $n \in \mathbb{N}$ we have n distinct n-th roots of unity in $\mathbb{C}^\times$. We will denote the set of all n-th roots of unity by μ_n, and the set of all roots of unity by

$$\mu_\infty = \bigcup_{n \in \mathbb{N}} \mu_n,$$

where we use the inclusions $\mu_m \subseteq \mu_n$ whenever $m \mid n$. These are abelian groups under multiplication.

Given a 1-dimensional representation over $\mathbb{C}$, the function Λ can be viewed as a homomorphism $\Lambda\colon G \to \mu_\infty$, or even $\Lambda\colon G \to \mu_{|G|}$ by Lagrange's Theorem.

For example, if $G = C$ is cyclic of order N say, then we must have for any 1-dimensional representation of C that $\Lambda\colon C \to \mu_N$. Note that there are exactly N of such homomorphisms.

EXAMPLE 2.4. Let G be a simple group which is not abelian. Then given a 1-dimensional representation $\rho\colon G \to \mathrm{GL}_\Bbbk(V)$ of G, the associated homomorphism $\Lambda\colon G \to \mu_{|G|}$ has abelian image, hence $\ker \Lambda$ has to be bigger than $\{e_G\}$. Since G has no proper normal subgroups, we must have $\ker \Lambda = G$. Hence, $\rho(g) = \mathrm{Id}_V$.

Indeed, for any representation $\rho\colon G \to \mathrm{GL}_\Bbbk(V)$ we have $\ker \rho = G$ or $\ker \rho = \{e_G\}$. Hence, either the representation is trivial or ρ is an injective homomorphism, which therefore embeds G into $\mathrm{GL}_\Bbbk(V)$. This severely restricts the smallest dimension of non-trivial representations of non-abelian simple groups.

EXAMPLE 2.5. Let $G = \{e, \tau\} \cong \mathbb{Z}/2$ and let V be any representation over any field not of characteristic 2. Then there are $\Bbbk$-vector subspaces V_+, V_- of V for which $V = V_+ \oplus V_-$ and the action of G is given by

$$\tau \cdot v = \begin{cases} v & \text{if } v \in V_+, \\ -v & \text{if } v \in V_-. \end{cases}$$

PROOF. Define linear transformations $\varepsilon_+, \varepsilon_- \colon V \to V$ by

$$\varepsilon_+(v) = \frac{1}{2}(v + \tau \cdot v), \quad \varepsilon_-(v) = \frac{1}{2}(v - \tau \cdot v).$$

It is easily verified that

$$\varepsilon_+(\tau \cdot v) = \varepsilon_+(v), \quad \varepsilon_-(\tau \cdot v) = -\varepsilon_-(v).$$

We take $V_+ = \operatorname{im} \varepsilon_+$ and $V_- = \operatorname{im} \varepsilon_-$ and the direct sum decomposition follows from the identity

$$v = \varepsilon_+(v) + \varepsilon_-(v). \qquad \square$$

The decomposition in this example corresponds to the two distinct irreducible representations of $\mathbb{Z}/2$. Later we will see (at least over the complex numbers $\mathbb{C}$) that there is always such a decomposition of a representation of a finite group G with factors corresponding to the distinct irreducible representations of G.

EXAMPLE 2.6. Let D_{2n} be the dihedral group of order $2n$ described in Section A.7.2. This group is generated by elements α of order n and β of order 2, subject to the relation

$$\beta\alpha\beta = \alpha^{-1}.$$

We can realise D_{2n} as the symmetry group of the regular n-gon centred at the origin and with vertices on the unit circle (we take the first vertex to be $(1, 0)$). It is easily checked that relative the standard basis $\{e_1, e_2\}$ of $\mathbb{R}^2$, we get

$$\alpha^r = \begin{bmatrix} \cos 2r\pi/n & -\sin 2r\pi/n \\ \sin 2r\pi/n & \cos 2r\pi/n \end{bmatrix} \qquad \beta\alpha^r = \begin{bmatrix} \cos 2r\pi/n & -\sin 2r\pi/n \\ -\sin 2r\pi/n & -\cos 2r\pi/n \end{bmatrix}$$

for $r = 0, \ldots, (n - 1)$.

Thus we have a 2-dimensional representation $\rho^{\mathbb{R}}$ of D_{2n} over $\mathbb{R}$, where the matrices of $\rho^{\mathbb{R}}(\alpha^r)$ and $\rho^{\mathbb{R}}(\beta\alpha^r)$ are given by the above. We can also view $\mathbb{R}^2$ as a subset of $\mathbb{C}^2$ and interpret these matrices as having coefficients in $\mathbb{C}$. Thus we obtain a 2-dimensional complex representation $\rho^{\mathbb{C}}$ of D_{2n} with the above matrices relative to the $\mathbb{C}$-basis $\{e_1, e_2\}$.

2.2. G-homomorphisms and irreducible representations

Suppose that we have two representations $\rho\colon G \to \mathrm{GL}_{\Bbbk}(V)$ and $\sigma\colon G \to \mathrm{GL}_{\Bbbk}(W)$. Then a linear transformation $f\colon V \to W$ is called *G-equivariant*, *G-linear* or a *G-homomorphism* with respect to ρ and σ, if for each $g \in G$ the diagram

$$\begin{tikzcd} V \arrow[r, "f"] \arrow[d, "\rho_g"'] & W \arrow[d, "\sigma_g"] \\ V \arrow[r, "f"] & W \end{tikzcd}$$

commutes, i.e., $\sigma_g \circ f = f \circ \rho_g$ or equivalently, $\sigma_g \circ f \circ \rho_{g^{-1}} = f$. A G-homomorphism which is a linear isomorphism is called a *G-isomorphism* or *G-equivalence* and we say that the representations are *G-isomorphic* or *G-equivalent.*

We define an action of G on $\mathrm{Hom}_{\Bbbk}(V, W)$, the vector space of $\Bbbk$-linear transformations $V \to W$, by

$$(g \cdot f)(v) = \sigma_g f(\rho_{g^{-1}} v) \quad (f \in \mathrm{Hom}_{\Bbbk}(V, W)).$$

This is another G-representation. The G-invariant subspace $\mathrm{Hom}_G(V,W) = \mathrm{Hom}_{\Bbbk}(V,W)^G$ is then equal to the set of all G-homomorphisms.

If the only G-subspaces of V are $\{0\}$ and V, ρ is called *irreducible* or *simple*.

Given a subrepresentation $W \subseteq V$, the quotient vector space V/W also admits a linear action of G, $\overline{\rho}_W : G \to \mathrm{GL}_{\Bbbk}(V/W)$, the *quotient representation*, where

$$\overline{\rho}_W(g)(v+W) = \rho(g)(v) + W,$$

which is well defined since whenever $v' - v \in W$,

$$\rho(g)(v') + W = \rho(g)(v + (v'-v)) + W = \big(\rho(g)(v) + \rho(g)(v'-v)\big) + W = \rho(g)(v) + W.$$

Proposition 2.7. *If $f\colon V \to W$ is a G-homomorphism, then*

(a) $\ker f$ *is a G-subspace of V;*

(b) $\operatorname{im} f$ *is a G-subspace of W.*

Proof. (a) Let $v \in \ker f$. Then for $g \in G$,

$$f(\rho_g v) = \sigma_g f(v) = 0,$$

so $\rho_g v \in \ker f$. Hence $\ker f$ is a G-subspace of V

(b) Let $w \in \operatorname{im} f$ with $w = f(u)$ for some $u \in V$. Now

$$\sigma_g w = \sigma_g f(u) = f(\rho_g u) \in \operatorname{im} f,$$

hence $\operatorname{im} f$ is a G-subspace of W. □

Theorem 2.8 (**Schur's Lemma**). *Let $\rho\colon G \to \mathrm{GL}_{\mathbb{C}}(V)$ and $\sigma\colon G \to \mathrm{GL}_{\mathbb{C}}(W)$ be irreducible representations of G over the field $\mathbb{C}$, and let $f\colon V \to W$ be a G-linear map.*

(a) *If f is not the zero map, then f is an isomorphism.*

(b) *If $V = W$ and $\rho = \sigma$, then for some $\lambda \in \mathbb{C}$, f is given by*

$$f(v) = \lambda v \quad (v \in V).$$

Remark 2.9. Part (a) is true for any field $\Bbbk$ in place of $\mathbb{C}$. Part (b) is true for any algebraically closed field in place of $\mathbb{C}$.

Proof. (a) Proposition 2.7 implies that $\ker f \subseteq V$ and $\operatorname{im} f \subseteq W$ are G-subspaces. By the irreducibility of V, either $\ker f = V$ (in which case f is the zero map) or $\ker f = \{0\}$ in which case f is injective. Similarly, irreducibility of W implies that $\operatorname{im} f = \{0\}$ (in which case f is the zero map) or $\operatorname{im} f = W$ in which case f is surjective. Thus if f is not the zero map it must be an isomorphism.

(b) Let $\lambda \in \mathbb{C}$ be an eigenvalue of f, with eigenvector $v_0 \neq 0$. Let $f_\lambda\colon V \to V$ be the linear transformation for which

$$f_\lambda(v) = f(v) - \lambda v \quad (v \in V).$$

For each $g \in G$,

$$\begin{aligned} \rho_g f_\lambda(v) &= \rho_g f(v) - \rho_g \lambda v \\ &= f(\rho_g v) - \lambda \rho_g v, \\ &= f_\lambda(\rho_g v), \end{aligned}$$

showing that f_λ is G-linear. Since $f_\lambda(v_0) = 0$, Proposition 2.7 shows that $\ker f_\lambda = V$. As

$$\dim_{\mathbb{C}} V = \dim_{\mathbb{C}} \ker f_\lambda + \dim_{\mathbb{C}} \operatorname{im} f_\lambda,$$

we see that $\operatorname{im} f_\lambda = \{0\}$ and so

$$f_\lambda(v) = 0 \quad (v \in V). \qquad \square$$

A linear transformation $f\colon V \to V$ is sometimes called a *homothety* if it has the form

$$f(v) = \lambda v \quad (v \in V).$$

In this proof, it is essential that we take $\Bbbk = \mathbb{C}$ rather than $\Bbbk = \mathbb{R}$ for example, since we need the fact that every polynomial over $\mathbb{C}$ has a root to guarantee that linear transformations $V \to V$ always have eigenvalues. This theorem can fail to hold for representations over $\mathbb{R}$ as the next example shows.

Example 2.10. Let $\Bbbk = \mathbb{R}$ and $V = \mathbb{C}$ considered as a 2-dimensional $\mathbb{R}$-vector space. Let

$$G = \mu_4 = \{1, -1, i, -i\}$$

be the group of all 4th roots of unity with $\rho\colon \mu_4 \to \mathrm{GL}_{\Bbbk}(V)$ given by

$$\rho_\alpha z = \alpha z.$$

Then this defines a 2-dimensional representation of G over $\mathbb{R}$. If we use the basis $\{u = 1, v = i\}$, then

$$\rho_i u = v, \quad \rho_i v = -u.$$

From this we see that any G-subspace of V containing a non-zero element $w = au + bv$ also contains $-bu + av$, and hence it must be all of V (exercise). So V is irreducible.

But the linear transformation $\varphi\colon V \to V$ given by

$$\varphi(au + bv) = -bu + av = \rho_i(au + bv)$$

is G-linear, but not the same as multiplication by a real number (this is left as an exercise).

We will give a version of Schur's Lemma which does not assume the field $\Bbbk$ is algebraically closed. First we recall some notation. Let D be a ring which has a ring homomorphism $\eta\colon \Bbbk \to D$ such that for all $t \in \Bbbk$ and $x \in D$,

$$\eta(t)x = x\eta(t).$$

Since η is injective, we identify $\Bbbk$ with a subring of D and take η to be the inclusion function. Taking scalar multiplication to be $t \cdot x = tx$, D becomes a $\Bbbk$-vector space. If D is a finite dimensional and every non-zero element $x \in D$ is invertible, then D is called a $\Bbbk$-*division algebra*; if $\Bbbk$ is the centre of D, then D is called a $\Bbbk$-*central division algebra*. When $\Bbbk = \mathbb{R}$, then up to isomorphism, the only $\mathbb{R}$-division algebras are $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{H}$ (the quaternions, of dimension 4). Over an algebraically closed field things are simpler.

Proposition 2.11. *$\Bbbk$ is algebraically closed then the only $\Bbbk$-central division algebra is $\Bbbk$.*

Proof. Suppose that D is a $\Bbbk$-central division algebra. Let $z \in D$ be a non-zero element. Multiplication by z gives a $\Bbbk$-linear transformation $\tau_z\colon D \to D$. By the usual theory of eigenvalues over an algebraically closed field, τ_z has an eigenvalue λ say, with eigenvector $v \in D$, i.e., $v \neq 0$ and

$$(\lambda - z)v = 0.$$

Multiplying by v^{-1} gives $(\lambda - z) = 0$, hence $z = \lambda \in \Bbbk$. $\square$

The next result is proved in a similar way to Part (a) of Schur's Lemma 2.8.

THEOREM 2.12 (**Schur's Lemma: general version**). *Let $\Bbbk$ be a field and G a finite group. Let $\rho\colon G \to \mathrm{GL}_{\Bbbk}(W)$ be an irreducible $\Bbbk$-representation. Then $\mathrm{Hom}_G(W, W)$ is a $\Bbbk$-division algebra.*

The next result is also valid for all fields in which $|G|$ is invertible.

THEOREM 2.13 (**Maschke's Theorem**). *Let V be a $\Bbbk$-vector space and $\rho\colon G \to \mathrm{GL}_{\Bbbk}(V)$ a $\Bbbk$-representation. Let $W \subseteq V$ be a G-subspace of V. Then there is a projection onto W which is G-equivariant. Equivalently, there is a linear complement W' of W which is also a G-subspace.*

PROOF. Let $p\colon V \to V$ be a projection onto W. Define a linear transformation $p_0\colon V \to V$ by

$$p_0(v) = \frac{1}{|G|}\sum_{g\in G} \rho_g \circ p \circ \rho_g^{-1}(v).$$

Then for $v \in V$,

$$\rho_g \circ p \circ \rho_g^{-1}(v) \in W$$

since $\operatorname{im} p = W$ and W is a G-subspace; hence $p_0(v) \in W$. We also have

$$\begin{aligned}
p_0(\rho_g v) &= \frac{1}{|G|}\sum_{h\in G} \rho_h p(\rho_h^{-1}\rho_g v) \\
&= \frac{1}{|G|}\sum_{h\in G} \rho_g\rho_{g^{-1}h} p(\rho_{g^{-1}h}^{-1} v) \\
&= \rho_g \left(\frac{1}{|G|}\sum_{h\in G} \rho_{g^{-1}h} p(\rho_{g^{-1}h}^{-1} v)\right) \\
&= \rho_g \left(\frac{1}{|G|}\sum_{h\in G} \rho_h p(\rho_{h^{-1}} v)\right) \\
&= \rho_g p_0(v),
\end{aligned}$$

which shows that p_0 is G-equivariant. If $w \in W$,

$$\begin{aligned}
p_0(w) &= \frac{1}{|G|}\sum_{g\in G} \rho_g p(\rho_{g^{-1}} w) \\
&= \frac{1}{|G|}\sum_{g\in G} \rho_g \rho_{g^{-1}} w \\
&= \frac{1}{|G|}\sum_{g\in G} w \\
&= \frac{1}{|G|}(|G|\, w) = w.
\end{aligned}$$

Hence $p_0{}_{|W} = \mathrm{Id}_W$, showing that p_0 has image W.

Now consider $W' = \ker p_0$, which is a G-subspace by part (a) of Proposition 2.7. This is a linear complement for W since given the quotient map $q\colon V \to V/W$, if $v \in W'$ then $q(v) = 0 + W$ implies $v \in W \cap W'$ and hence $0 = p_0(v) = v$. $\square$

THEOREM 2.14. *Let $\rho\colon G \to \mathrm{GL}_{\Bbbk}(V)$ be a linear representation of a finite group with V non-trivial. Then there are G-spaces $U_1, \ldots, U_r \subseteq V$, each of which is a non-trivial irreducible subrepresentation and*

$$V = U_1 \oplus \cdots \oplus U_r.$$

PROOF. We proceed by Induction on $n = \dim_{\Bbbk} V$. If $n = 1$, the result is true with $U_1 = V$.

So assume that the result holds whenever $\dim_{\Bbbk} V < n$. Now either V is irreducible or there is a proper G-subspace $U_1 \subseteq V$. By Theorem 2.13, there is a G-complement U_1' of U_1 in V with $\dim_{\Bbbk} U_1' < n$. By the Inductive Hypothesis there are irreducible G-subspaces $U_2, \ldots, U_r \subseteq U_1' \subseteq V$ for which

$$U_1' = U_2 \oplus \cdots \oplus U_r,$$

and so we find

$$V = U_1 \oplus U_2 \oplus \cdots \oplus U_r. \qquad \square$$

We will see later that given any two such collections of non-trivial irreducible subrepresentations $U_1, \ldots, U_r$ and $W_1, \ldots, W_s$, we have $s = r$ and for each k, the number of W_j G-isomorphic to U_k is equal to the number of U_j G-isomorphic to U_k. The proof of this will use *characters*, which give further information such as the *multiplicity* of each irreducible which occurs as a summand in V. The irreducible representations U_k are called the *irreducible factors* or *summands* of the representation V.

An important example of a G-subspace of any representation ρ on V is the *G-invariant* subspace

$$V^G = \{v \in V : \rho_g v = v \ \forall g \in G\}.$$

We can construct a projection map $V \to V^G$ which is G-linear, *provided that the characteristic of $\Bbbk$ does not divide $|G|$*. In practice, we will be mainly interested in the case where $\Bbbk = \mathbb{C}$, so in this section from now on, we will assume that $\Bbbk$ has characteristic 0.

PROPOSITION 2.15. *Let $\varepsilon\colon V \to V$ be the $\Bbbk$-linear transformation defined by*

$$\varepsilon(v) = \frac{1}{|G|} \sum_{g \in G} \rho_g v.$$

Then

(a) *For $g \in G$ and $v \in V$, $\rho_g \varepsilon(v) = \varepsilon(v)$;*
(b) *ε is G-linear;*
(c) *for $v \in V^G$, $\varepsilon(v) = v$ and so $\operatorname{im} \varepsilon = V^G$.*

PROOF. (a) Let $g \in G$ and $v \in V$. Then

$$\rho_g \varepsilon(v) = \rho_g \left(\frac{1}{|G|} \sum_{h \in G} \rho_h v \right) = \frac{1}{|G|} \sum_{h \in G} \rho_g \rho_h v = \frac{1}{|G|} \sum_{h \in G} \rho_{gh} v = \frac{1}{|G|} \sum_{h \in G} \rho_h v = \varepsilon(v).$$

(b) Similarly, for $g \in G$ and $v \in V$,

$$\varepsilon(\rho_g v) = \frac{1}{|G|} \sum_{h \in G} \rho_h(\rho_g v) = \frac{1}{|G|} \sum_{h \in G} \rho_{hg} v = \frac{1}{|G|} \sum_{k \in G} \rho_k v = \varepsilon(v).$$

By (a), this agrees with $\rho_g\varepsilon(v)$. Hence, ε is G-linear.
(c) For $v \in V^G$,

$$\varepsilon(v) = \frac{1}{|G|}\sum_{g\in G}\rho_g v = \frac{1}{|G|}\sum_{g\in G} v = \frac{1}{|G|}|G|v = v.$$

Notice that this also shows that $\operatorname{im}\varepsilon = V^G$. $\square$

2.3. New representations from old

Let G be a finite group and $\Bbbk$ a field. In this section we will see how new representations can be manufactured from existing ones. As well as allowing interesting new examples to be constructed, this sometimes gives ways of understanding representations in terms of familiar ones. This will be important when we have learnt how to decompose representations in terms of irreducibles and indeed is sometimes used to construct the latter.

Let $V_1, \dots, V_r$ be $\Bbbk$-vector spaces admitting representations $\rho_1, \dots, \rho_r$ of G. Then for each $g \in G$ and each j, we have the corresponding linear transformation ${\rho_j}_g \colon V_j \to V_j$. By Proposition 1.20 there is a unique linear transformation

$${\rho_1}_g \otimes \cdots \otimes {\rho_r}_g \colon V_1 \otimes \cdots \otimes V_r \to V_1 \otimes \cdots \otimes V_r.$$

It is easy to verify that this gives a representation of G on the tensor product $V_1 \otimes \cdots \otimes V_r$, called the *tensor product* of the original representations. By Proposition 1.20 we have the formula

$$(2.1) \qquad {\rho_1}_g \otimes \cdots \otimes {\rho_r}_g(v_1 \otimes \cdots \otimes v_r) = {\rho_1}_g v_1 \otimes \cdots \otimes {\rho_r}_g v_r$$

for $v_j \in V_j$ $(j = 1, \dots, r)$.

