Finite Group Representations

for the

Pure Mathematician

by

Peter Webb

Preface

This book started as notes for courses given at the graduate level at the University of Minnesota. It is intended to be used at the level of a second-year graduate course in an American university. At this level the book should provide material for a year-long course in representation theory.

It is supposed that the reader has already studied the material in a first-year graduate course on algebra and is familiar with the basic properties, for example, of Sylow subgroups and solvable groups, as well as the examples which are introduced in a first group theory course, such as the dihedral, symmetric, alternating and quaternion groups. The reader should also be familiar with other aspects of algebra which appear in or before a first-year graduate course, such as Galois Theory, tensor products, Noetherian properties of commutative rings, the structure of modules over a principal ideal domain, and the first properties of ideals.

The Pure Mathematician for whom this course is intended may well have a primary interest in an area of pure mathematics other than the representation theory of finite groups. Group representations arise naturally in many areas, such as number theory, combinatorics and topology, to name just three, and the aim of this course is to give students in a wide range of areas the technique to understand the representations which they encounter. This point of view has determined to a large extent the nature of this book: it should be sufficiently short, so that students who are not specialists in group representations can get to the end of it. Since the representations which arise in many areas are defined over rings other than fields of characteristic zero, such as rings of algebraic integers or finite fields, the theory is developed over arbitrary ground rings where possible. The student finishing this course should feel no lack of confidence in working in characteristic p.

A selection of topics has been made at every stage, and where a result appears to have predominantly technical interest, perhaps confined to those who specialize in group representations, then in some cases it has been omitted.

The exercises at the ends of sections are an important part of this book. They provide a place to indicate how the subject may be developed beyond what is described in the text. They provide a stock of examples which provide a firmer