Let V, W be $\Bbbk$-vector spaces supporting representations $\rho \colon G \to \mathrm{GL}_\Bbbk(V)$ and $\sigma \colon G \to \mathrm{GL}_\Bbbk(W)$. Recall that $\mathrm{Hom}_\Bbbk(V, W)$ is the set of all linear transformations $V \to W$ which is a $\Bbbk$-vector space whose addition and multiplication are given by the following formulæ for $\varphi, \theta \in \mathrm{Hom}_\Bbbk(V, W)$ and $t \in \Bbbk$:

$$(\varphi + \theta)(u) = \varphi(u) + \theta(u),$$
$$(t\varphi)(u) = t(\varphi(u)) = \varphi(tu).$$

There is an action of G on $\mathrm{Hom}_\Bbbk(V, W)$ defined by

$$(\tau_g\varphi)(u) = \sigma_g\varphi(\rho_{g^{-1}}u).$$

This turns out to be a linear representation of G on $\mathrm{Hom}_\Bbbk(V, W)$.

As a particular example of this, taking $W = \Bbbk$ with the trivial action of G (i.e., $\sigma_g = \mathrm{Id}_\Bbbk$), we obtain an action of G on the dual of V,

$$V^* = \mathrm{Hom}_\Bbbk(V, \Bbbk).$$

This action determines the *contragredient representation* ρ^*. Explicitly, this satisfies

$$\rho^*_g\varphi = \varphi \circ \rho_{g^{-1}}.$$

PROPOSITION 2.16. *Let $\rho \colon G \to \mathrm{GL}_\Bbbk(V)$ be a representation, and $\mathbf{v} = \{v_1, \dots, v_n\}$ be a basis of V. Suppose that relative to $\mathbf{v}$,*

$$[\rho_g]_{\mathbf{v}} = [r_{ij}(g)] \quad (g \in G).$$

Then relative to the dual basis $\mathbf{v}^* = \{v_1^*, \dots, v_n^*\}$*, we have*

$$[\rho_g^*]_{\mathbf{v}^*} = [r_{ji}(g^{-1})] \quad (g \in G),$$

or equivalently,

$$[\rho_g^*]_{\mathbf{v}^*} = [\rho_{g^{-1}}]^T.$$

Proof. If we write

$$[\rho_g^*]_{\mathbf{v}^*} = [t_{ij}(g)],$$

then by definition,

$$\rho_g^* v_s^* = \sum_{r=1}^n t_{rs}(g) v_r^*.$$

Now for each $i = 1, \dots, n$,

$$(\rho_g^* v_j^*)(v_i) = \sum_{r=1}^n t_{rj}(g) v_r^*(v_i),$$

which gives

$$v_j^*(\rho_{g^{-1}} v_i) = t_{ij}(g),$$

and hence

$$t_{ij}(g) = v_j^*(\sum_{k=1}^n r_{ki}(g^{-1}) v_i) = r_{ji}(g^{-1}). \qquad \square$$

Another perspective on the above is provided by the next result, whose proof is left as an exercise.

Proposition 2.17. *The* $\Bbbk$*-linear isomorphism*

$$\mathrm{Hom}_{\Bbbk}(V, W) \cong W \underset{\Bbbk}{\otimes} V^*$$

is a G*-isomorphism where the right hand side carries the tensor product representation* $\sigma \otimes \rho^*$*.*

Using these ideas together with Proposition 2.15 we obtain the following useful result

Proposition 2.18. *For* $\Bbbk$ *of characteristic* 0*, the* G*-homomorphism*

$$\varepsilon\colon\ \mathrm{Hom}_{\Bbbk}(V, W) \to \mathrm{Hom}_{\Bbbk}(V, W)$$

of Proposition 2.15 has image equal to the set of G*-homomorphisms* $V \to W$*,* $\mathrm{Hom}_{\Bbbk}(V, W)^G$ *which is also* G*-isomorphic to* $(W \otimes_{\Bbbk} V^*)^G$*.*

Now let $\rho\colon G \to \mathrm{GL}_{\Bbbk}(V)$ be a representation of G and let $H \leqslant G$. We can restrict ρ to H and obtain a representation $\rho_{|_H}\colon H \to \mathrm{GL}_{\Bbbk}(V)$ of H, usually denoted $\rho \downarrow_H^G$ or $\mathrm{res}_H^G \rho$; the H-module V is also denoted $V \downarrow_H^G$ or $\mathrm{res}_H^G V$.

Similarly, if $G \leqslant K$, then we can form the *induced representation* $\rho \uparrow_G^K\colon K \to \mathrm{GL}_{\Bbbk}(V \uparrow_G^K)$ as follows. Take K_R to be the G-set consisting of the underlying set of K with the G-action

$$g \cdot x = xg^{-1}.$$

Define

$$V \uparrow_G^K = \mathrm{ind}_G^K V = \mathrm{Map}(K_R, V)^G = \{f\colon K \to V : f(x) = \rho_g f(xg)\ \forall x \in K\}.$$

Then K acts linearly on $V \uparrow_G^K$ by

$$(k \cdot f)(x) = f(kx),$$

and so we obtain a linear representation of K. The induced representation is often denoted $\rho\uparrow_G^K$ or $\operatorname{ind}_G^K \rho$. The dimension of $V\uparrow_G^K$ is $\dim_{\Bbbk} V\uparrow_G^K = |K/G| \dim_{\Bbbk} V$. Later we will meet *Reciprocity Laws* relating these induction and restriction operations.

2.4. Permutation representations

Let G be a finite group and X a finite G-set, i.e., a finite set X equipped with an action of G on X, written gx. A finite dimensional G-representation $\rho\colon G \to \mathrm{GL}_{\mathbb{C}}(V)$ over $\Bbbk$ is a *permutation representation on* X if there is an injective G-map $j\colon X \to V$ and $\operatorname{im} j = j(X) \subseteq V$ is a $\Bbbk$-basis for V. Notice that a permutation representation really depends on the injection j. We frequently have situations where $X \subseteq V$ and j is the inclusion of the subset X. The condition that j be a G-map amounts to the requirement that

$$\rho_g(j(x)) = j(gx) \quad (g \in G,\, x \in X).$$

DEFINITION 2.19. A *homomorphism* from a permutation representation $j_1\colon X_1 \to V_1$ to a second $j_2\colon X_2 \to V_2$ is a G-linear transformation $\Phi\colon V_1 \to V_2$ such that

$$\Phi(j_1(x)) \in \operatorname{im} j_2 \quad (x \in X_1).$$

A G-homomorphism of permutation representations which is a G-isomorphism is called a G-*isomorphism* of permutation representations.

Notice that by the injectivity of j_2, this implies the existence of a unique G-map $\varphi\colon X_1 \to X_2$ for which

$$j_2(\varphi(x)) = \Phi(j_1(x)) \quad (x \in X_1).$$

Equivalently, we could specify the G-map $\varphi\colon X_1 \to X_2$ and then $\Phi\colon V_1 \to V_2$ would be the unique linear extension of φ restricted to $\operatorname{im} j_2$ (see Proposition 1.1). In the case where Φ is a G-isomorphism, it is easily verified that $\varphi\colon X_1 \to X_2$ is a G-equivalence.

To show that such permutations representations exist in abundance, we proceed as follows. Let X be a finite set equipped with a G-action. Let $\Bbbk[X] = \operatorname{Map}(X, \Bbbk)$, the set of all functions $X \to \Bbbk$. This is a finite dimensional $\Bbbk$-vector space with addition and scalar multiplication defined by

$$(f_1 + f_2)(x) = f_1(x) + f_2(x), \quad (tf)(x) = t(f(x)),$$

for $f_1, f_2, f \in \operatorname{Map}(X, \Bbbk)$, $t \in \Bbbk$ and $x \in X$. There is an action of G on $\operatorname{Map}(X, \Bbbk)$ given by

$$(g \cdot f)(x) = f(g^{-1}x).$$

If Y is a second finite G-set, and $\varphi\colon X \to Y$ a G-map, then we define the *induced function* $\varphi_*\colon \Bbbk[X] \to \Bbbk[Y]$ by

$$(\varphi_* f)(y) = \sum_{x \in \varphi^{-1}\{y\}} f(x) = \sum_{\varphi(x)=y} f(x).$$

THEOREM 2.20. *Let G be a finite group.*

(a) *For a finite G-set X, $\Bbbk[X]$ is a finite dimensional permutation representation of dimension* $\dim_{\Bbbk} \Bbbk[X] = |X|$.
(b) *For a G-map $\varphi\colon X \to Y$, the induced function $\varphi_*\colon \Bbbk[X] \to \Bbbk[Y]$ is a G-linear transformation.*

PROOF.
a) For each $x \in X$ we have a function $\delta_x \colon X \to \Bbbk$ given by

$$\delta_x(y) = \begin{cases} 1 & \text{if } y = x, \\ 0 & \text{otherwise.} \end{cases}$$

The map $j \colon X \to \Bbbk[X]$ given by

$$j(x) = \delta_x$$

is easily seen to be an injection. It is also a G-map, since

$$\delta_{gx}(y) = 1 \iff \delta_x(g^{-1}y) = 1,$$

and hence

$$j(gx)(y) = \delta_{gx}(y) = \delta_x(g^{-1}y) = (g \cdot \delta_x)(y).$$

Given a function $f \colon X \to \Bbbk$, consider

$$f - \sum_{x \in X} f(x)\delta_x \in \Bbbk[X].$$

Then for $y \in X$,

$$f(y) - \sum_{x \in X} f(x)\delta_x(y) = f(y) - f(y) = 0,$$

hence $f - \sum_{x \in X} f(x)\delta_x$ is the constant function taking the value 0 on X. So the functions δ_x ($x \in X$) span $\Bbbk[X]$. They are also linearly independent, since if the 0 valued constant function is expressed in the form

$$\sum_{x \in X} t_x \delta_x$$

for some $t_x \in \Bbbk$, then for each $y \in X$,

$$0 = \sum_{x \in X} t_x \delta_x(y) = t_y,$$

hence all the coefficients t_x must be 0.
b) The $\Bbbk$-linearity of φ_* is easily checked. To show it is a G-map, for $g \in G$,

$$\begin{aligned} (g \cdot \varphi_* f)(y) &= (\varphi_* f)(g^{-1}y) \\ &= \sum_{x \in \varphi^{-1}\{g^{-1}y\}} f(x) \\ &= \sum_{x \in \varphi^{-1}\{y\}} f(g^{-1}x), \end{aligned}$$

since

$$\begin{aligned} \varphi^{-1}\{g^{-1}y\} &= \{x \in X : g\varphi(x) = y\} \\ &= \{x \in X : \varphi(gx) = y\} \\ &= \{g^{-1}x : x \in X,\ x \in \varphi^{-1}\{y\}\}. \end{aligned}$$

Since by definition

$$(g \cdot f)(x) = f(g^{-1}x),$$

we have

$$(g \cdot \varphi_* f) = \varphi_*(g \cdot f). \qquad \square$$

Given a permutation representation $\Bbbk[X]$, we will often use the injection j to identify X with a subset of $\Bbbk[X]$. If $\varphi\colon X \to Y$ is a G-map, notice that

$$\varphi_*(\sum_{x\in X} t_x\delta_x) = \sum_{x\in X} t_x\delta_{\varphi(x)}.$$

We will sometimes write x instead of δ_x, and a typical element of $\Bbbk[X]$ as $\sum_{x\in X} t_x x$, where each $t_x \in \Bbbk$, rather than $\sum_{x\in X} t_x\delta_x$. Another convenient notational device is to list the elements of X as $x_1, x_2, \dots, x_n$ and then identify $\mathbf{n} = \{1, 2, \dots, n\}$ with X via the correspondence $k \longleftrightarrow x_k$. Then we can identify $\Bbbk[\mathbf{n}] \cong \Bbbk^n$ with $\Bbbk[X]$ using the correspondence

$$(t_1, t_2, \dots, t_n) \longleftrightarrow \sum_{k=1}^{n} t_k x_k.$$

2.5. Properties of permutation representations

Let X be a finite G-set. The result shows how to reduce an arbitrary permutation representation to a direct sum of those induced from transitive G-sets.

PROPOSITION 2.21. *Let $X = X_1 \coprod X_2$ where $X_1, X_2 \subseteq X$ are closed under the action of G. Then there is a G-isomorphism*

$$\Bbbk[X] \cong \Bbbk[X_1] \oplus \Bbbk[X_2].$$

PROOF. Let $j_1\colon X_1 \to X$ and $j_2\colon X_2 \to X$ be the inclusion maps, which are G-maps. By Theorem 2.20(b), there are G-linear transformations $j_{1*}\colon \Bbbk[X_1] \to \Bbbk[X]$ and $j_{2*}\colon \Bbbk[X_2] \to \Bbbk[X]$. For

$$f = \sum_{x\in X} t_x x \in \Bbbk[X],$$

we have the 'restrictions'

$$f_1 = \sum_{x\in X_1} t_x x, \quad f_2 = \sum_{x\in X_2} t_x x.$$

We define our linear map $\Bbbk[X] \cong \Bbbk[X_1] \oplus \Bbbk[X_2]$ by

$$f \longmapsto (f_1, f_2).$$

It is easily seen that this is a linear transformation, and moreover has an inverse given by

$$(h_1, h_2) \longmapsto j_{1*}h_1 + j_{2*}h_2.$$

Finally, this is a G-map since the latter is the sum of two G-maps, so its inverse is a G-map. $\square$

Let X_1 and X_2 be G-sets. Then $X = X_1 \times X_2$ can be made into a G-set with action given by

$$g \cdot (x_1, x_2) = (gx_1, gx_2).$$

PROPOSITION 2.22. *Let X_1 and X_2 be G-sets. Then there is a G-isomorphism*

$$\Bbbk[X_1] \otimes \Bbbk[X_2] \cong \Bbbk[X_1 \times X_2].$$

PROOF. The function $F\colon \Bbbk[X_1] \times \Bbbk[X_2] \to \Bbbk[X_1 \times X_2]$ defined by

$$F(\sum_{x\in X_1} s_x x, \sum_{y\in X_2} t_y y) = \sum_{x\in X_1}\sum_{y\in X_2} s_x t_y (x, y)$$

is $\Bbbk$-bilinear. Hence by the universal property of the tensor product (Section 1.4, UP-TP), there is a unique linear transformation $F' \colon \Bbbk[X_1] \otimes \Bbbk[X_2] \to \Bbbk[X_1 \times X_2]$ for which

$$F'(x \otimes y) = (x, y) \quad (x \in X_1,\ y \in X_2).$$

This is easily seen to to be a G-linear isomorphism. □

Definition 2.23. Let G be a finite group. The *regular representation over* $\Bbbk$ is the G-representation $\Bbbk[G]$. This has dimension $\dim_{\Bbbk} \Bbbk[G] = |G|$.

Proposition 2.24. *The regular representation of a finite group G over a field $\Bbbk$ is a ring (in fact a $\Bbbk$-algebra). Moreover, this ring is commutative if and only if G is abelian.*

Proof. Let $a = \sum_{g \in G} a_g g$ and $b = \sum_{g \in G} b_g g$ where $a_g, b_g \in G$. Then we define the product of a and b by

$$ab = \sum_{g \in G} \left(\sum_{h \in G} a_h b_{h^{-1}g} \right) g.$$

Note that for $g, h \in G$ in $\Bbbk[G]$ we have

$$(1g)(1h) = gh.$$

For commutativity, each such product $(1g)(1h)$ must agree with $(1h)(1g)$, which happens if and only if G is abelian. The rest of the details are left as an exercise. □

The ring $\Bbbk[G]$ is called the *group algebra* or *group ring* of G over $\Bbbk$. The next result is left as an exercise for those who know about modules. It provides a link between the study of modules over $\Bbbk[G]$ and G-representations, and so the group ring construction provides an important source of non-commutative rings and their modules.

Proposition 2.25. *Let V be a $\Bbbk$ vector space. Then if V carries a G-representation, it admits the structure of a $\Bbbk[G]$ module defined by*

$$(\sum_{g \in G} a_g g)v = \sum_{g \in G} a_g g v.$$

Conversely, if V is a $\Bbbk[G]$-module, then it admits a G-representation with action defined by

$$g \cdot v = (1g)v.$$

2.6. Calculating in permutation representations

In this section, we determine how the permutation representation $\Bbbk[X]$ looks in terms of the basis consisting of elements x $(x \in X)$. We know that $g \in G$ acts by sending x to gx. Hence, if we label the rows and columns of a matrix by the elements of X, the $|X| \times |X|$ matrix $[g]$ of g with respect to this basis has xy entry

$$[g]_{xy} = \delta_{x,gy} = \begin{cases} 1 & \text{if } x = gy, \\ 0 & \text{otherwise,} \end{cases} \tag{2.2}$$

where $\delta_{a,b}$ denotes the *Kronecker δ function* which is 0 except for when $a = b$ and it then takes the value 1. Thus there is exactly one 1 in each row and column, and 0's everywhere else. The following is an important example.

Let $X = \mathbf{n} = \{1, 2, \ldots, n\}$ and $G = S_n$, the symmetric group of degree n, acting on $\mathbf{n}$ in the usual way. We may take as a basis for $\Bbbk[\mathbf{n}]$, the functions δ_j $(1 \leqslant j \leqslant n)$ given by

$$\delta_j(k) = \begin{cases} 1 & \text{if } k = j, \\ 0 & \text{otherwise.} \end{cases}$$

Relative to this basis, the action of $\sigma \in S_n$ is given by the $n \times n$ matrix $[\sigma]$ whose ij-th entry is

$$[\sigma]_{ij} = \begin{cases} 1 & \text{if } i = \sigma(j), \\ 0 & \text{otherwise.} \end{cases} \tag{2.3}$$

Taking $n = 3$, we get

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

As expected, we also have

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

An important fact about permutation representations is the following, which makes their *characters* easy to calculate.

PROPOSITION 2.26. *Let X be a finite G-set, and $\Bbbk[X]$ the associated permutation representation. Let $g \in G$ and $\rho_g \colon \Bbbk[X] \to \Bbbk[X]$ be the linear transformation induced by g. Then*

$$\operatorname{tr} \rho_g = |X^g| = |\{x \in X : gx = x\}| = \text{number of elements of } X \text{ fixed by } g.$$

PROOF. Take the elements of X to be a basis for $\Bbbk[X]$. Then $\operatorname{tr} \rho_g$ is the sum of the diagonal terms in the matrix $[\rho_g]$ relative to this basis. Now making use of Equation (2.2) we see that

$$\operatorname{tr} \rho_g = \text{number of non-zero diagonal terms in } [\rho_g] = \text{number of elements of } X \text{ fixed by } g. \qquad \square$$

Our next result shows that permutation representations are self-dual.

PROPOSITION 2.27. *Let X be a finite G-set, and $\Bbbk[X]$ the associated permutation representation. Then there is a G-isomorphism $\Bbbk[X] \cong \Bbbk[X]^*$.*

PROOF. Take as a basis of $\Bbbk[X]$ the elements $x \in X$. Then a basis for the dual space $\Bbbk[X]^*$ consists of the elements x^*. By definition of the action of G on $\Bbbk[X]^* = \operatorname{Hom}_{\Bbbk}(\Bbbk[X], \Bbbk)$, we have

$$(g \cdot x^*)(y) = x^*(g^{-1}x) \quad (g \in G,\ y \in X).$$

A familiar calculation shows that $g \cdot x^* = (gx)^*$, and so this basis is also permuted by G. Now define a function $\varphi \colon \Bbbk[X] \to \Bbbk[X]^*$ by

$$\varphi(\sum_{x \in X} a_x x) = \sum_{x \in X} a_x x^*.$$

This is a $\Bbbk$-linear isomorphism also satisfying

$$\varphi\left(g \sum_{x \in X} a_x x\right) = \varphi\left(\sum_{x \in X} a_x (gx)\right) = \sum_{x \in X} a_x (gx)^* = g \cdot \varphi\left(\sum_{x \in X} a_x x\right).$$

Hence φ is a G-isomorphism. $\square$

2.7. Generalized permutation representations

It is useful to generalize the notion of permutation representation somewhat. Let V be a finite dimensional $\Bbbk$-vector space with a representation of G, $\rho\colon G \to \mathrm{GL}_{\Bbbk}(V)$; we will usually write $gv = \rho_g v$. We can consider the set of all functions $X \to V$, $\mathrm{Map}(X, V)$, and this is also a finite dimensional $\Bbbk$-vector space with addition and scalar multiplication defined by

$$(f_1 + f_2)(x) = f_1(x) + f_2(x), \quad (tf)(x) = t(f(x)),$$

for $f_1, f_2, f \in \mathrm{Map}(X, V)$, $t \in \Bbbk$ and $x \in X$. There is a representation of G on $\mathrm{Map}(X, V)$ given by

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

We call this a *generalized permutation representation* of G.

Proposition 2.28. *Let* $\mathrm{Map}(X, V)$ *be a permutation representation of* G*, where* V *has basis* $\mathbf{v} = \{v_1, \ldots, v_n\}$*. Then the functions* $\delta_{x,j}\colon X \to V$ $(x \in X,\ 1 \leqslant j \leqslant n)$ *given by*

$$\delta_{x,j}(y) = \begin{cases} v_j & \text{if } y = x, \\ 0 & \text{otherwise,} \end{cases}$$

for $y \in X$*, form a basis for* $\mathrm{Map}(X, V)$*. Hence,*

$$\dim_{\Bbbk} \mathrm{Map}(X, V) = |X| \dim_{\Bbbk} V.$$

Proof. Let $f\colon X \to V$. Then for any $y \in X$,

$$f(y) = \sum_{j=1}^{n} f_j(y) v_j,$$

where $f_j\colon X \to \Bbbk$ is a function. It suffices now to show that any function $h\colon X \to \Bbbk$ has a unique expression as

$$h = \sum_{x \in X} h_x \delta_x$$

where $h_x \in \Bbbk$ and $\delta_x\colon X \to \Bbbk$ is given by

$$\delta_x(y) = \begin{cases} 1 & \text{if } y = x, \\ 0 & \text{otherwise.} \end{cases}$$

But for $y \in X$,

$$h(y) = \sum_{x \in X} h_x \delta_x(y) \quad \iff \quad h(y) = h_y.$$

Hence $h = \sum_{x \in X} h(x)\delta_x$ is the unique expansion of this form. Combining this with the above we have

$$f(y) = \sum_{j=1}^{n} f_j(y) v_j = \sum_{j=1}^{n} \sum_{x \in X} f_j(x)\delta_x(y) v_j,$$

and so

$$f = \sum_{j=1}^{n} \sum_{x \in X} f_j(x) \delta_{xj},$$

is the unique such expression, since $\delta_{xj}(y) = \delta_x(y) v_j$. $\square$

PROPOSITION 2.29. *If $V = V_1 \oplus V_2$ is a direct sum of representations V_1, V_2, then there is a G-isomorphism*

$$\mathrm{Map}(X, V) \cong \mathrm{Map}(X, V_1) \oplus \mathrm{Map}(X, V_2).$$

PROOF. Recall that every $v \in V$ has a unique expression of the form $v = v_1 + v_2$. Define a function

$$\mathrm{Map}(X, V) \to \mathrm{Map}(X, V_1) \oplus \mathrm{Map}(X, V_2); \quad f \to f_1 + f_2,$$

where $f_1 \colon X \to V_1$ and $f_2 \colon X \to V_2$ satisfy

$$f(x) = f_1(x) + f_2(x) \quad (x \in X).$$

This is easily seen to be both a linear isomorphism and a G-homomorphism, hence a G-isomorphism. $\square$

PROPOSITION 2.30. *Let $X = X_1 \coprod X_2$ where $X_1, X_2 \subseteq X$ are closed under the action of G. Then there is a G-isomorphism*

$$\mathrm{Map}(X, V) \cong \mathrm{Map}(X_1, V) \oplus \mathrm{Map}(X_2, V).$$

PROOF. Let $j_1 \colon X_1 \to X$ and $j_2 \colon X_2 \to X$ be the inclusion maps, which are G-maps. Then given $f \colon X \to V$, we have two functions $f_k \colon X \to V$ $(k = 1, 2)$ given by

$$f_k(x) = \begin{cases} f(x) & \text{if } x \in X_k, \\ 0 & \text{otherwise.} \end{cases}$$

Define a function

$$\mathrm{Map}(X, V) \cong \mathrm{Map}(X_1, V) \to \mathrm{Map}(X_2, V); \quad f \longmapsto f_1 + f_2.$$

This is easily seen to be a linear isomorphism. Using the fact that X_k is closed under the action of G, we see that

$$(g \cdot f)_k = g \cdot f_k,$$

so

$$g \cdot (f_1 + f_2) = g \cdot f_1 + g \cdot f_2.$$

Therefore this map is a G-isomorphism. $\square$

These results tell us how to reduce an arbitrary generalized permutation representation to a direct sum of those induced from a transitive G-set X and an irreducible representation V.

Exercises on Chapter 2

2-1. Consider the function $\sigma \colon D_{2n} \to \mathrm{GL}_{\mathbb{C}}(\mathbb{C}^2)$ given by

$$\sigma_{\alpha^r}(xe_1 + ye_2) = \zeta^r xe_1 + \zeta^{-r} ye_2, \quad \sigma_{\alpha^r\beta}(xe_1 + ye_2) = \zeta^r ye_1 + \zeta^{-r} xe_2,$$

where $\sigma_g = \sigma(g)$ and $\zeta = e^{2\pi i/n}$. Show that this defines a 2-dimensional representation of D_{2n} over $\mathbb{C}$. Show that this representation is irreducible and determine $\ker \sigma$.

2-2. Show that there is a 3-dimensional real representation $\theta \colon Q_8 \to \mathrm{GL}_{\mathbb{R}}(\mathbb{R}^3)$ of the quaternion group Q_8 for which

$$\theta_{\mathbf{i}}(xe_1 + ye_2 + ze_3) = \quad xe_1 - ye_2 - ze_3, \quad \theta_{\mathbf{j}}(xe_1 + ye_2 + ze_3) = -xe_1 + ye_2 - ze_3.$$

Show that this representation is not irreducible and determine $\ker\theta$.

2-3. Consider the 2-dimensional complex vector space

$$V = \{(x_1, x_2, x_3) \in \mathbb{C}^3 : x_1 + x_2 + x_3 = 0\}.$$

Show that the symmetric group S_3 has a representation ρ on V defined by

$$\rho_\sigma(x_1, x_2, x_3) = (x_{\sigma^{-1}(1)}, x_{\sigma^{-1}(2)}, x_{\sigma^{-1}(3)})$$

for $\sigma \in S_3$. Show that this representation is irreducible.

2-4. If p is a prime and G is a non-trivial finite p-group, show that there is a non-trivial 1-dimensional representation of G. More generally show this holds for a finite solvable group.

2-5. Let $X = \{1, 2, 3\} = \mathbf{3}$ with the usual action of the symmetric group S_3. Consider the complex permutation representation of S_3 associated to this with underlying vector space $V = \mathbb{C}[\mathbf{3}]$.

(i) Show that the invariant subspace

$$V^{S_3} = \{v \in V : \sigma \cdot v = v \ \forall \sigma \in S_3\}$$

is 1-dimensional.

(ii) Find a 2-dimensional S_3-subspace $W \subseteq V$ such that $V = V^{S_3} \oplus W$.

(iii) Show that W of (ii) is irreducible.

(iv) Show that the restriction $W \downarrow_H^{S_3}$ of the representation of S_3 on W to the subgroup $H = \{e, (1\,2)\}$ is not irreducible.

(v) Show that the restriction of the representation $W \downarrow_K^{S_3}$ of S_3 on W to the subgroup $K = \{e, (1\,2\,3), (1\,3\,2)\}$ is not irreducible.

2-6. Let the finite group G act on the finite set X and let $\mathbb{C}[X]$ be the associated complex permutation representation.

(i) If the action of G on X is transitive (i.e., there is exactly one orbit), show that there is a 1-dimensional G-subspace $\mathbb{C}\{v_X\}$ with basis vector $v_X = \sum_{x\in X} x$. Find a G-subspace $W_X \subseteq \mathbb{C}[X]$ for which $\mathbb{C}[X] = \mathbb{C}\{v_X\} \oplus W_X$.

(ii) For a general G-action on X, for each G-orbit Y in X use (a) to find a 1-dimensional G-subspace V_Y and another W_Y of dimension $(|Y| - 1)$ such that

$$\mathbb{C}[X] = V_{Y_1} \oplus W_{Y_1} \oplus \cdots \oplus V_{Y_r} \oplus W_{Y_r}$$

where $Y_1, \ldots, Y_r$ are the distinct G-orbits of X.

2-7. If $\rho\colon G \to \mathrm{GL}_{\Bbbk}(V)$ is an irreducible representation, prove that the contragredient representation $\rho^*\colon G \to \mathrm{GL}_{\Bbbk}(V^*)$ is also irreducible.

2-8. Let $\Bbbk$ be a field of characteristic different from 2. Let G be a finite group of even order and let $C \leqslant G$ be a subgroup of order 2 with generator γ. Consider the regular representation of G, which comes from the natural *left* action of G on $\Bbbk[G]$.

Now consider the action of the generator γ by multiplication of basis vectors on the *right*. Denote the $+1, -1$ eigenspaces for this action by $\Bbbk[G]^+, \Bbbk[G]^-$ respectively.

Show that the subspaces $\Bbbk[G]^{\pm}$ are G-subspaces and that

$$\dim_{\Bbbk} \Bbbk[G]^{+} = \dim_{\Bbbk} \Bbbk[G]^{-} = \frac{|G|}{2}.$$

Deduce that $\Bbbk[G] = \Bbbk[G]^{+} \oplus \Bbbk[G]^{-}$ as G-representations.

CHAPTER 3

Character theory

3.1. Characters and class functions on a finite group

Let G be a finite group and let $\rho\colon G \to \mathrm{GL}_{\mathbb{C}}(V)$ be a finite dimensional $\mathbb{C}$-representation of dimension $\dim_{\mathbb{C}} V = n$. For $g \in G$, the linear transformation $\rho_g\colon V \to V$ will sometimes be written $g\cdot$ or g. The *character* of g in the representation ρ is the trace of g on V, i.e.,

$$\chi_\rho(g) = \operatorname{tr}\rho_g = \operatorname{tr} g.$$

We can view χ_ρ as a function $\chi_\rho\colon G \to \mathbb{C}$, the *character* of the representation ρ.

Definition 3.1. A function $\theta\colon G \to \mathbb{C}$ is a *class function* if for all $g, h \in G$,

$$\theta(hgh^{-1}) = \theta(g),$$

i.e., θ is constant on each conjugacy class of G.

Proposition 3.2. *For all $g, h \in G$,*

$$\chi_\rho(hgh^{-1}) = \chi_\rho(g).$$

Hence $\chi_\rho\colon G \to \mathbb{C}$ is a class function on G.

Proof. We have

$$\rho_{hgh^{-1}} = \rho_h \circ \rho_g \circ \rho_{h^{-1}} = \rho_h \circ \rho_g \circ \rho_h^{-1}$$

and so

$$\chi_\rho(hgh^{-1}) = \operatorname{tr}\rho_h \circ \rho_g \circ \rho_h^{-1} = \operatorname{tr}\rho_g = \chi_\rho(g). \qquad \square$$

Example 3.3. Let $G = S_3$ act on the set $\mathbf{3} = \{1, 2, 3\}$ in the usual way. Let $V = \mathbb{C}[\mathbf{3}]$ be the associated permutation representation over $\mathbb{C}$, where we take as a basis $\mathbf{e} = \{e_1, e_2, e_3\}$ with action

$$\sigma \cdot e_j = e_{\sigma(j)}.$$

Let us determine the character of this representation $\rho\colon S_3 \to \mathrm{GL}_{\mathbb{C}}(V)$.

The elements of S_3 written using cycle notation are the following:

$$1,\ (1\ 2),\ (2\ 3),\ (1\ 3),\ (1\ 2\ 3),\ (1\ 3\ 2).$$

The matrices of these elements with respect to $\mathbf{e}$ are

$$I_3,\ \begin{bmatrix}0&1&0\\1&0&0\\0&0&1\end{bmatrix},\ \begin{bmatrix}1&0&0\\0&0&1\\0&1&0\end{bmatrix},\ \begin{bmatrix}0&0&1\\0&1&0\\1&0&0\end{bmatrix},\ \begin{bmatrix}0&0&1\\1&0&0\\0&1&0\end{bmatrix},\ \begin{bmatrix}0&1&0\\0&0&1\\1&0&0\end{bmatrix}.$$

Taking traces we obtain

$$\chi_\rho(1) = 3,\ \chi_\rho(1\ 2) = \chi_\rho(2\ 3) = \chi_\rho(1\ 3) = 1,\ \chi_\rho(1\ 2\ 3) = \chi_\rho(1\ 3\ 2) = 0.$$

Notice that we have $\chi_\rho(g) \in \mathbb{Z}$ for all $g \in G$. Indeed, by Proposition 2.26 we have the following important and useful result.

Proposition 3.4. *Let X be a G-set and ρ the associated permutation representation on $\mathbb{C}[X]$. Then for each $g \in G$,*

$$\chi_\rho(g) = |X^g| = |\{x \in X : g \cdot x = x\}| = \text{the number of elements of } X \text{ fixed by } g,$$

in particular, $\chi_\rho(g)$ is a non-negative integer.

The next result sheds further light on the significance of the character of a G-representation over the complex number field $\mathbb{C}$ and makes use of linear algebra developed in Section 1.3 of Chapter 1.

Theorem 3.5. *For $g \in G$, there is a basis $\mathbf{v} = \{v_1, \ldots, v_n\}$ of V consisting of eigenvectors of the linear transformation g.*

Proof. Let $d = |g|$, the order of g. For $v \in V$,

$$(g^d - \mathrm{Id}_V)(v) = 0.$$

Now we can apply Lemma 1.16 with the polynomial $f(X) = X^d - 1$, which has d distinct roots in $\mathbb{C}$. $\square$

There may well be a smaller degree polynomial identity satisfied by the linear transformation g on V. However, if a polynomial $f(X)$ satisfied by g has $\deg f(X) \leqslant d$ and no repeated linear factors, then $f(X) | (X^d - 1)$.

Corollary 3.6. *The distinct eigenvalues of the linear transformation g on V are dth roots of unity. More precisely, if d_0 is the smallest natural number such that for all $v \in V$,*

$$(g^{d_0} - \mathrm{Id}_V)(v) = 0,$$

then the distinct eigenvalues of g are d_0th roots of unity.

Proof. An eigenvalue λ (with eigenvector $v_\lambda \neq 0$) of g satisfies

$$(g^d - \mathrm{Id}_V)(v_\lambda) = 0,$$

hence

$$(\lambda^d - 1)v_\lambda = 0.$$

$\square$

Corollary 3.7. *For any $g \in G$ we have*

$$\chi_\rho(g) = \sum_{j=1}^{n} \lambda_j$$

where $\lambda_1, \ldots, \lambda_n$ are the n eigenvalues of ρ_g on V, including repetitions.

Corollary 3.8. *For $g \in G$ we have*

$$\chi_\rho(g^{-1}) = \overline{\chi_\rho(g)} = \chi_{\rho^*}(g).$$

Proof. If the eigenvalues of ρ_g including repetitions are $\lambda_1, \ldots, \lambda_n$, then the eigenvalues of $\rho_{g^{-1}}$ including repetitions are easily seen to be $\lambda_1^{-1}, \ldots, \lambda_n^{-1}$. But if ζ is a root of unity, then $\zeta^{-1} = \overline{\zeta}$, and so $\chi_\rho(g^{-1}) = \overline{\chi_\rho(g)}$. The second equality follows from Proposition 2.16. $\square$

Now let us return to the idea of functions on a group which are invariant under conjugation. Denote by G_c the set G and let G act on it by conjugation,

$$g \cdot x = gxg^{-1}.$$

The set of all functions $G_c \to \mathbb{C}$, $\operatorname{Map}(G_c, \mathbb{C})$ has an action of G given by

$$(g \cdot \alpha)(x) = \alpha(gxg^{-1})$$

for $\alpha \in \operatorname{Map}(G_c, \mathbb{C})$, $g \in G$ and $x \in G_c$. Then the class functions are those which are invariant under conjugation and hence form the set $\operatorname{Map}(G_c, \mathbb{C})^G$ which is a $\mathbb{C}$-vector subspace of $\operatorname{Map}(G_c, \mathbb{C})$.

Proposition 3.9. *The $\mathbb{C}$-vector space $\operatorname{Map}(G_c, \mathbb{C})^G$ has as a basis the set of all functions $\Delta_C \colon G_c \to \mathbb{C}$ for C a conjugacy class in G, defined by*

$$\Delta_C(x) = \begin{cases} 1 & \text{if } x \in C, \\ 0 & \text{if } x \notin C. \end{cases}$$

Thus $\dim_{\mathbb{C}} \operatorname{Map}(G_c, \mathbb{C})^G$ is the number of conjugacy classes in G.

Proof. From the proof of Theorem 2.20, we know that a class function $\alpha \colon G_c \to \mathbb{C}$ has a unique expression of the form

$$\alpha = \sum_{x \in G_c} a_x \delta_x$$

for suitable $a_x \in G_c$. But

$$g \cdot \alpha = \sum_{x \in G_c} a_x (g \cdot \delta_x) = \sum_{x \in G_c} a_x \delta_{gxg^{-1}} = \sum_{x \in G_c} a_{gxg^{-1}} \delta_x.$$

Hence by uniqueness and the definition of class function, we must have

$$a_{gxg^{-1}} = a_x \quad (g \in G,\, x \in G_c).$$

Hence,

$$\alpha = \sum_C a_C \sum_{x \in C} \delta_x,$$

where for each conjugacy class C we choose any element $c_0 \in C$ and put $a_C = a_{c_0}$. Here the outer sum is over all the conjugacy classes C of G. We now find that

$$\Delta_C = \sum_{x \in C} \delta_x$$

and the rest of the proof is straightforward. $\square$

We will see that the characters of non-isomorphic irreducible representations of G also form a basis of $\operatorname{Map}(G_c, \mathbb{C})^G$. We set $\mathcal{C}(G) = \operatorname{Map}(G_c, \mathbb{C})^G$.

3.2. Properties of characters

In this section we will see some other important properties of characters.

THEOREM 3.10. *Let G be a finite group with finite dimensional complex representations $\rho\colon G \to \mathrm{GL}_{\mathbb{C}}(V)$ and $\sigma\colon G \to \mathrm{GL}_{\mathbb{C}}(W)$. Then*

(a) $\chi_\rho(e) = \dim_{\mathbb{C}} V$ *and for $g \in G$, $|\chi_\rho(g)| \leqslant \chi_\rho(e)$.*

(b) *The tensor product representation $\rho \otimes \sigma$ has character*

$$\chi_{\rho\otimes\sigma} = \chi_\rho \chi_\sigma,$$

i.e., for each $g \in G$,

$$\chi_{\rho\otimes\sigma}(g) = \chi_\rho(g)\chi_\sigma(g).$$

(c) *Let $\tau\colon G \to \mathrm{GL}_{\mathbb{C}}(U)$ be a representation which is G-isomorphic to the direct sum of ρ and σ, so $U \cong V \oplus W$. Then*

$$\chi_\tau = \chi_\rho + \chi_\sigma,$$

i.e., for each $g \in G$,

$$\chi_\tau(g) = \chi_\rho(g) + \chi_\sigma(g).$$

PROOF. (a) The first statement is immediate from the definition. For the second, using Theorem 3.5, we may choose a basis $\mathbf{v} = \{v_1, \ldots, v_r\}$ of V for which $\rho_g v_k = \lambda_k v_k$, where λ_k is a root of unity (hence satisfies $|\lambda_k| = 1$). Then

$$|\chi_\rho(g)| = |\sum_{k=1}^{r} \lambda_k| \leqslant \sum_{k=1}^{r} |\lambda_k| = r = \chi_\rho(e).$$

(b) Let $g \in G$. By Theorem 3.5, there are bases $\mathbf{v} = \{v_1, \ldots, v_r\}$ and $\mathbf{w} = \{w_1, \ldots, w_s\}$ for V and W consisting of eigenvectors for ρ_g and σ_g with corresponding eigenvalues $\lambda_1, \ldots, \lambda_r$ and $\mu_1, \ldots, \mu_s$. The elements $v_i \otimes w_j$ form a basis for $V \otimes W$ and by the formula of Equation (2.1), the action of g on these vectors is given by

$$(\rho \otimes \sigma)_g \cdot (v_i \otimes w_j) = \lambda_i \mu_j v_i \otimes w_j.$$

Finally Corollary 3.7 implies

$$\mathrm{tr}(\rho \otimes \sigma)_g = \sum_{i,j} \lambda_i \mu_j = \chi_\rho(g)\chi_\sigma(g).$$

(c) For $g \in G$, choose bases $\mathbf{v} = \{v_1, \ldots, v_r\}$ and $\mathbf{w} = \{w_1, \ldots, w_s\}$ for V and W consisting of eigenvectors for ρ_g and σ_g with corresponding eigenvalues $\lambda_1, \ldots, \lambda_r$ and $\mu_1, \ldots, \mu_s$. Then $\mathbf{v} \cup \mathbf{w} = \{v_1, \ldots, v_r, w_1, \ldots, w_s\}$ is a basis for U consisting of eigenvectors for τ_g with the above eigenvalues. Then

$$\chi_\tau(g) = \mathrm{tr}\,\tau_g = \lambda_1 + \cdots + \lambda_r + \mu_1 + \cdots + \mu_s = \chi_\rho(g) + \chi_\sigma(g). \qquad \square$$

3.3. Inner products of characters

In this section we will discuss a way to 'compare' characters, using a *scalar* or *inner product* on the vector space of class functions $\mathcal{C}(G)$. In particular, we will see that the character of a representation determines it up to a G-isomorphism. We will again work over the field of complex numbers $\mathbb{C}$.

We begin with the notion of *scalar* or *inner product* on a finite dimensional $\mathbb{C}$-vector space V. A function $(\ |\ ): V \times V \to \mathbb{C}$ is called a *hermitian inner* or *scalar product* on V if for $v, v_1, v_2, w \in V$ and $z_1, z_2 \in \mathbb{C}$,

(LLin) $$(z_1 v_1 + z_2 v_2 | w) = z_1 (v_1|w) + z_2 (v_2|w),$$

(RLin) $$(w|z_1 v_1 + z_2 v_2) = \overline{z_1}(w|v_1) + \overline{z_2}(w|v_2),$$

(Symm) $$(v|w) = \overline{(w|v)},$$

(PoDe) $$0 \leqslant (v|v) \in \mathbb{R} \text{ with equality if and only if } v = 0.$$

A set of vectors $\{v_1, \dots, v_k\}$ is said to be *orthonormal* if

$$(v_i|v_j) = \delta_{ij} = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{else.} \end{cases}$$

We will define an inner product $(\ |\ )_G$ on $\mathcal{C}(G) = \mathrm{Map}(G_c, \mathbb{C})^G$, often writing $(\ |\ )$ when the group G is clear from the context.

Definition 3.11. For $\alpha, \beta \in \mathcal{C}(G)$, let

$$(\alpha|\beta)_G = \frac{1}{|G|} \sum_{g \in G} \alpha(g)\overline{\beta(g)}.$$

Proposition 3.12. $(\ |\ ) = (\ |\ )_G$ *is an hermitian inner product on* $\mathcal{C}(G)$.

Proof. The properties LLin, RLin and Symm are easily checked. We will show that PoDe holds. We have

$$(\alpha|\alpha) = \frac{1}{|G|} \sum_{g \in G} \alpha(g)\overline{\alpha(g)} = \frac{1}{|G|} \sum_{g \in G} |\alpha(g)|^2 \geqslant 0$$

with equality if and only if $\alpha(g) = 0$ for all $g \in G$. Hence $(\alpha|\alpha)$ satisfies PoDe. $\square$

Now let $\rho: G \to \mathrm{GL}_{\mathbb{C}}(V)$ and $\theta: G \to \mathrm{GL}_{\mathbb{C}}(W)$ be finite dimensional representations over $\mathbb{C}$. We know how to determine $(\chi_\rho|\chi_\theta)_G$ from the definition. Here is another interpretation of this quantity. Recall from Proposition 2.17 the representations of G on $W \otimes V^*$ and $\mathrm{Hom}_{\mathbb{C}}(V, W)$; in fact these are G-isomorphic, $W \otimes V^* \cong \mathrm{Hom}_{\mathbb{C}}(V, W)$. By Proposition 2.18, the G-invariant subspaces $(W \otimes V^*)^G$ and $\mathrm{Hom}_{\mathbb{C}}(V, W)^G$ are subrepresentations and are images of G-homomorphisms $\varepsilon_1: W \otimes V^* \to W \otimes V^*$ and $\varepsilon_2: \mathrm{Hom}_{\mathbb{C}}(V, W) \to \mathrm{Hom}_{\mathbb{C}}(V, W)$.

Proposition 3.13. *We have*

$$(\chi_\theta|\chi_\rho)_G = \operatorname{tr} \varepsilon_1 = \operatorname{tr} \varepsilon_2.$$

Proof. Let $g \in G$. By Theorem 3.5 and Corollary 3.7 we can find bases $\mathbf{v} = \{v_1, \dots, v_r\}$ for V and $\mathbf{w} = \{w_1, \dots, w_s\}$ for W consisting of eigenvectors with corresponding eigenvalues

$\lambda_1, \dots, \lambda_r$ and $\mu_1, \dots, \mu_s$. The elements $w_j \otimes v_i^*$ form a basis for $W \otimes V^*$ and moreover g acts on these by

$$(\theta \otimes \rho^*)_g (w_j \otimes v_i^*) = \mu_j \overline{\lambda_i} w_j \otimes v_i^*,$$

using Proposition 2.16. By Corollary 3.7 we have

$$\operatorname{tr}(\theta \otimes \rho^*)_g = \sum_{i,j} \mu_j \overline{\lambda_i} = \Big(\sum_j \mu_j\Big)\Big(\sum_i \overline{\lambda_i}\Big) = \chi_\theta(g)\overline{\chi_\rho(g)}.$$

By definition of ε_1, we have

$$\operatorname{tr} \varepsilon_1 = \frac{1}{|G|} \sum_{g \in G} \operatorname{tr}(\theta \otimes \rho^*)_g = \frac{1}{|G|} \sum_{g \in G} \chi_\theta(g)\overline{\chi_\rho(g)} = (\chi_\theta | \chi_\rho).$$

Since ε_2 corresponds to ε_1 under the G-isomorphism

$$W \otimes V^* \cong \operatorname{Hom}_{\mathbb{C}}(V, W),$$

we obtain $\operatorname{tr} \varepsilon_1 = \operatorname{tr} \varepsilon_2$. □

Corollary 3.14. *For irreducible representations ρ and θ,*

$$(\chi_\theta | \chi_\rho) = \begin{cases} 1 & \text{if } \rho \text{ and } \theta \text{ are } G\text{-equivalent}, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. By Schur's Lemma, Theorem 2.8,

$$\dim_{\Bbbk} \operatorname{Hom}_{\Bbbk}(V, W)^G = \begin{cases} 1 & \text{if } \rho \text{ and } \theta \text{ are } G\text{-equivalent}, \\ 0 & \text{otherwise.} \end{cases}$$

Since ε_2 is the identity on $\operatorname{Hom}_{\Bbbk}(V, W)^G$, the result follows. □

Thus if we take a collection of non-equivalent irreducible representations $\{\rho_1, \dots, \rho_r\}$, their characters form an *orthonormal* set $\{\chi_{\rho_1}, \dots, \chi_{\rho_r}\}$ in $\mathcal{C}(G)$, i.e.,

$$(\chi_{\rho_i} | \chi_{\rho_j}) = \delta_{ij}.$$

By Proposition 3.9 we know that $\dim_{\mathbb{C}} \mathcal{C}(G)$ is equal to the number of conjugacy classes in G. We will show that the characters of the distinct inequivalent irreducible representations form a basis for $\mathcal{C}(G)$, thus there must be $\dim_{\mathbb{C}} \mathcal{C}(G)$ such distinct inequivalent irreducibles.

Theorem 3.15. *The characters of all the distinct inequivalent irreducible representations of G form an orthonormal basis for $\mathcal{C}(G)$.*

Proof. Suppose $\alpha \in \mathcal{C}(G)$ and for every irreducible ρ we have $(\alpha | \chi_\rho) = 0$. We will show that $\alpha = 0$.

Suppose that $\rho\colon G \to \operatorname{GL}_{\mathbb{C}}(V)$ is any representation of G. Then define $\rho_\alpha\colon V \to V$ by

$$\rho_\alpha(v) = \sum_{g \in G} \alpha(g) \rho_g v.$$

For any $h \in G$ and $v \in V$ we have

$$\begin{aligned}\rho_\alpha(\rho_h v) &= \sum_{g\in G} \alpha(g)\rho_g(\rho_h v)\\ &= \rho_h\Big(\sum_{g\in G} \alpha(g)\rho_{h^{-1}gh} v\Big)\\ &= \rho_h\Big(\sum_{g\in G} \alpha(h^{-1}gh)\rho_{h^{-1}gh} v\Big)\\ &= \rho_h\Big(\sum_{g\in G} \alpha(g)\rho_g v\Big)\\ &= \rho_h\rho_\alpha(v).\end{aligned}$$

Hence $\rho_\alpha \in \operatorname{Hom}_{\mathbb{C}}(V,V)^G$, i.e., ρ_α is G-linear.

Now applying this to an irreducible ρ with $\dim\rho = n$, by Schur's Lemma, Theorem 2.8, there must be a $\lambda \in \mathbb{C}$ for which $\rho_\alpha = \lambda \operatorname{Id}_V$.

Taking traces, we have $\operatorname{tr}\rho_\alpha = n\lambda$. Also

$$\operatorname{tr}\rho_\alpha = \sum_{g\in G} \alpha(g)\operatorname{tr}\rho_g = \sum_{g\in G} \alpha(g)\chi_\rho(g) = |G|(\alpha|\chi_{\rho^*}).$$

Hence we obtain

$$\lambda = \frac{|G|}{\dim_{\mathbb{C}} V}(\alpha|\chi_{\rho^*}).$$

If $(\alpha|\chi_\rho) = 0$ for all irreducible ρ, then as ρ^* is irreducible whenever ρ is, we must have $\rho_\alpha = 0$ for every such irreducible ρ.

Since every representation ρ decomposes into a sum of irreducible subrepresentations, it is easily verified that for every ρ we also have $\rho_\alpha = 0$ for such an α.

Now apply this to the regular representation $\rho = \rho_{\mathrm{reg}}$ on $V = \mathbb{C}[G]$. Taking the basis vector $e \in \mathbb{C}[G]$ we have

$$\rho_\alpha(e) = \sum_{g\in G} \alpha(g)\rho_g e = \sum_{g\in G} \alpha(g) g e = \sum_{g\in G} \alpha(g) g.$$

But this must be 0, hence we have

$$\sum_{g\in G} \alpha(g) g = 0$$

in $\mathbb{C}[G]$ which can only happen if $\alpha(g) = 0$ for every $g \in G$, since the $g \in G$ form a basis of $\mathbb{C}[G]$. Thus $\alpha = 0$ as desired.

Now for any $\alpha \in \mathcal{C}(G)$, we can form the function

$$\alpha' = \alpha - \sum_{i=1}^{r} (\alpha|\chi_{\rho_i})\chi_{\rho_i},$$

where $\rho_1, \rho_2, \ldots, \rho_r$ is a complete set of non-isomorphic irreducible representation of G. For each k we have

$$\begin{aligned}(\alpha'|\chi_{\rho_k}) &= (\alpha|\chi_{\rho_k}) - \sum_{i=1}^{r} (\alpha|\chi_{\rho_i})(\chi_{\rho_i}|\chi_{\rho_k})\\ &= (\alpha|\chi_{\rho_k}) - \sum_{i=1}^{r} (\alpha|\chi_{\rho_i})\delta_{i\,k}\\ &= (\alpha|\chi_{\rho_k}) - (\alpha|\chi_{\rho_k}) = 0,\end{aligned}$$

hence $\alpha' = 0$. So the characters χ_{ρ_i} span $\mathcal{C}(G)$, and orthogonality shows that they are linearly independent, hence they form a basis. $\square$

Recall Theorem 2.14 which says that any representation V can be decomposed into irreducible G-subspaces,

$$V = V_1 \oplus \cdots \oplus V_m.$$

THEOREM 3.16. *Let $V = V_1 \oplus \cdots \oplus V_m$ be a decomposition into irreducible subspaces. If $\rho_k \colon G \to \mathrm{GL}_{\mathbb{C}}(V_k)$ is the representation on V_k and $\rho \colon G \to \mathrm{GL}_{\mathbb{C}}(V)$ is the representation on V, then $(\chi_\rho|\chi_{\rho_k}) = (\chi_{\rho_k}|\chi_\rho)$ is equal to the number of the factors V_j G-equivalent to V_k.*

More generally, if also $W = W_1 \oplus \cdots \oplus W_n$ is a decomposition into irreducible subspaces with $\sigma_k \colon G \to \mathrm{GL}_{\mathbb{C}}(W_k)$ the representation on W_k and $\sigma \colon G \to \mathrm{GL}_{\mathbb{C}}(W)$ is the representation on W, then

$$(\chi_\sigma|\chi_{\rho_k}) = (\chi_{\rho_k}|\chi_\sigma)$$

is equal to the number of the factors W_j G-equivalent to V_k, and

$$\begin{aligned}(\chi_\rho|\chi_\sigma) &= (\chi_\sigma|\chi_\rho)\\ &= \sum_k (\chi_\sigma|\chi_{\rho_k})\\ &= \sum_\ell (\chi_{\sigma_\ell}|\chi_\rho).\end{aligned}$$

3.4. Character tables

The *character table* of a finite group G is the array formed as follows. Its columns correspond to the conjugacy classes of G while its rows correspond to the characters χ_i of the inequivalent irreducible representations of G. The jth conjugacy class C_j is indicated by displaying a representative $c_j \in C_j$. In the (i, j)th entry we put $\chi_i(c_j)$.

	c_1	c_2	$\cdots$	c_n
χ_1	$\chi_1(c_1)$	$\chi_1(c_2)$	$\cdots$	$\chi_1(c_n)$
χ_2	$\chi_2(c_1)$	$\chi_2(c_2)$	$\cdots$	$\chi_2(c_n)$
$\vdots$		$\ddots$		
χ_n	$\chi_n(c_1)$	$\chi_n(c_2)$	$\cdots$	$\chi_n(c_n)$

Conventionally we take $c_1 = e$ and χ_1 to be the *trivial character* corresponding to the trivial 1-dimensional representation. Since $\chi_1(g) = 1$ for $g \in G$, the top of the table will always have the form

	e	c_2	$\cdots$	c_n
χ_1	1	1	$\cdots$	1

Also, the first column will consist of the dimensions of the irreducibles ρ_i, $\chi_i(e)$.

For the symmetric group S_3 we have

	e	$(1\,2)$	$(1\,2\,3)$
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

The representations corresponding to the χ_j will be discussed later. Once we have the character table of a group G we can decompose an arbitrary representation into its irreducible constituents, since if the distinct irreducibles have characters χ_j $(1 \leqslant j \leqslant r)$ then a representation ρ on V has a decomposition

$$V \cong n_1 V_1 \oplus \cdots \oplus n_r V_r,$$

where $n_j V_j \cong V_j \oplus \cdots \oplus V_j$ means a G-subspace isomorphic to the sum of n_j copies of the irreducible representation corresponding to χ_j. Theorem 3.16 now gives $n_j = (\chi_\rho | \chi_j)$. The non-negative integer n_j is called the *multiplicity* of the irreducible V_j in V. The following *irreducibility criterion* is very useful.

PROPOSITION 3.17. *If $\rho\colon G \to \mathrm{GL}_{\mathbb{C}}(V)$ is a non-zero representation, then V is irreducible if and only if $(\chi_\rho|\chi_\rho) = 1$.*

PROOF. If $V = n_1 V_1 \oplus \cdots \oplus n_r V_r$, then by orthonormality of the χ_j,

$$(\chi_\rho|\chi_\rho) = (\sum_i n_i \chi_i | \sum_j n_j \chi_j) = \sum_i \sum_j n_i n_j (\chi_i|\chi_j) = \sum_j n_j^2.$$

So $(\chi_\rho|\chi_\rho) = 1$ if and only if $n_1^2 + \cdots + n_r^2 = 1$. Remembering that the n_j are non-negative integers we see that $(\chi_\rho|\chi_\rho) = 1$ if and only if all but one of the n_j is zero and for some k, $n_k = 1$. Thus $V \cong V_k$ and so is irreducible. □

Notice that for the character table of S_3 we can check that the characters satisfy this criterion and are also orthonormal. Provided we believe that the rows really do represent characters we have found an orthonormal basis for the class functions $\mathcal{C}(S_3)$. We will return to this problem later.

EXAMPLE 3.18. Let us assume that the above character table for S_3 is correct and let $\rho = \rho_{\mathrm{reg}}$ be the regular representation of S_3 on the vector space $V = \mathbb{C}[S_3]$. Let us take as a basis for V the elements of S_3. Then

$$\rho_\sigma \tau = \sigma\tau,$$

hence the matrix $[\rho_\sigma]$ of ρ_σ relative to this basis has 0's down its main diagonal, except when $\sigma = e$ for which it is the 6×6 identity matrix. The character is χ given by

$$\chi(\sigma) = \mathrm{tr}[\rho_\sigma] = \begin{cases} 6 & \text{if } \sigma = e, \\ 0 & \text{otherwise.} \end{cases}$$

Thus we obtain

$$(\chi_\rho|\chi_1) = \frac{1}{6} \sum_{\sigma \in S_3} \chi_\rho(\sigma)\overline{\chi_1(\sigma)} = \frac{1}{6} \times 6 = 1,$$
$$(\chi_\rho|\chi_2) = \frac{1}{6} \sum_{\sigma \in S_3} \chi_\rho(\sigma)\overline{\chi_2(\sigma)} = \frac{1}{6} \times 6 = 1,$$
$$(\chi_\rho|\chi_3) = \frac{1}{6} \sum_{\sigma \in S_3} \chi_\rho(\sigma)\overline{\chi_3(\sigma)} = \frac{1}{6}(6 \times 2) = 2.$$

Hence we have

$$\mathbb{C}[S_3] \cong V_1 \oplus V_2 \oplus V_3 \oplus V_3 = V_1 \oplus V_2 \oplus 2V_3.$$

In fact we have seen the representation V_3 already in Problem Sheet 2, Qu. 5(b). It is easily verified that the character of that representation is χ_3.

Of course, in order to use character tables, we first need to determine them! So far we do not know much about this beyond the fact that the number of rows has to be the same as the number of conjugacy classes of the group G and the existence of the 1-dimensional trivial character which we will always denote by χ_1 and whose value is $\chi_1(g) = 1$ for $g \in G$. The characters of the distinct complex irreducible representations of G are the *irreducible characters of G*.

Theorem 3.19. *Let G be a finite group. Let $\chi_1, \dots, \chi_r$ be the distinct complex irreducible characters and ρ_{reg} the regular representation of G on $\mathbb{C}[G]$.*

(a) *Every complex irreducible representation of G occurs in $\mathbb{C}[G]$. Equivalently, for each irreducible character χ_j, $(\chi_{\rho_{\mathrm{reg}}}|\chi_j) \neq 0$.*
(b) *The multiplicity n_j of the irreducible V_j with character χ_j in $\mathbb{C}[G]$ is given by*

$$n_j = \dim_{\mathbb{C}} V_j = \chi_j(e).$$

So to find all the irreducible characters, we only have to decompose the regular representation!

Proof. Using the formulæ

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

we have

$$n_j = (\chi_{\rho_{\mathrm{reg}}}|\chi_j) = \frac{1}{|G|}\sum_{g\in G} \chi_{\rho_{\mathrm{reg}}}(g)\overline{\chi_j(g)} = \frac{1}{|G|}\chi_{\rho_{\mathrm{reg}}}(e)\overline{\chi_j(e)} = \chi_j(e). \qquad \square$$

Corollary 3.20. *We have*

$$|G| = \sum_{j=1}^{r} n_j^2 = \sum_{j=1}^{r} (\chi_{\rho_{\mathrm{reg}}}|\chi_j)^2.$$

The following result also holds but as the proof requires some Algebraic Number Theory we do not give it.

Proposition 3.21. *For each irreducible character χ_j, $n_j = (\chi_{\rho_{\mathrm{reg}}}|\chi_j)$ divides the order of G, i.e., $n_j \mid |G|$.*

The following row and column orthogonality relations for the character table of a group G are very important.

Theorem 3.22. *Let $\chi_1, \dots, \chi_r$ be the distinct complex irreducible characters of G and $e = g_1, \dots, g_r$ be a collection of representatives for the conjugacy classes of G and for each k, let $\mathrm{C}_G(g_k)$ be the centralizer of g_k.*

(a) **Row orthogonality:** *For $1 \leqslant i, j \leqslant r$,*

$$\sum_{k=1}^{r} \frac{\chi_i(g_k)\overline{\chi_j(g_k)}}{|\,\mathrm{C}_G(g_k)|} = (\chi_i|\chi_j) = \delta_{ij}.$$

(b) **Column orthogonality:** *For* $1 \leqslant i, j \leqslant r$,

$$\sum_{k=1}^{r} \frac{\chi_k(g_i)\overline{\chi_k(g_j)}}{|\operatorname{C}_G(g_i)|} = \delta_{ij}.$$

PROOF.
(a) We have

$$\begin{aligned}
\delta_{ij} = (\chi_i|\chi_j) &= \frac{1}{|G|}\sum_{g\in G}\chi_i(g)\overline{\chi_j(g)} \\
&= \frac{1}{|G|}\sum_{k=1}^{r}\frac{|G|}{|\operatorname{C}_G(g_k)|}\chi_i(g_k)\overline{\chi_j(g_k)}
\end{aligned}$$

[since the conjugacy class of g_k contains $|G|/|\operatorname{C}_G(g_k)|$ elements]

$$= \sum_{k=1}^{r}\frac{\chi_i(g_k)\overline{\chi_j(g_k)}}{|\operatorname{C}_G(g_k)|}.$$

(b) Let $\psi_s \colon G \to \mathbb{C}$ be the function given by

$$\psi_s(g) = \begin{cases} 1 & \text{if } g \text{ is conjugate to } g_s, \\ 0 & \text{if } g \text{ is not conjugate to } g_s. \end{cases}$$

By Theorem 3.15, there are $\lambda_k \in \mathbb{C}$ such that

$$\psi_s = \sum_{k=1}^{r}\lambda_k\chi_k.$$

But then $\lambda_j = (\psi_s|\chi_j)$. We also have

$$\begin{aligned}
(\psi_s|\chi_j) &= \frac{1}{|G|}\sum_{g\in G}\psi_s(g)\overline{\chi_j(g)} \\
&= \sum_{k=1}^{r}\frac{\psi_s(g_k)\overline{\chi_j(g_k)}}{|\operatorname{C}_G(g_k)|} \\
&= \frac{\overline{\chi_j(g_s)}}{|\operatorname{C}_G(g_s)|},
\end{aligned}$$

hence

$$\psi_s = \sum_{j=1}^{r}\frac{\overline{\chi_j(g_s)}}{|\operatorname{C}_G(g_s)|}\chi_j.$$

Thus we have the required formula

$$\delta_{st} = \psi_s(g_t) = \sum_{j=1}^{r}\frac{\chi_j(g_t)\overline{\chi_j(g_s)}}{|\operatorname{C}_G(g_s)|}. \qquad \square$$

3.5. Examples of character tables

Equipped with the results of the last section, we can proceed to find some character tables. For abelian groups we have the following result which follows from what we have seen already together with the fact that in an abelian group every conjugacy class has exactly one element.

PROPOSITION 3.23. *Let G be a finite abelian group. Then there are $|G|$ distinct complex irreducible characters, each of which is 1-dimensional. Moreover, in the regular representation each irreducible occurs with multiplicity 1, i.e.,*

$$\mathbb{C}[G] \cong V_1 \oplus \cdots \oplus V_{|G|}.$$

EXAMPLE 3.24. Let $G = \langle g_0 \rangle \cong \mathbb{Z}/n$ be cyclic of order n. Let $\zeta_n = e^{2\pi i/n}$, the 'standard' primitive n-th root of unity. Then for each $k = 0, 1, \ldots, (n-1)$ we may define a 1-dimensional representation $\rho_k \colon G \to \mathbb{C}^\times$ by

$$\rho_k(g_0^r) = \zeta_n^{rk}.$$

The character of ρ_k is χ_k given by

$$\chi_k(g_0^r) = \zeta_n^{rk}.$$

Clearly these are all irreducible and non-isomorphic.

Let us consider the orthogonality relations for these characters. We have

$$\begin{aligned}(\chi_k|\chi_k) &= \frac{1}{n}\sum_{r=0}^{n-1} \chi_k(g_0^r)\overline{\chi_k(g_0^r)} \\ &= \frac{1}{n}\sum_{r=0}^{n-1} \zeta_n^{kr}\overline{\zeta_n^{kr}} \\ &= \frac{1}{n}\sum_{r=0}^{n-1} 1 = \frac{n}{n} = 1.\end{aligned}$$

For $0 \leqslant k < \ell \leqslant (n-1)$ we have

$$\begin{aligned}(\chi_k|\chi_\ell) &= \frac{1}{n}\sum_{r=0}^{n-1} \chi_k(g_0^r)\overline{\chi_\ell(g_0^r)} \\ &= \frac{1}{n}\sum_{r=0}^{n-1} \zeta_n^{kr}\overline{\zeta_n^{\ell r}} \\ &= \frac{1}{n}\sum_{r=0}^{n-1} \zeta_n^{(k-\ell)r}.\end{aligned}$$

By row orthogonality this sum is 0. This is a special case of the following identity which is often used in many parts of Mathematics.

LEMMA 3.25. *Let $d \in \mathbb{N}$, $m \in \mathbb{Z}$ and $\zeta_d = e^{2\pi i/d}$. Then*

$$\sum_{r=0}^{d-1} \zeta_d^{mr} = \begin{cases} d & \text{if } d \mid m, \\ 0 & \text{otherwise.}\end{cases}$$

PROOF. We give a proof which does *not* use character theory!

If $d \nmid m$, then $\zeta_d^m \neq 1$. Then we have

$$\begin{aligned}\zeta_d^m \sum_{r=0}^{d-1} \zeta_d^{mr} &= \sum_{r=0}^{d-1} \zeta_d^{m(r+1)} \\ &= \sum_{s=1}^{d} \zeta_d^{ms} \\ &= \sum_{r=0}^{d-1} \zeta_d^{mr},\end{aligned}$$

hence

$$(\zeta_d^m - 1) \sum_{r=0}^{d-1} \zeta_d^{mr} = 0,$$

and so

$$\sum_{r=0}^{d-1} \zeta_d^{mr} = 0.$$

If $d \mid m$ then

$$\sum_{r=0}^{d-1} \zeta_d^{mr} = \sum_{r=0}^{d-1} 1 = d.$$

□

As a special case of Exercise 3.24, consider the case where $n = 3$ and $G = \langle g_0 \rangle \cong \mathbb{Z}/3$. The character table of G is

	e	g_0	g_0^2
χ_1	1	1	1
χ_2	1	ζ_3	ζ_3^2
χ_3	1	ζ_3^2	ζ_3

EXAMPLE 3.26. Let $G = \langle a_0, b_0 \rangle$ be abelian of order 4, so $G \cong \mathbb{Z}/2 \times \mathbb{Z}/2$. The character table of G is as follows.

	e	a_0	b_0	a_0b_0
$\chi_1 = \chi_{00}$	1	1	1	1
χ_{10}	1	-1	1	-1
χ_{01}	1	1	-1	-1
χ_{11}	1	-1	-1	1

EXAMPLE 3.27. The character table of the quaternion group of order 8, Q_8, is as follows.

	$\mathbf{1}$	$\mathbf{-1}$	$\mathbf{i}$	$\mathbf{j}$	$\mathbf{k}$
χ_1	1	1	1	1	1
$\chi_{\mathbf{i}}$	1	1	1	-1	-1
$\chi_{\mathbf{j}}$	1	1	-1	1	-1
$\chi_{\mathbf{k}}$	1	1	-1	-1	1
χ_2	2	-2	0	0	0

PROOF. There are 5 conjugacy classes:

$$\{\mathbf{1}\},\ \{-\mathbf{1}\},\ \{\mathbf{i},-\mathbf{i}\},\ \{\mathbf{j},-\mathbf{j}\},\ \{\mathbf{k},-\mathbf{k}\}.$$

As always we have the trivial character χ_1. There are 3 homomorphisms $Q_8 \to \mathbb{C}^\times$ given by

$$\begin{aligned} \rho_{\mathbf{i}}(\mathbf{i}^r) &= 1 \quad \text{and} \quad \rho_{\mathbf{i}}(\mathbf{j}) = \rho_{\mathbf{i}}(\mathbf{k}) = -1, \\ \rho_{\mathbf{j}}(\mathbf{j}^r) &= 1 \quad \text{and} \quad \rho_{\mathbf{j}}(\mathbf{i}) = \rho_{\mathbf{i}}(\mathbf{k}) = -1, \\ \rho_{\mathbf{k}}(\mathbf{k}^r) &= 1 \quad \text{and} \quad \rho_{\mathbf{k}}(\mathbf{i}) = \rho_{\mathbf{k}}(\mathbf{j}) = -1. \end{aligned}$$

These provide three 1-dimensional representations with characters $\chi_{\mathbf{i}}, \chi_{\mathbf{j}}, \chi_{\mathbf{k}}$ taking values

$$\begin{aligned} \chi_{\mathbf{i}}(\mathbf{i}^r) &= 1 \quad \text{and} \quad \chi_{\mathbf{i}}(\mathbf{j}) = \chi_{\mathbf{i}}(\mathbf{k}) = -1, \\ \chi_{\mathbf{j}}(\mathbf{j}^r) &= 1 \quad \text{and} \quad \chi_{\mathbf{j}}(\mathbf{i}) = \chi_{\mathbf{i}}(\mathbf{k}) = -1, \\ \chi_{\mathbf{k}}(\mathbf{k}^r) &= 1 \quad \text{and} \quad \chi_{\mathbf{k}}(\mathbf{i}) = \chi_{\mathbf{k}}(\mathbf{j}) = -1. \end{aligned}$$

Since $|Q_8| = 8$, we might try looking for a 2-dimensional complex representation. But the definition of Q_8 provides us with the inclusion homomorphism $j\colon Q_8 \to \mathrm{GL}_{\mathbb{C}}(\mathbb{C}^2)$, where we interpret the matrices as taken in terms of the standard basis. The character of this representation is χ_2 given by

$$\chi_2(\mathbf{1}) = 2,\ \chi_2(-\mathbf{1}) = -2,\ \chi_2(\pm\mathbf{i}) = \chi_2(\pm\mathbf{j}) = \chi_2(\pm\mathbf{k}) = 0.$$

This completes the determination of the character table of Q_8. □

EXAMPLE 3.28. The character table of the dihedral group of order 8, D_8, is as follows.

	e	α^2	α	β	$\alpha\beta$
χ_1	1	1	1	1	1
χ_2	1	1	1	-1	-1
χ_3	1	1	-1	1	-1
χ_4	1	1	-1	-1	1
χ_5	2	-2	0	0	0

PROOF. The elements of D_8 are

$$e, \alpha, \alpha^2, \alpha^3, \beta, \alpha\beta, \alpha^2\beta, \alpha^3\beta$$

and these satisfy the relations

$$\alpha^4 = e = \beta^2, \quad \beta\alpha\beta = \alpha^{-1}.$$

The conjugacy classes are the sets

$$\{e\},\ \{\alpha^2\},\ \{\alpha,\alpha^3\},\ \{\beta,\alpha^2\beta\},\ \{\alpha\beta,\alpha^3\beta\}.$$

There are two obvious 1-dimensional representations, namely the trivial one ρ_1 and also ρ_2, where

$$\rho_2(\alpha) = 1, \quad \rho_2(\beta) = -1.$$

The character of ρ_2 is determined by

$$\chi_2(\alpha^r) = 1, \quad \chi_2(\beta\alpha^r) = -1.$$

A third 1-dimensional representation comes from the homomorphism $\rho_3\colon D_8 \to \mathbb{C}^\times$ given by

$$\rho_3(\alpha) = -1, \quad \rho_3(\beta) = 1.$$

The fourth 1-dimensional representation comes from the homomorphism $\rho_4 \colon D_8 \to \mathbb{C}^\times$ for which

$$\rho_4(\alpha) = -1, \quad \rho_4(\beta) = -1.$$

The characters $\chi_1, \chi_2, \chi_3, \chi_4$ are clearly distinct and thus orthonormal.

Before describing χ_5 as the character of a 2-dimensional representation, we will determine it up to a scalar factor. Suppose that

$$\chi_5(e) = a,\ \chi_5(\alpha^2) = b,\ \chi_5(\alpha) = c,\ \chi_5(\beta) = d,\ \chi_5(\beta\alpha) = e$$

for $a, b, c, d, e \in \mathbb{C}$. The orthonormality conditions give $(\chi_5|\chi_j) = \delta_{j\,5}$. For $j = 1, 2, 3, 4$, we obtain the following linear system:

$$\begin{bmatrix} 1 & 1 & 2 & 2 & 2 \\ 1 & 1 & 2 & -2 & -2 \\ 1 & 1 & -2 & 2 & -2 \\ 1 & 1 & -2 & -2 & 2 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \\ d \\ e \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \tag{3.1}$$

which has solutions

$$b = -a, \quad c = d = e = 0.$$

If χ_5 is an irreducible character we must also have $(\chi_5|\chi_5) = 1$, giving

$$1 = \frac{1}{8}\left(a^2 + a^2\right) = \frac{a^2}{4},$$

and so $a = \pm 2$. So we must have the stated bottom row. The corresponding representation appears in Example 2.6 where it is viewed as a complex representation which is easily seen to have character χ_5. □

Remark 3.29. The groups Q_8 and D_8 have identical character tables even though they are non-isomorphic! This shows that character tables do not always distinguish non-isomorphic groups.

Example 3.30. The character table of the symmetric group S_4, is as follows.

	e [1]	$(1\,2)$ [6]	$(1\,2)(3\,4)$ [3]	$(1\,2\,3)$ [8]	$(1\,2\,3\,4)$ [6]
χ_1	1	1	1	1	1
χ_2	1	-1	1	1	-1
χ_3	3	1	-1	0	-1
χ_4	3	-1	-1	0	1
χ_5	2	0	2	-1	0

Proof. Recall that the conjugacy classes correspond to the different cycle types which are represented by the elements in the following list, where the numbers in brackets [ ] give the sizes of the conjugacy classes:

$$e\ [1],\ (1\,2)\ [6], (1\,2)(3\,4)\ [3],\ (1\,2\,3)\ [8],\ (1\,2\,3\,4)\ [6].$$

So there are 5 rows and columns in the character table. The sign representation $\mathrm{sign} \colon S_4 \to \mathbb{C}^\times$ is 1-dimensional and has character

$$\chi_2(e) = \chi_2((1\,2)(3\,4)) = \chi_2(1\,2\,3) = 1 \quad \text{and} \quad \chi_2(1\,2) = \chi_2(1\,2\,3\,4) = -1.$$

The 4-dimensional permutation representation $\tilde{\rho}_4$ corresponding to the action on $\mathbf{4} = \{1, 2, 3, 4\}$ has character $\chi_{\tilde{\rho}_4}$ given by

$$\chi_{\tilde{\rho}_4}(\sigma) = \text{number of fixed points of } \sigma.$$

So we have

$$\chi_{\tilde{\rho}_4}(e) = 4,\ \chi_{\tilde{\rho}_4}((1\,2)(3\,4)) = \chi_{\tilde{\rho}_4}(1\,2\,3\,4) = 0,\ \chi_{\tilde{\rho}_4}(1\,2\,3) = 1,\ \chi_{\tilde{\rho}_4}(1\,2) = 2.$$

We know that this representation has the form

$$\mathbb{C}[\mathbf{4}] = \mathbb{C}[\mathbf{4}]^{S_4} \oplus W$$

where W is a 3-dimensional S_4-subspace whose character χ_3 is determined by

$$\chi_1 + \chi_3 = \chi_{\tilde{\rho}_4},$$

hence

$$\chi_3 = \chi_{\tilde{\rho}_4} - \chi_1.$$

So we obtain the following values for χ_3

$$\chi_3(e) = 3,\ \chi_3((1\,2)(3\,4)) = \chi_3(1\,2\,3\,4) = -1,\ \chi_3(1\,2\,3) = 0,\ \chi_3(1\,2) = 1.$$

Calculating the inner product of this with itself gives

$$(\chi_3|\chi_3) = \frac{1}{24}\,(9 + 6 + 3 + 0 + 6) = 1,$$

and so χ_3 is the character of an irreducible representation.

From this information we can deduce that the two remaining irreducibles must have dimensions n_4, n_5 for which

$$n_4^2 + n_5^2 = 24 - 1 - 1 - 9 = 13,$$

and thus we can take $n_4 = 3$ and $n_5 = 2$, since these are the only possible values up to order.

If we form the tensor product $\rho_2 \otimes \rho_3$ we get a character χ_4 given by

$$\chi_4(g) = \chi_2(g)\chi_3(g),$$

hence the 4-th line in the table. Then $(\chi_4|\chi_4) = 1$ and so χ_4 really is an irreducible character.

For χ_5, recall that the regular representation ρ_{reg} has character $\chi_{\rho_{\text{reg}}}$ decomposing as

$$\chi_{\rho_{\text{reg}}} = \chi_1 + \chi_2 + 3\chi_3 + 3\chi_4 + 2\chi_5,$$

hence we have

$$\chi_5 = \frac{1}{2}\left(\chi_{\rho_{\text{reg}}} - \chi_1 - \chi_2 - 3\chi_3 - 3\chi_4\right),$$

which gives the last row of the table. $\square$

Notice that in this example, the tensor product $\rho_3 \otimes \rho_5$ which is a 6-dimensional representation that cannot be irreducible. Its character $\chi_{\rho_3 \otimes \rho_5}$ must be a linear combination of the irreducibles,

$$\chi_{\rho_3 \otimes \rho_5} = \sum_{j=1}^{5} (\chi_{\rho_3 \otimes \rho_5}|\chi_j)\chi_j.$$

Recall that for $g \in S_4$,

$$\chi_{\rho_3 \otimes \rho_5}(g) = \chi_{\rho_3}(g)\chi_{\rho_5}(g).$$

For the values of the coefficients we have

$$\begin{aligned}
(\chi_{\rho_3\otimes\rho_5}|\chi_1) &= \frac{1}{24}(6+0-6+0+0) = 0,\\
(\chi_{\rho_3\otimes\rho_5}|\chi_2) &= \frac{1}{24}(6+0-6+0+0) = 0,\\
(\chi_{\rho_3\otimes\rho_5}|\chi_3) &= \frac{1}{24}(18+0+6+0+0) = 1,\\
(\chi_{\rho_3\otimes\rho_5}|\chi_4) &= \frac{1}{24}(18+0+6+0+0) = 1,\\
(\chi_{\rho_3\otimes\rho_5}|\chi_5) &= \frac{1}{24}(12+0-12+0+0) = 0.
\end{aligned}$$

Thus we have

$$\chi_{\rho_3\otimes\rho_5} = \chi_3 + \chi_4.$$

In general it is hard to predict how the tensor product of representations decomposes in terms of irreducibles.

3.6. Reciprocity formulae

Let $H \leqslant G$, let $\rho\colon G \to \mathrm{GL}_{\mathbb{C}}(V)$ be a representation of G and let $\sigma\colon H \to \mathrm{GL}_{\mathbb{C}}(W)$ be a representation of H. Recall that the induced representation $\operatorname{ind}_H^G \sigma = \sigma\uparrow_H^G$ is of dimension $|G/H| \dim_{\mathbb{C}} W$, while the restriction $\operatorname{res}\rho_H^G = \rho\downarrow_H^G$ has dimension $\dim_{\mathbb{C}} V$. We will write $\chi_\rho\downarrow_H^G$ and $\chi_\sigma\uparrow_H^G$ for the characters of these representations. First we show how to calculate the character of an induced representation.

Lemma 3.31. *The character of the induced representation $\sigma\uparrow_H^G$ is given by*

$$\chi_\sigma\uparrow_H^G(g) = \frac{1}{|H|}\sum_{\substack{x\in G\\ g\in xHx^{-1}}} \chi_\sigma(x^{-1}gx).$$

Proof. See [**1**, §16]. □

Example 3.32. Let $H = \{e, \alpha, \alpha^2, \alpha^3\} \leqslant D_8$ and let $\sigma\colon H \to \mathbb{C}^\times$ be the 1-dimensional representation of H for which

$$\sigma(\alpha^k) = i^k.$$

Decompose the induced representation $\sigma\uparrow_H^{D_8}$ into its irreducible summands over the group D_8.

Proof. We will use the character table of D_8 given in Example 3.28. Notice that $H \lhd D_8$, hence for $x \in D_8$ we have $xHx^{-1} = H$. Let $\chi = \chi_\sigma\uparrow_H^{D_8}$ be the character of this induced representation. We have

$$\begin{aligned}
\chi(g) &= \frac{1}{4}\sum_{\substack{x\in D_8\\ g\in xHx^{-1}}} \chi_\sigma(x^{-1}gx)\\
&= \begin{cases} \dfrac{1}{4}\displaystyle\sum_{x\in D_8} \chi_\sigma(x^{-1}gx) & \text{if } g \in H,\\[2ex] 0 & \text{if } g \notin H. \end{cases}
\end{aligned}$$

Thus if $g \in H$ we find that

$$\chi(g) = \begin{cases} \frac{1}{4}\left(4\chi_\sigma(\alpha) + 4\chi_\sigma(\alpha^3)\right) & \text{if } g = \alpha, \alpha^3, \\ \frac{1}{4}\left(8\chi_\sigma(\alpha^2)\right) & \text{if } g = \alpha^2, \\ \frac{1}{4}\left(8\chi_\sigma(e)\right) & \text{if } g = e. \end{cases}$$

Hence we have

$$\chi(g) = \begin{cases} i + i^3 = 0 & \text{if } g = \alpha, \alpha^3, \\ -2 & \text{if } g = \alpha^2, \\ \ \ 2 & \text{if } g = e, \\ \ \ 0 & \text{if } g \notin H. \end{cases}$$

Taking inner products with the irreducible characters χ_j we obtain the following.

$$\begin{aligned} (\chi|\chi_1)_{D_8} &= \frac{1}{8}(2 - 2 + 0 + 0 + 0) = 0, \\ (\chi|\chi_2)_{D_8} &= \frac{1}{8}(2 - 2 + 0 + 0 + 0) = 0, \\ (\chi|\chi_3)_{D_8} &= \frac{1}{8}(2 - 2 + 0 + 0 + 0) = 0, \\ (\chi|\chi_4)_{D_8} &= \frac{1}{8}(2 - 2 + 0 + 0 + 0) = 0, \\ (\chi|\chi_5)_{D_8} &= \frac{1}{8}(4 + 4 + 0 + 0 + 0) = 1. \end{aligned}$$

Hence we must have $\chi = \chi_5$, giving another derivation of the representation ρ_5. □

THEOREM 3.33 (**Frobenius Reciprocity**). *There is a linear isomorphism*

$$\operatorname{Hom}_G(W \uparrow_H^G, V) \cong \operatorname{Hom}_H(W, V \downarrow_H^G).$$

Equivalently on characters we have

$$(\chi_\sigma \uparrow_H^G |\chi_\rho)_G = (\chi_\sigma|\chi_\rho \downarrow_H^G)_H.$$

PROOF. See [**1**, §16]. □

EXAMPLE 3.34. Let σ be the irreducible representation of S_3 with character χ_3 and underlying vector space W. Decompose the induced representation $W \uparrow_{S_3}^{S_4}$ into its irreducible summands over the group S_4.

PROOF. Let

$$W \uparrow_{S_3}^{S_4} \cong n_1V_1 \oplus n_2V_2 \oplus n_3V_3 \oplus n_4V_4 \oplus n_5V_5.$$

Then

$$n_j = (\chi_j|\chi_\sigma \uparrow_{S_3}^{S_4})_{S_4} = (\chi_j \downarrow_{S_3}^{S_4} |\chi_\sigma)_{S_3}.$$

To evaluate the restriction $\chi_j \downarrow_{S_3}^{S_4}$ we take only elements of S_4 lying in S_3. Hence we have

$$\begin{aligned}
n_1 &= (\chi_1 \downarrow_{S_3}^{S_4} | \chi_\sigma)_{S_3} = \frac{1}{6}(2+0-2) = 0, \\
n_2 &= (\chi_2 \downarrow_{S_3}^{S_4} | \chi_\sigma)_{S_3} = \frac{1}{6}(1\cdot 2+0+1\cdot(-2)) = 0, \\
n_3 &= (\chi_3 \downarrow_{S_3}^{S_4} | \chi_\sigma)_{S_3} = \frac{1}{6}(3\cdot 2+0+0\cdot(-2)) = 1, \\
n_4 &= (\chi_4 \downarrow_{S_3}^{S_4} | \chi_\sigma)_{S_3} = \frac{1}{6}(3\cdot 2+0+0\cdot(-2)) = 1, \\
n_5 &= (\chi_5 \downarrow_{S_3}^{S_4} | \chi_\sigma)_{S_3} = \frac{1}{6}(2\cdot 2+0+-2\cdot(-1)) = \frac{6}{6} = 1.
\end{aligned}$$

Hence we have

$$W \uparrow_{S_3}^{S_4} \cong V_3 \oplus V_4 \oplus V_5. \qquad \square$$

The following result also shows how induction and restriction interact. It is often called the *Mackey double coset formula*. We will explain the ingredients after the statement.

THEOREM 3.35. *Let G be a finite group and let $H \leqslant G$ and $K \leqslant G$ be subgroups. Let U be a complex representation of K. Then*

$$\operatorname{res}_H^G \operatorname{ind}_K^G U \cong \bigoplus_{g:K\backslash G/K} \operatorname{ind}_{H\cap gKg^{-1}}^H \operatorname{res}_{H\cap gKg^{-1}}^{gKg^{-1}} [g]U$$

where the sum is taken over a complete set of double coset representatives for G with respect to K. If the character of U is χ, then

$$\chi \uparrow_K^G \downarrow_H^G = \sum_{g:K\backslash G/K} ([g]U) \downarrow_{H\cap gKg^{-1}}^{gKg^{-1}} \uparrow_{H\cap gKg^{-1}}^H .$$

EXPLANATION OF INGREDIENTS.
$[g]U$: The group K acts on U, so there is an induced action of gKg^{-1} given by

$$gkg^{-1}\cdot u = ku$$

for $k \in K$, $u \in U$. We denote the associated representation by $[g]U$.
Double cosets: Given a subgroup $K \leqslant G$, there is an action of $K \times K$ on the set G given by

$$(h_1, h_2)\cdot g = h_1 g h_2^{-1}.$$

The orbit of this action containing g is written KgK and is called a *double coset*. If $K \lhd G$ then $KgK = gK = Kg$, but for non-normal subgroups double cosets are unions of left (or right cosets). A *complete set of double coset representatives for G with respect to K* is a subset $S \subseteq G$ such that every double coset contains exactly one element $s \in S$. $\square$

When $K \lhd G$, this formula becomes

$$\operatorname{res}_H^G \operatorname{ind}_K^G U \cong \bigoplus_{g:G/K} \operatorname{ind}_{H\cap K}^H \operatorname{res}_{H\cap K}^K [g]U$$

where the sum is over a complete set of representatives for the left cosets of G with respect to K.

3.7. Representations of semi-direct products

Recall the notion of a *semi-direct product* $G = N \rtimes H$; this has $N \lhd G$, $H \leqslant G$, $H \cap N = \{e\}$ and $HN = NH = G$. We will describe a way to produce the irreducible characters of G from those of the groups $N \lhd G$ and $H \leqslant G$.

PROPOSITION 3.36. *Let $\varphi\colon Q \to G$ be a homomorphism and let $\rho\colon G \to \mathrm{GL}_{\mathbb{C}}(V)$ be a representation of G. Then the composite $\varphi^*\rho = \rho \circ \varphi$ is a representation of Q on V. Moreover, if $\varphi^*\rho$ is irreducible over Q, then ρ is irreducible over G.*

PROOF. The first part is clear.

For the second, suppose that $W \subseteq V$ is a G-subspace. Then for $h \in Q$ and $w \in W$ we have

$$(\varphi^*\rho)_h w = \rho_{\varphi(h)} w \in W.$$

Hence W is a Q-subspace. By irreducibility of $\varphi^*\rho$, $W = \{0\}$ or $W = V$, hence V is irreducible over G. $\square$

The representation $\varphi^*\rho$ is called the representation on V *induced* by φ and we often denote the underlying Q-module by φ^*V. If $j\colon Q \to G$ is the inclusion of a subgroup, then $j^*\rho = \rho\downarrow_Q^G$, the restriction of ρ to Q.

In the case of $G = N \rtimes H$, there is a surjection $\pi\colon G \to H$ given by

$$\pi(nh) = h \quad (n \in N,\ h \in H),$$

as well as the inclusions $i\colon N \to G$ and $j\colon H \to G$. We can apply the above to each of these homomorphisms.

Now let $\rho\colon G \to \mathrm{GL}_{\mathbb{C}}(V)$ be an irreducible representation of the semi-direct product $G = N \rtimes H$. Then i^*V decomposes as

$$i^*V = W_1 \oplus \cdots \oplus W_m$$

where W_k is a non-zero irreducible N-subspace. For each $g \in G$, notice that if $x \in N$ and $w \in W_1$, then

$$\rho_x(\rho_g w) = \rho_{xg} w = \rho_g \rho_{g^{-1}xg} w = \rho_g w'$$

for $w' = \rho_{g^{-1}xg} w$. Since $g^{-1}xg \in g^{-1}Ng = N$,

$$gW_1 = \{\rho_g w : w \in W_1\}$$

is an N-subspace of i^*V. If we take

$$\tilde{W}_1 = \left\{ \sum_{g \in G} \rho_g w_g : w_g \in W_1 \right\},$$

then we can verify that $\tilde{W}_1$ is a non-zero N-subspace of i^*V and in fact is also a G-subspace of V. Since V is irreducible, this shows that $V = \tilde{W}_1$.

Now let

$$H_1 = \{h \in H : hW_1 = W_1\} \subseteq H.$$

Then we can verify that $H_1 \leqslant H \leqslant G$. The semidirect product

$$G_1 = N \rtimes H_1 = \{nh \in G : n \in N,\ h \in H_1\} \leqslant G$$

also acts on W_1 since for $nh \in G_1$ and $w \in W_1$,

$$\rho_{nh} w = \rho_n \rho_h w = \rho_n w'' \in W_1$$

where $w'' = \rho_h w$; hence W_1 is a G_1-subspace of $V \downarrow^G_{G_1}$. Notice that by the second part of Proposition 3.36, W_1 is irreducible over G_1.

LEMMA 3.37. *There is a G-isomorphism*

$$W_1 \uparrow^G_{G_1} \cong V.$$

PROOF. See the books [**3, 4**]. □

Thus every irreducible of $G = N \rtimes H$ arises from an irreducible representation of N which extends to a representation (actually irreducible) of such a subgroup $N \rtimes K \leqslant N \rtimes H = G$ for $K \leqslant H$ but to no larger subgroup.

EXAMPLE 3.38. Let D_{2n} be the dihedral group of order $2n$. Then every irreducible representation of D_{2n} has dimension 1 or 2.

PROOF. We have $D_{2n} = N \rtimes H$ where $N = \langle \alpha \rangle \cong \mathbb{Z}/n$ and $H = \{e, \beta\}$. The n distinct irreducibles ρ_k of N are all 1-dimensional by Example 3.24. Hence for each of these we have a subgroup $H_k \leqslant H$ such that the action of N extends to $N \rtimes H_k$ and so the corresponding induced representation $V_k \uparrow^{D_{2n}}_{H_k}$ is irreducible and has dimension $|D_{2n}/(N \rtimes H_k)| = 2/|H_k|$. Every irreducible of D_{2n} occurs this way. □

For $n = 4$, it is a useful exercise to identify the irreducibles in the character table in this way.

3.8. Real representations

This section is inspired by [**4**, §13.2], to which the reader is referred for details.

Suppose that $\rho \colon G \to \mathrm{GL}_{\mathbb{C}}(V)$ is an irreducible complex representation of a finite group G, where $\dim_{\mathbb{C}} V = n$. We can view V as a real vector space and then $\dim_{\mathbb{R}} V = 2n$. Thus we have an underlying real representation $\rho_{\mathbb{R}} \colon G \to \mathrm{GL}_{\mathbb{R}}(V)$.

If we view $\mathbb{C}$ as a 2-dimensional $\mathbb{R}$-vector space, then we can consider the $4n$-dimensional real vector space $\mathbb{C} \otimes_{\mathbb{R}} V$ as a $2n$-dimensional $\mathbb{C}$-vector space by defining scalar multiplication on basic tensors to be given by

$$z \cdot (w \otimes v) = (zw) \otimes v$$

for $z, w \in \mathbb{C}$ and $v \in V$. A basis $\{v_1, \ldots, v_n\}$ for V as a $\mathbb{C}$-vector space gives rise to a basis $\{1 \otimes v_1, i \otimes v_1, 1 \otimes v_2, i \otimes v_2, \ldots, 1 \otimes v_n, i \otimes v_n\}$ for $\mathbb{C} \otimes_{\mathbb{R}} V$ as a $\mathbb{C}$-vector space. Furthermore, there is an action of G on $\mathbb{C} \otimes_{\mathbb{R}} V$ given on basic tensors by

$$g \cdot (w \otimes v) = w \otimes \rho_g v.$$

It is easy to see that this is $\mathbb{C}$-linear and so we obtain a $2n$-dimensional complex representation

$$\mathbb{C} \otimes \rho_{\mathbb{R}} \colon G \to \mathrm{GL}_{\mathbb{C}}(\mathbb{C} \otimes_{\mathbb{R}} V),$$

called the *complexification* of the real representation $\rho_{\mathbb{R}}$. It is not difficult to see that

$$\chi_{\mathbb{C} \otimes \rho_{\mathbb{R}}} = \chi_\rho + \overline{\chi}_\rho. \tag{3.2}$$

Notice that when χ_ρ takes only real values,

$$2\chi_{\mathbb{C}\otimes\rho_{\mathbb{R}}} = \chi_\rho,$$

so $\mathbb{C}\otimes\rho_{\mathbb{R}} = 2\rho = \rho + \rho$.

There are 3 different mutually exclusive situations that can occur.

(A) $\chi_\rho \neq \overline{\chi}_\rho$.

(B) $\chi_\rho = \overline{\chi}_\rho$ and $\rho = \mathbb{C}\otimes_{\mathbb{R}}\rho_0$ for some real representation ρ_0 of G.

(C) $\chi_\rho = \overline{\chi}_\rho$ but ρ is not the complexification of a real representation.

Exercises on Chapter 3

3-1. Determine the characters of the representations in Questions 1,2,3 of Chapter 2.

3-2. Let $\rho_c\colon G \to \mathrm{GL}_{\mathbb{C}}(\mathbb{C}[G_c])$ denote the permutation representation associated to the conjugation action of G on its own underlying set G_c, i.e., $g \cdot x = gxg^{-1}$. Let $\chi_c = \chi_{\rho_c}$ be the character of ρ_c.

(i) For $x \in G$ show that the vector subspace V_x spanned by all the conjugates of x is a G-subspace. What is $\dim V_x$?

(ii) For $g \in G$ show that $\chi_c(g) = |\,\mathrm{C}_G(g)|$ where $\mathrm{C}_G(g)$ is the centralizer of g in G.

(iii) For any class function $\alpha \in \mathcal{C}(G)$ determine $(\alpha|\chi_c)$.

(iv) If $\chi_1, \ldots, \chi_r$ are the distinct irreducible characters of G and $\rho_1, \ldots, \rho_r$ are the corresponding irreducible representations, determine the multiplicity of ρ_j in $\mathbb{C}[G_c]$.

(v) Carry out these calculations for the groups S_3, S_4, A_4, D_8, Q_8.

3-3. Let G be a finite group and $H \leqslant G$ a subgroup. Consider the set of cosets G/H as a G-set with action given by $g \cdot xH = gxH$ and let ρ be the associated permutation representation on $\mathbb{C}[G/H]$.

(i) Show that for $g \in G$,

$$\chi_\rho(g) = |\{xH \in G/H : g \in xHx^{-1}\}|.$$

(ii) If $H \lhd G$ (i.e., H is a normal subgroup), show that

$$\chi_\rho(g) = \begin{cases} 0 & \text{if } g \notin H, \\ |G/H| & \text{if } g \in H. \end{cases}$$

(iii) Determine the character χ_ρ when $G = S_4$ (the permutation group of the set $\{1, 2, 3, 4\}$) and $H = S_3$ (viewed as the subgroup of all permutations fixing 4).

3-4. Let $\rho\colon G \to \mathrm{GL}_{\mathbb{C}}(W)$ be a representation and let $\rho_j\colon G \to \mathrm{GL}_{\mathbb{C}}(V_j)$ $(j = 1, \ldots, r)$ be the distinct irreducible representations of G with characters $\chi_j = \chi_{\rho_j}$.

(i) For each i, show that $\varepsilon_i\colon W \to W$ is a G-linear transformation, where

$$\varepsilon_i(w) = \frac{\chi_i(e)}{|G|}\sum_{g\in G}\overline{\chi_i(g)}\rho_g w.$$

(ii) Let $W_{j,k} \subseteq W$ be non-zero G-subspaces such that

$$W = W_{1,1} \oplus \cdots \oplus W_{1,s_1} \oplus W_{2,1} \oplus \cdots \oplus W_{2,s_2} \oplus \cdots \oplus W_{r,1} \oplus \cdots \oplus W_{r,s_r}$$

and $W_{j,k}$ is G-isomorphic to V_j. Show that if $w \in W_{j,k}$ then $\varepsilon_i(w) \in W_{j,k}$.

(iii) By considering for each pair j, k the restriction of ε_i to a G-linear transformation $\varepsilon_i' \colon W_{j,k} \to W_{j,k}$, show that if $w \in W_{j,k}$ then

$$\varepsilon_i(w) = \begin{cases} w & \text{if } i = j, \\ 0 & \text{otherwise.} \end{cases}$$

Deduce that $\operatorname{im} \varepsilon_i = W_{i,1} \oplus \cdots W_{i,s_i}$.

[Remark: *The subspace $W_i = \operatorname{im} \varepsilon_i$ is called the* subspace associated to the irreducible *ρ_i and depends only on ρ and ρ_i. Consequently, the decomposition $W = W_1 \oplus \cdots \oplus W_r$ is called the* canonical decomposition *of W. Given each W_j, there are many different ways to decompose it into irreducible G-isomorphic to V_j, hence the original finer decomposition is* non-canonical.]

(iv) Show that

$$\varepsilon_i \circ \varepsilon_j = \begin{cases} \varepsilon_i & \text{if } i = j, \\ 0 & \text{otherwise.} \end{cases}$$

(v) For the group S_3, use these ideas to find the canonical decomposition for the regular representation $\mathbb{C}[S_3]$. Repeat this for some other groups and non-irreducible representations.

3-5. Let A_4 be the alternating group and $\zeta = e^{2\pi i/3} \in \mathbb{C}$.

(i) Verify the *orthogonality relations* for the character table of A_4 given below.

	e	$(1\,2)(3\,4)$	$(1\,2\,3)$	$(1\,3\,2)$
	[1]	[3]	[4]	[4]
χ_1	1	1	1	1
χ_2	1	1	ζ	ζ^{-1}
χ_3	1	1	ζ^{-1}	ζ
χ_4	3	-1	0	0

(ii) Let $\rho \colon A_4 \to \mathrm{GL}_{\mathbb{C}}(V)$ be the *permutation representation* of A_4 associated to the conjugation action of A_4 on the set $X = A_4$. Using the character table in (i), express V as a direct sum $n_1V_1 \oplus n_2V_2 \oplus n_3V_3 \oplus n_4V_4$, where V_j denotes an irreducible representation with character χ_j.

(iii) For each of the representations V_i, determine its contragredient representation V_i^* as a direct sum $n_1V_1 \oplus n_2V_2 \oplus n_3V_3 \oplus n_4V_4$.

(iv) For each of the representations $V_i \otimes V_j$, determine its direct sum decomposition $n_1V_1 \oplus n_2V_2 \oplus n_3V_3 \oplus n_4V_4$.

3-6. Let $A \leqslant S_n$ be an abelian group which acts transitively on the set $\mathbf{n}$.

(i) Show that for each $k \in \mathbf{n}$ the stabilizer of k is trivial. Deduce that $|A| = n$.

(ii) Show that the permutation representation $\mathbb{C}[\mathbf{n}]$ of A decomposes as

$$\mathbb{C}[\mathbf{n}] = \rho_1 \oplus \cdots \oplus \rho_n,$$

where $\rho_1, \dots, \rho_n$ are the distinct irreducible representations of A.

CHAPTER 4

Some applications to group theory

In this chapter we will see some applications of representation theory to Group Theory.

4.1. Characters and the structure of groups

In this section we will give some results relating the character table of a finite group to its subgroup structure.

Let $\rho\colon G \to \mathrm{GL}_{\mathbb{C}}(V)$ be a representation for which $\dim_{\mathbb{C}} V = n = \chi_\rho(e)$. Define a subset of G by

$$\ker \chi_\rho = \{g \in G : \chi_\rho(g) = n\}.$$

Proposition 4.1. *We have*

$$\ker \chi_\rho = \ker \rho,$$

hence $\ker \chi_\rho$ *is a normal subgroup of* G*,* $\ker \chi_\rho \lhd G$*.*

Proof. For $g \in \ker \chi_\rho$, let $\mathbf{v} = \{v_1, \dots, v_n\}$ be a basis of V consisting of eigenvectors of ρ_g, so $\rho_g v_k = \lambda_k v_k$ for suitable $\lambda_k \in \mathbb{C}$, and indeed each λ_k is a root of unity and so has the form $\lambda_k = e^{t_k i}$ for $t_k \in \mathbb{R}$. Then

$$\chi_\rho(g) = \sum_{k=1}^{n} \lambda_k.$$

Recall that for $t \in \mathbb{R}$, $e^{ti} = \cos t + i \sin t$. Hence

$$\chi_\rho(g) = \sum_{k=1}^{n} \cos t_k + i \sum_{k=1}^{n} \sin t_k.$$

Since $\chi_\rho(e) = n$,

$$\sum_{k=1}^{n} \cos t_k = n,$$

which can only happen if each $\cos t_k = 1$, but then $\sin t_k = 0$. So we have all $\lambda_k = 1$ which implies that $\rho_g = \mathrm{Id}_V$. Thus $\ker \chi_\rho = \ker \rho$ as claimed. $\square$

Proposition 4.2. *Let* $\chi_1, \dots, \chi_r$ *be the distinct irreducible characters of* G*. Then*

$$\bigcap_{k=1}^{r} \ker \chi_k = \{e\}.$$

Proof. Set

$$K = \bigcap_{k=1}^{r} \ker \chi_k \leqslant G.$$

By Proposition 4.1, for each k, $\ker \chi_k = \ker \rho_k$, hence $K \lhd G$. Indeed, since $K \leqslant \ker \rho_k$ there is a factorisation of $\rho_k\colon G \to \mathrm{GL}_{\mathbb{C}}(V_k)$,

$$G \xrightarrow{p} G/K \xrightarrow{\rho_k'} \mathrm{GL}_{\mathbb{C}}(V_k),$$

where $p\colon G \to G/K$ is the quotient homomorphism. As p is surjective, it is easy to check that ρ'_k is an irreducible representation of G/K, with character χ'_k. Clearly the χ'_k are distinct irreducible characters of the corresponding irreducible representations and $n_k = \chi_k(e) = \chi'_k(eK)$ are their dimensions.

Since the χ_k are the distinct irreducible characters of G,

$$n_1^2 + \cdots + n_r^2 = |G|$$

by Corollary 3.20. Also

$$n_1^2 + \cdots + n_r^2 \leqslant |G/K|$$

since the χ'_k are some of the distinct irreducible characters of G/K. Combining these we have $|G| \leqslant |G/K|$ which can only happen if $|G/K| = |G|$, i.e., if $K = \{e\}$. So in fact

$$\bigcap_{k=1}^{r} \ker \chi_k = \{e\}. \qquad \square$$

Proposition 4.3. *Let $\chi_1, \ldots, \chi_r$ be the distinct irreducible characters of G and let $\mathbf{r} = \{1, \ldots, r\}$. Then a subgroup $N \leqslant G$ is normal if and only it has the form*

$$N = \bigcap_{k \in S} \ker \chi_k$$

for some subset $S \subseteq \mathbf{r}$.

Proof. Let $N \lhd G$ and suppose the quotient group G/N has s distinct irreducible representations $\sigma_k\colon G/N \to \mathrm{GL}_{\mathbb{C}}(W_k)$ $(k = 1, \ldots, s)$ with characters $\tilde{\chi}_k$. Each of these gives rise to a composite representation of G

$$\sigma'_k\colon G \xrightarrow{q} G/N \xrightarrow{\sigma_k} \mathrm{GL}_{\mathbb{C}}(W_k)$$

and again this is irreducible because the quotient homomorphism $q\colon G \to G/N$ is surjective. This gives s distinct irreducible characters of G, so each $\chi_{\sigma'_k}$ is actually one of the χ_j.

By Proposition 4.2 applied to the quotient group G/N,

$$\bigcap_{k=1}^{s} \ker \sigma_k = \bigcap_{k=1}^{s} \ker \tilde{\chi}_k = \{eN\},$$

hence since $\ker \sigma'_k = q^{-1} \ker \sigma_k$, we have

$$\bigcap_{k=1}^{s} \ker \chi_{\sigma'_k} = \bigcap_{k=1}^{s} \ker \sigma'_k = N.$$

Conversely, for any $S \subseteq \mathbf{r}$,

$$\bigcap_{k \in S} \ker \chi_k \lhd G$$

since for each k, $\ker \chi_k \lhd G$. $\square$

Corollary 4.4. *G is simple if and only if for every irreducible character $\chi_k \neq \chi_1$ and $e \neq g \in G$, $\chi_k(g) \neq \chi_k(e)$. Hence the character table can be used to decide whether G is simple.*

Corollary 4.5. *The character table can be used to decide whether G is solvable.*

Proof. G is solvable if and only if there is a sequence of subgroups

$$\{e\} = G_\ell \lhd G_{\ell-1} \lhd \cdots \lhd G_1 \lhd G_0 = G$$

for which the quotient groups G_s/G_{s+1} are abelian. This can be seen from the character table. For a solvable group we can take the subgroups to be the *lower central series* given by $G_{(0)} = G$, and in general $G_{(s+1)} = [G_{(s)}, G_{(s)}]$. It is easily verified that $G_{(s)} \lhd G$ and $G_{(s)}/G_{(s+1)}$ is abelian. By Proposition 4.3 we can now check whether such a sequence of normal subgroups exists using the character table. $\square$

We can also define the subset

$$\ker|\chi_\rho| = \{g \in G : |\chi_\rho(g)| = \chi_\rho(e)\}.$$

Proposition 4.6. $\ker|\chi_\rho|$ *is a normal subgroup of* G.

Proof. If $g \in \ker|\chi_\rho|$, then using the notation of the proof of Proposition 4.1 so that $|\chi_\rho(g)| = \chi_\rho(e) = n$, we find that

$$\begin{aligned}
n^2 = |\chi_\rho(g)|^2 &= |\sum_{k=1}^{n} \cos t_k + i \sum_{k=1}^{n} \sin t_k|^2 \\
&= \left(\sum_{k=1}^{n} \cos t_k\right)^2 + \left(\sum_{k=1}^{n} \sin t_k\right)^2 \\
&= \sum_{k=1}^{n} \cos^2 t_k + \sum_{k=1}^{n} \sin^2 t_k + 2 \sum_{1\leqslant k<\ell\leqslant n} (\cos t_k \cos t_\ell + \sin t_k \sin t_\ell) \\
&= n + 2 \sum_{1\leqslant k<\ell\leqslant n} \cos(t_k - t_\ell) \\
&\leqslant n + 2\binom{n}{2} = n + n(n-1) = n^2.
\end{aligned}$$

with equality possible if and only if $\cos(t_k - t_\ell) = 1$ whenever $1 \leqslant k < \ell \leqslant n$. Assuming that $t_j \in [0, 2\pi)$ for each j, we must have $t_\ell = t_k$, since we do indeed have equality here. Hence $\rho(g) = \lambda_g \operatorname{Id}_V$. In fact, $|\lambda_g| = 1$ since eigenvalues of ρ_g are roots of unity.

If $g_1, g_2 \in \ker|\chi_\rho|$, then

$$\rho_{g_1 g_2} = \lambda_{g_1}\lambda_{g_2} \operatorname{Id}_V$$

and so $g_1 g_2 \in \ker|\chi_\rho|$, hence $\ker|\chi_\rho|$ is a subgroup of G. Normality is also easily verified. $\square$

4.2. A result on representations of simple groups

Let G be a finite non-abelian simple group (hence of order $|G| > 1$). We already know that G has no non-trivial 1-dimensional representations.

Theorem 4.7. *An irreducible* 2*-dimensional representation of a finite non-abelian simple group* G *is trivial.*

Proof. Suppose we have a non-trivial 2-dimensional irreducible representation ρ of G. By choosing a basis we can assume that we are considering a representation $\rho\colon G \to \mathrm{GL}_{\mathbb{C}}(\mathbb{C}^2)$.

We can form the composition $\det \circ \rho \colon G \to \mathbb{C}^{\times}$ which is a homomorphism whose kernel is a non-trivial normal subgroup of G, hence it must be G. Therefore $\rho \colon G \to \mathrm{SL}_{\mathbb{C}}(\mathbb{C}^2)$, where

$$\mathrm{SL}_{\mathbb{C}}(\mathbb{C}^2) = \{A \in \mathrm{GL}_{\mathbb{C}}(\mathbb{C}^2) : \det A = 1\}.$$

Notice that since ρ is irreducible and 2-dimensional, Proposition 3.21 tells us that $|G|$ is even (this is the only time we have actually used this result!) Now by Cauchy's Lemma, Theorem A.13, there is an element $t \in G$ of order 2. Hence $\rho_t \in \mathrm{SL}_{\mathbb{C}}(\mathbb{C}^2)$ also has order 2 since ρ is injective. Since ρ_t satisfies the polynomial identity

$$\rho_t^2 - I_2 = O_2,$$

its eigenvalues must be ± 1. By Theorem 3.5 ρ_t is diagonalizable, so at least one of its eigenvalues must be -1. If the other eigenvalue were 1 then for a suitable invertible matrix P we would have

$$\rho_t = P \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} P^{-1}$$

implying $\det \rho_t = -1$ and contradicting the fact that $\det \rho_t = 1$. Hence we must have -1 as a repeated eigenvalue and so for suitable invertible matrix Q,

$$\rho_t = Q \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} Q^{-1} = Q(-I_2)Q^{-1} = -I_2$$

which is in the centre of $\mathrm{SL}_{\mathbb{C}}(\mathbb{C}^2)$. Now for $g \in G$,

$$\rho_{gtg^{-1}} = \rho_g \rho_t \rho_g^{-1} = \rho_g(-I_2)\rho_g^{-1} = -I_2 = \rho_t,$$

so since ρ is injective, $gtg^{-1} = t$. Thus $e \neq t \in \mathrm{Z}(G) = \{e\}$ since $\mathrm{Z}(G) \lhd G$. This provides a contradiction. □

4.3. A Theorem of Frobenius

Let G be a finite group and $H \leqslant G$ a subgroup which has the following property:

For all $g \in G - H$, $gHg^{-1} \cap H = \{e\}$.

Such a subgroup H is called a *Frobenius complement.*

Theorem 4.8 (**Frobenius's Theorem**). *Let $H \leqslant G$ be a Frobenius complement and let*

$$K = G - \bigcup_{g \in G} gHg^{-1} \subseteq G,$$

the subset of G consisting of all elements of G which are not conjugate to elements of H. Then $N = K \cup \{e\}$ is a normal subgroup of G which is the semidirect product $G = N \rtimes H$.

Such a subgroup N is called a *Frobenius kernel* of G.

The remainder of this section will be devoted to giving a proof of this theorem using Character Theory. We begin by showing that

$$|K| = \frac{|G|}{|H|} - 1. \tag{4.1}$$

First observe that if $e \neq g \in xHx^{-1} \cap yHy^{-1}$, then $e \neq x^{-1}gx \in H \cap x^{-1}yHy^{-1}x$; the latter can only occur if $x^{-1}y \in H$. Notice that the normalizer $\mathrm{N}_G(H)$ is no bigger than H, hence $\mathrm{N}_G(H) = H$. Thus there are exactly $|G|/|\mathrm{N}_G(H)| = |G|/|H|$ distinct conjugates of H, with only one element e in common to two or more of them. So the number elements of G which are conjugate to elements of H is

$$\frac{|G|}{|H|}(|H|-1)+1.$$

Hence,

$$|K| = |G| - \frac{|G|}{|H|}(|H|-1) - 1 = \frac{|G|}{|H|} - 1.$$

Now let $\alpha \in \mathcal{C}(H)$ be a class function on the group H. We can define a function $\tilde{\alpha}\colon G \to \mathbb{C}$ by

$$\tilde{\alpha}(g) = \begin{cases} \alpha(xgx^{-1}) & \text{if } xgx^{-1} \in H, \\ \alpha(e) & \text{if } g \in K. \end{cases}$$

This is well defined and also a class function on G. We also have

$$\tilde{\alpha} = \alpha \uparrow_H^G - \alpha(e)(\chi_\xi \uparrow_H^G - \chi_1^G), \tag{4.2}$$

where we use the notation of Qu. 4 in the Problems. In fact, $\chi_\xi \uparrow_H^G - \chi_1^G$ is the character of a representation of G.

Given two class functions α, β on H,

$$\begin{aligned}
(\tilde{\alpha}|\tilde{\beta})_G &= \frac{1}{|G|}\left(\sum_{g\in G} \tilde{\alpha}(g)\overline{\tilde{\beta}(g)}\right) \\
&= \frac{1}{|G|}\left((|K|+1)\alpha(e)\overline{\beta(e)} + \sum_{g\in G-N} \tilde{\alpha}(g)\overline{\tilde{\beta}(g)}\right) \\
&= \frac{1}{|G|}\left(\frac{|G|}{|H|}\alpha(e)\overline{\beta(e)} + \frac{|G|}{|H|}\sum_{e\neq h\in H} \tilde{\alpha}(h)\overline{\tilde{\beta}(h)}\right) \\
&\qquad\qquad \text{[by Equation (4.1)]} \\
&= \frac{1}{|H|}\left(\sum_{h\in H} \tilde{\alpha}(h)\overline{\tilde{\beta}(h)}\right) \\
&= (\tilde{\alpha}|\tilde{\beta})_H.
\end{aligned}$$

For χ an irreducible character of H,

$$(\tilde{\chi}|\tilde{\chi})_G = (\chi|\chi)_H = 1$$

by Proposition 3.17. Also, Equation (4.2) implies that

$$\tilde{\chi} = \sum_j m_j \chi_j^G,$$

where $m_j \in \mathbb{Z}$ and the χ_j^G are the distinct irreducible characters of G. Using Frobenius Reciprocity 3.33, these coefficients m_j are given by

$$m_j = (\tilde{\chi}|\chi_j^G)_G = (\chi|\chi_j^G \downarrow_H^G)_H \geqslant 0$$

since $\chi, \chi_j^G \downarrow_H^G$ are characters of H. As $\tilde{\chi}(e) = \chi(e) > 0$, $\tilde{\chi}$ is itself the character of some representation ρ of G, i.e., $\tilde{\chi} = \chi_\rho$. Notice that

$$N = \{g \in G : \chi_\rho(g) = \chi_\rho(e)\} = \ker \rho.$$

Hence, by Proposition 4.1, N is a normal subgroup of G.

Now $H \cap N = \{e\}$ by construction. Moreover,

$$|NH| \geqslant |H|\,|N| = |G|,$$

hence $NH = NH = G$. So $G = N \rtimes H$. This completes the proof of Theorem 4.8.

An equivalent formulation of this result is the following which can be found in [**1**, Chapter 6].

THEOREM 4.9 (**Frobenius's Theorem: group action version**). *Let the finite group G act transitively on the set X, and suppose that each element $g \neq e$ fixes at most one element of X, i.e., $|X^g| \leqslant 1$. Then*

$$N = \{g \in G : |X^g| = 0\} \cup \{e\}$$

is a normal subgroup of G.

PROOF. Let $x \in X$ be fixed by some element of G not equal to the identity element e, and let $H = \mathrm{Stab}_G(x)$. Then for $k \in G - H$, $k \cdot x \neq x$ has

$$\mathrm{Stab}_G(k \cdot x) = k\,\mathrm{Stab}_G(x)k^{-1} = kHk^{-1}.$$

If $e \neq g \in H \cap kHk^{-1}$, then g stabilizes x and $k \cdot x$, but this contradicts the assumption on the number of fixed points of elements in G. Hence H is a Frobenius complement. Now the result follows from Theorem 4.8. $\square$

EXAMPLE 4.10. The subgroup $H = \{e, (1\,2)\} \leqslant S_3$ satisfies the conditions of Theorem 4.8. Then

$$\bigcup_{g \in S_3} gHg^{-1} = \{e, (1\,2), (1\,3), (2\,3)\}$$

and $N = \{e, (1\,2\,3), (1\,3\,2)\}$ is a Frobenius kernel.

Exercises on Chapter 4

4-1. Let $\rho\colon G \to \mathrm{GL}_{\mathbb{C}}(V)$ be a representation.

(i) Show that the sets

$$\ker \chi_\rho = \{g \in G : \chi_\rho(g) = \chi_\rho(e)\} \subseteq G,$$
$$\ker |\chi_\rho| = \{g \in G : |\chi_\rho(g)| = \chi_\rho(e)\} \subseteq G,$$

are normal subgroups of G for which $\ker \chi_\rho \leqslant \ker |\chi_\rho|$ and $\ker \chi_\rho = \ker \rho$.
[Hint: *Recall that for $t \in \mathbb{R}$, $e^{ti} = \cos t + i \sin t$.*]

(ii) Show that the commutator subgroup $[\ker |\chi_\rho|, \ker |\chi_\rho|]$ of $\ker |\chi_\rho|$ is a subgroup of $\ker \chi_\rho$.

4-2. Let G be a finite group and $X = G/H$ the finite G-set on which G acts transitively with action written $g \cdot kH = gkH$ for $g, k \in G$. Let ξ be the associated permutation representation on $\mathbb{C}[X]$.

(i) Using the definition of induced representations, show that ξ is G-isomorphic to $\xi_1^H \uparrow_H^G$, where ξ_1^H is the trivial 1-dimensional representation of H.

(ii) Let $W_X \subseteq \mathbb{C}[X]$ be the G-subspace of Qu. 2.7(i) and θ the representation on W_X. Show that $\chi_\theta = \chi_\xi - \chi_1^G$, where χ_1^G is the character of the trivial 1-dimensional representation of G.

(iii) Use Frobenius Reciprocity to prove that $(\chi_\theta|\chi_1^G)_G = 0$.

4-3. Continuing with the setup in Qu. 4.3 with the additional assumption that $|X| \geqslant 2$, let $Y = X \times X$ be given the associated diagonal action $g \cdot (x_1, x_2) = (g \cdot x_1, g \cdot x_2)$ and let σ be the associated permutation representation on $\mathbb{C}[Y]$. The action on X is said to be *doubly transitive* or 2-*transitive* if, whenever $(x_1, x_2), (x_1', x_2') \in Y$ with $x_1 \neq x_2$ and $x_1' \neq x_2'$, there is a $g \in G$ for which $g \cdot (x_1, x_2) = (x_1', x_2')$.

(i) Show that $\chi_\sigma = {\chi_\xi}^2$, i.e., show that for every $g \in G$, $\chi_\sigma(g) = \chi_\xi(g)^2$.

(ii) Show that the action on X is 2-transitive if and only if the action on Y has exactly two orbits.

(iii) Show that the action on X is 2-transitive if and only if $(\chi_\sigma|\chi_1^G)_G = 2$.

(iv) Show that the action on X is 2-transitive if and only if θ is irreducible.

4-4. The following is the character table of a certain group G of order 60, where the numbers in brackets [ ] are the numbers in the conjugacy classes of G, χ_k is the character of an irreducible representation ρ_k and $\alpha = (1+\sqrt{5})/2$, $\beta = (1-\sqrt{5})/2$.

	$g_1 = e_G$ [1]	g_2 [20]	g_3 [15]	g_4 [12]	g_5 [12]
χ_1	1	1	1	1	1
χ_2	5	-1	1	0	0
χ_3	4	1	0	-1	-1
χ_4	3	0	-1	α	β
χ_5	a	b	c	d	e

(i) Determine the dimension of the representation ρ_5.

(ii) Use row orthogonality to determine χ_5.

(iii) Show that G is a simple group.

(iv) Decompose each of the contragredient representations ρ_j^* as a direct sum of the irreducible representations ρ_k.

(v) Decompose each of the tensor product representations $\rho_s \otimes \rho_t$ as a direct sum of the irreducible representations ρ_k.

(vi) Identify this group G up to isomorphism.

APPENDIX A

Background information on groups

A.1. The Isomorphism and Correspondence Theorems

The three Isomorphism Theorems and the Correspondence Theorem are fundamental results of Group Theory. We will write $H \leqslant G$ and $N \lhd G$ to indicate that H is a subgroup and N is a normal subgroup of G.

Recall that given a normal subgroup $N \lhd G$ the *quotient* or *factor* group G/N has for its elements the distinct cosets

$$gN = \{gn \in G : n \in N\} \quad (g \in G).$$

Then the *natural homomorphism*

$$\pi \colon G \to G/N; \quad \pi(g) = gN$$

is surjective with kernel $\ker \pi = N$.

Theorem A.1 (First Isomorphism Theorem). *Let $\varphi \colon G \to H$ be a homomorphism with $N = \ker \varphi$. Then there is a unique homomorphism $\overline{\varphi} \colon G/N \to H$ such that $\overline{\varphi} \circ \pi = \varphi$. Equivalently, there is a unique factorisation*

$$\varphi \colon G \xrightarrow{\pi} G/N \xrightarrow{\overline{\varphi}} H.$$

In diagram form this becomes

$$\begin{tikzcd}
G \arrow[rr, "q"] \arrow[dr, "\varphi"'] & & G/N \arrow[dl, dotted, "\exists!\,\overline{\varphi}"] \\
& H &
\end{tikzcd}$$

where all the arrows represent group homomorphisms.

Theorem A.2 (Second Isomorphism Theorem). *Let $H \leqslant G$ and $N \lhd G$. Then there is an isomorphism*

$$HN/N \cong H/(H \cap N); \quad hn \longleftrightarrow h(H \cap N).$$

Theorem A.3 (Third Isomorphism Theorem). *Let $K \lhd G$ and $N \lhd G$ with $N \lhd K$. Then $K/N \leqslant G/N$ is a normal subgroup, and there is an isomorphism*

$$G/K \cong (G/N)/(K/N); \quad gK \longleftrightarrow (gN)(K/N).$$

Theorem A.4 (Correspondence Theorem). *There is a one-one correspondence between subgroups of G containing N and subgroups of G/N, given by*

$$\begin{aligned} H &\longleftrightarrow \pi(H) = H/N, \\ \pi^{-1}Q &\longleftrightarrow Q, \end{aligned}$$

where

$$\pi^{-1}Q = \{g \in G : \pi(g) = gN \in Q\}.$$

Moreover, under this correspondence, $H \lhd G$ if and only if $\pi(H) \lhd G/N$.

A.2. Some definitions and notation

Let G be a group.

Definition A.5. The *centre* of G is the subset

$$\mathrm{Z}(G) = \{c \in G : gc = cg \; \forall g \in G\}.$$

This is a normal subgroup of G, i.e., $\mathrm{Z}(G) \lhd G$.

Definition A.6. Let $g \in G$, then the *centralizer* of g is

$$\mathrm{C}_G(g) = \{c \in G : cg = gc\}.$$

This is a subgroup of G, i.e., $\mathrm{C}_G(g) \leqslant G$.

Definition A.7. Let $H \leqslant G$. The *normalizer* of H in G is

$$\mathrm{N}_G(H) = \{c \in G : cHc^{-1} = H\}.$$

This is a subgroup of G containing H; moreover, H is a normal subgroup of $\mathrm{N}_G(H)$, i.e., $H \lhd \mathrm{N}_G(H)$.

Definition A.8. G is *simple* if its only normal subgroups are G and $\{e\}$. Equivalently, it has no non-trivial proper subgroups.

Definition A.9. The *order* of G, $|G|$, is the number of elements in G when G is finite, and ∞ otherwise. If $g \in G$, the *order* of g, $|g|$, is the smallest natural number $n \in \mathbb{N}$ such $g^n = e$ provided such a number exists, otherwise it is ∞. Equivalently, $|g| = |\langle g \rangle|$, the order of the cyclic group generated by g. If G is finite, then every element has finite order.

Theorem A.10 (Lagrange's Theorem). *If G is a finite group, and $H \leqslant G$, then $|H|$ divides $|G|$. In particular, for any $g \in G$, $|g|$ divides $|G|$.*

Definition A.11. Two elements $x, y \in G$ are *conjugate* in G if there exists $g \in G$ such that

$$y = gxg^{-1}.$$

The *conjugacy class* of x is the set of all elements of G conjugate to x,

$$x^G = \{y \in G : y = gxg^{-1} \text{ for some } g \in G\}.$$

Conjugacy is an equivalence relation on G and the distinct conjugacy classes are the distinct equivalence classes.

A.3. Group actions

Let G be a group (with identity element $e = e_G$) and X be a set. Recall that an *action of G on X* is a rule assigning to each $g \in G$ a bijection $\varphi_g \colon X \to X$ and satisfying the identities

$$\varphi_{gh} = \varphi_g \circ \varphi_h,$$
$$\varphi_{e_G} = \mathrm{Id}_X \,.$$

We will frequently make use of the notation

$$g \cdot x = \varphi_g(x)$$

(or even just write gx) when the action is clear, but sometimes we may need to refer explicitly to the action. It is often useful to view an action as corresponding to a function

$$\Phi \colon G \times X \to X;\ \varphi(g, x) = \varphi_g(x).$$

It is also frequently important to regard an action of G as corresponding to a group homomorphism

$$\varphi \colon G \to \mathrm{Perm}(X); \quad g \mapsto \varphi_g,$$

where $\mathrm{Perm}(X)$ denotes the group of all *permutations* (i.e., bijections $X \to X$) of the set X. If $\mathbf{n} = \{1, 2, \ldots, n\}$, then $S_n = \mathrm{Perm}(\mathbf{n})$ is the *symmetric group on n objects*; S_n has order $n!$, i.e., $|S_n| = n!$.

Given such an action of G on X, we make the following definitions:

$$\mathrm{Stab}_\varphi(x) = \{g \in G : \varphi_g(x) = x\},$$
$$\mathrm{Orb}_\varphi(x) = \{y \in X : \text{ for some } g \in G,\ y = \varphi_g(x)\},$$
$$X^G = \{x \in X : gx = x\ \forall g \in G\}.$$

Then $\mathrm{Stab}_\varphi(x)$ is called the *stabilizer* of x and is often denoted $\mathrm{Stab}_G(x)$ when the action is clear, while $\mathrm{Orb}_\varphi(x)$ is called the *orbit* of x and is often denoted $\mathrm{Orb}_G(x)$. X^G is called the *fixed point set* of the action.

THEOREM A.12. *Let φ be an action of G on X, and $x \in X$.*

(a) $\mathrm{Stab}_\varphi(x)$ *is a subgroup of G. Hence if G is finite, then so is* $\mathrm{Stab}_\varphi(x)$ *and by* Lagrange's Theorem, $|\mathrm{Stab}_\varphi(x)| \mid |G|$.

(b) *There is a bijection*

$$G/\mathrm{Stab}_\varphi(x) \longleftrightarrow \mathrm{Orb}_\varphi(x); \quad g\,\mathrm{Stab}_\varphi(x) \longleftrightarrow g \cdot x = \varphi_g(x).$$

*Furthermore, this bijection is G-*equivariant *in the sense that*

$$hg\,\mathrm{Stab}_\varphi(x) \leftrightarrow h \cdot (g \cdot x).$$

In particular, if G is finite, then so is $\mathrm{Orb}_\varphi(x)$ *and we have*

$$|\mathrm{Orb}_\varphi(x)| = |G| / |\mathrm{Stab}_\varphi(x)|.$$

(c) *The distinct orbits* partition *X into a disjoint union of subsets,*

$$X = \coprod_{\substack{\text{distinct} \\ \text{orbits}}} \mathrm{Orb}_\varphi(x).$$

Equivalently, there is an equivalence relation $\underset{G}{\sim}$ *on* X *for which the distinct orbits are the equivalence classes and given by*

$$x \underset{G}{\sim} y \iff \text{for some } g \in G,\ y = g \cdot x.$$

Hence, when X *is finite, then*

$$|X| = \sum_{\substack{\text{distinct}\\ \text{orbits}}} |\operatorname{Orb}_\varphi(x)|$$

This theorem is the basis of many arguments in Combinatorics and Number Theory as well as Group Theory. Here is an important group theoretic example, often called *Cauchy's Lemma.*

THEOREM A.13 (Cauchy's Lemma). *Let* G *be a finite group and let* p *be a prime for which* $p \mid |G|$. *Then there is an element* $g \in G$ *of order* p.

PROOF. Let

$$X = G^p = \{(g_1, g_2, \dots, g_p) : g_j \in G,\ g_1 g_2 \cdots g_p = e_G\}.$$

Let H be the group of all cyclic permutations of the set $\{1, 2, \dots, p\}$; this is a cyclic group of order p. Consider the following action of H on X:

$$\gamma \cdot (g_1, g_2, \dots, g_p) = (g_{\gamma^{-1}(1)}, g_{\gamma^{-1}(2)}, \dots, g_{\gamma^{-1}(p)}).$$

It is easily seen that this *is* an action. By Theorem A.12, the size of each orbit must divide $|H| = p$, hence it must be 1 or p since p is prime. On the other hand,

$$|X| = |G|^p \equiv 0 \pmod{p},$$

since $p \mid |G|$. Again by Theorem A.12, we have

$$|X| = \sum_{\substack{\text{distinct}\\ \text{orbits}}} |\operatorname{Orb}_H(x)|,$$

and hence

$$\sum_{\substack{\text{distinct}\\ \text{orbits}}} |\operatorname{Orb}_H(x)| \equiv 0 \pmod{p}.$$

But there is at least one orbit of size 1, namely that containing $\mathbf{e} = (e_G, \dots, e_G)$, hence,

$$\sum_{\substack{\text{distinct}\\ \text{orbits not}\\ \text{containing } \mathbf{e}}} |\operatorname{Orb}_H(x)| \equiv -1 \pmod{p}.$$

If all the left hand summands are p, then we obtain a contradiction, so at least one other orbit contains exactly one element. But such an orbit must have the form

$$\operatorname{Orb}_H((g, g, \dots, g)), \quad g^p = e_G.$$

Hence g is the desired element of order p. □

Later, we will meet the following type of action. Let $\Bbbk$ be a field and V a vector space over $\Bbbk$. Let $\mathrm{GL}_{\Bbbk}(V)$ denote the group of all invertible $\Bbbk$-linear transformations $V \to V$. Then for any group G, a group homomorphism $\rho\colon G \to \mathrm{GL}_{\Bbbk}(V)$ defines a $\Bbbk$-*linear action* of G on V by

$$g \cdot v = \rho(g)(v).$$

This is also called a $\Bbbk$-*representation* of G in (or on) V. One extreme example is provided by the case where $G = \mathrm{GL}_{\Bbbk}(V)$ with $\rho = \mathrm{Id}_{\mathrm{GL}_{\Bbbk}(V)}$. We will be mainly interested in the situation where G is finite and $\Bbbk = \mathbb{R}$ or $\Bbbk = \mathbb{C}$; however, other cases are important in Mathematics.

If we have actions of G on sets X and Y, a function $\varphi\colon X \to Y$ is called G-*equivariant* or a G-*map* if

$$\varphi(gx) = g\varphi(x) \quad (g \in G,\, x \in X).$$

An invertible G-map is called a G-*equivalence* (it is easily seen that the inverse map is itself a a G-map). We say that two G-sets are G-equivalent if there is a G-equivalence between them. Another way to understand these ideas is as follows. If $\mathrm{Map}(X, Y)$ denotes the set of all functions $X \to Y$, then we can define an action of G by

$$(g \cdot \varphi)(x) = g(\varphi(g^{-1}x)).$$

Then the fixed point set of this action is

$$\mathrm{Map}(X, Y)^G = \{\varphi : g\varphi(g^{-1}x) = \varphi(x)\ \forall x, g\} = \{\varphi : \varphi(gx) = g\varphi(x)\ \forall x, g\}.$$

So $\mathrm{Map}^G(X, Y) = \mathrm{Map}(X, Y)^G$ is just the set of all G-equivariant maps.

A.4. The Sylow theorems

The Sylow Theorems provide the beginnings of a systematic study of the structure of finite groups. For a finite group G, they connect the factorisation of $|G|$ into prime powers,

$$|G| = p_1^{r_1} p_2^{r_2} \cdots p_d^{r_d},$$

where $2 \leqslant p_1 < p_2 < \cdots < p_d$ with p_k prime, and $r_k > 0$, to the existence of subgroups of prime power order, often called *p-subgroups*. They also provide a sort of converse to Lagrange's Theorem.

Here are the three Sylow Theorems. Recall that a proper subgroup $H < G$ is *maximal* if it is contained in no larger proper subgroup; also a subgroup $P \leqslant G$ is a *p-Sylow subgroup* if $|P| = p^k$ where $p^{k+1} \nmid |G|$.

Theorem A.14 (**Sylow's First Theorem**). *A p-subgroup $P \leqslant G$ is maximal if and only if it is a p-Sylow subgroup. Hence every p-subgroup is contained in a p-Sylow subgroup.*

Theorem A.15 (**Sylow's Second Theorem**). *Any two p-Sylow subgroups $P, P' \leqslant G$ are conjugate in G.*

Theorem A.16 (**Sylow's Third Theorem**). *Let $P \leqslant G$ be a p-Sylow subgroup with $|P| = p^k$, so $|G| = p^k m$ where $p \nmid m$. Also let n_p be the number of distinct p-Sylow subgroups of G. Then*

(i) $$n_p \equiv 1 \pmod{p};$$

(ii) $$m \equiv 0 \pmod{n_p}.$$

Finally, we end with an important result on chains of subgroups in a finite p-group.

Theorem A.17. *Let P be a finite p-group. Then there is a sequence of subgroups*

$$\{e\} = P_0 \leqslant P_1 \leqslant \cdots \leqslant P_n = P,$$

with $|P_k| = p^k$ and $P_{k-1} \lhd P_k$ for $1 \leqslant k \leqslant n$.

We also have the following which can be proved directly by the method in the proof of Theorem A.13. Recall that for any group G, its *centre* is the normal subgroup

$$\mathrm{Z}(G) = \{c \in G : \forall g \in G,\ cg = gc\} \lhd G.$$

THEOREM A.18. *Let P be a non-trivial finite p-group. Then the centre of P is non-trivial, i.e., $\mathrm{Z}(P) \neq \{e\}$.*

Sylow theory seemingly reduces the study of structure of a finite group to the interaction between the different Sylow subgroups as well as their internal structure. In reality, this is just the beginning of a difficult subject, but the idea seems simple enough!

A.5. Solvable groups

DEFINITION A.19. A group G which has a sequence of subgroups

$$\{e\} = H_0 \leqslant H_1 \leqslant \cdots \leqslant H_n = G,$$

with $H_{k-1} \lhd H_k$ and H_k/H_{k-1} cyclic of prime order, is called *solvable (soluble* or *soluable).*

Solvable groups are generalizations of p-groups in that every finite p-group is solvable. A finite solvable group G can be thought of as built up from the abelian subquotients H_k/H_{k-1}. Since finite abelian groups are easily understood, the complexity is then in the way these subquotients are 'glued' together.

More generally, for a group G, a series of subgroups

$$G = G_0 > G_1 > \cdots > G_r = \{e\}$$

is called a *composition series* for G if $G_{j+1} \lhd G_j$ for each j, and each successive quotient group G_j/G_{j+1} is simple. The quotient groups G_j/G_{j+1} (and groups isomorphic to them) are called the *composition factors* of the series, which is said to have *length* r. Every finite group has a composition series, with solvable groups being the ones with abelian subquotients. Thus, to study a general finite group requires that we analyse both finite simple groups and also the ways that they can be glued together to appear as subquotients for composition series.

A.6. Product and semi-direct product groups

Given two groups H, K, their *product* $G = H \times K$ is the set of ordered pairs

$$H \times K = \{(h, k) : h \in H,\ k \in K\}$$

with multiplication $(h_1, k_1) \cdot (h_2, k_2) = (h_1h_2, k_1k_2)$, identity $e_G = (e_H, e_K)$ and inverses given by $(h, k)^{-1} = (h^{-1}, k^{-1})$.

A group G is the *semi-direct product* $G = N \rtimes H$ of the subgroups N, H if $N \lhd G$, $H \leqslant G$, $H \cap N = \{e\}$ and $HN = NH = G$. Thus, each element $g \in G$ has a unique expression $g = hn$ where $n \in N, h \in H$. The multiplication is given in terms of such factorisations by

$$(h_1n_1)(h_2n_2) = (h_1h_2)(h_2^{-1}n_1h_2n_2),$$

where $h_2^{-1}n_1h_2 \in N$ by the normality of N.

An example of a semi-direct product is provided by the symmetric group on 3 letters, S_3. Here we can take

$$N = \{e, (1\,2\,3), (1\,3\,2)\}, \quad H = \{e, (1\,2)\}.$$

H can also be one of the subgroups $\{e, (1\,3)\}, \{e, (2\,3)\}$.

A.7. Some useful groups

In this section we define various groups that will prove useful as test examples in the theory we will develop. Some of these will be familiar although the notation may vary from that in previous encounters with these groups.

A.7.1. The quaternion group. The *quaternion group of order* 8, Q_8, has as elements the following 2×2 complex matrices:

$$\pm\mathbf{1},\ \pm\mathbf{i},\ \pm\mathbf{j},\ \pm\mathbf{k},$$

where

$$\mathbf{1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I_2, \quad \mathbf{i} = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \quad \mathbf{j} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \quad \mathbf{k} = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}.$$

A.7.2. Dihedral groups.

Definition A.20. The *dihedral group of order* $2n$, D_{2n}, is generated by two elements α, β of orders $|\alpha| = n$ and $|\beta| = 2$ which satisfy the relation

$$\beta\alpha\beta = \alpha^{-1}.$$

The distinct elements of D_{2n} are

$$\alpha^r,\ \alpha^r\beta \quad (r = 0, \ldots, n-1).$$

Notice that we also have $\alpha^r\beta = \beta\alpha^{-r}$. A useful geometric interpretation of D_{2n} is provided by the following.

Proposition A.21. *The group D_{2n} is isomorphic to the symmetry group of a regular n-gon in the plane, with α corresponding to a rotation through $2\pi/n$ about the centre and β corresponding to the reflection in a line through a vertex and the centre.*

A.7.3. Symmetric and alternating groups. The symmetric group on n objects S_n is best handled using *cycle notation.* Thus, if $\sigma \in S_n$, then we express σ in terms of its *disjoint cycles.* Here the cycle $(i_1\ i_2\ \ldots\ i_k)$ is the element which acts on the set $\mathbf{n} = \{1, 2, \ldots, n\}$ by sending i_r to i_{r+1} (if $r < k$) and i_k to i_1, while fixing the remaining elements of $\mathbf{n}$; the *length* of this cycle is k and we say that it is a *k-cycle.* Every permutation σ has a unique expression (apart from order) as a composition of its *disjoint cycles*, i.e., cycles with no common entries. We usually supress the cycles of length 1, thus $(1\,2\,3)(4\,6)(5) = (1\,2\,3)(4\,6)$.

It is also possible to express a permutation σ as a composition of 2-cycles; such a decomposition is not unique, but the number of the 2-cycles taken modulo 2 (or equivalently, whether this number is even or odd, i.e., its parity) *is* unique. The *sign* of σ is

$$\operatorname{sign}\sigma = (-1)^{\text{number of 2-cycles}} = \pm 1.$$

Theorem A.22. *The function* $\operatorname{sign}\colon S_n \to \{1, -1\}$ *is a surjective group homomorphism.*

The kernel of sign is called the *alternating group* A_n and its elements are called *even* permutations, while elements of S_n not in A_n are called *odd* permutations. Notice that $|A_n| = |S_n|/2 = n!/2$. S_n is the disjoint union of the two cosets $eA_n = A_n$ and τA_n where $\tau \in S_n$ is any odd permutation.

Here are the elements of A_3 and S_3 expressed in cycle notation.

A_3: $e = (1)(2)(3),\ (1\,2\,3) = (1\,3)(1\,2),\ (1\,3\,2) = (1\,2)(1\,3).$

S_3: $e,\ (1\,2\,3),\ (1\,3\,2),\ (1\,2)e = (1\,2),\ (1\,2)(1\,2\,3) = (1)(2\,3),\ (1\,2)(1\,3\,2) = (2)(1\,3).$

A.8. Some useful Number Theory

In the section we record some number theoretic results that are useful in studying finite groups. These should be familiar and no proofs are given. Details can be found in [**2**] or any other basic book on abstract algebra.

Definition A.23. Given two integers a, b, their *highest common factor* or *greatest common divisor* is the highest positive common factor, and is written (a, b). It has the property that any integer common divisor of a and b divides (a, b).

Definition A.24. Two integers a, b are *coprime* if $(a, b) = 1$.

Theorem A.25. *Let $a, b \in Z$. Then there are integers r, s such that $ra + sb = (a, b)$. In particular, if a and b are coprime, then there are integers r, s such that $ra + sb = 1$.*

More generally, if $a_1, \ldots, a_n$ are pairwise coprime, then there are integers $r_1, \ldots, r_n$ such that

$$r_1a_1 + \cdots + r_na_n = 1.$$

These results are consequences of the *Euclidean* or *Division Algorithm* for $\mathbb{Z}$.

EA: *Let $a, b \in \mathbb{Z}$. Then there are unique $q, r \in \mathbb{Z}$ for which $0 \leqslant r < |b|$ and $a = qb + r$.*

It can be shown that in this situation, $(a, b) = (b, r)$. This allows a determination of the highest common factor of a and b by repeatedly using EA until the remainder r becomes 0, when the previous remainder will be (a, b).

Bibliography

[1] J. L. Alperin & R. B. Bell, Groups and Representations, Springer-Verlag (1995).

[2] J. B. Fraleigh, A First Course in Abstract Algebra, 5th Edition, Addison-Wesley (1994).

[3] G. James & M. Liebeck, Representations and Characters of Groups, Cambridge University Press (1993).

[4] J-P. Serre, Linear Representations of Finite Groups, Springer-Verlag (1977).

[5] S. Sternberg, Group theory and physics, Cambridge University Press (1994).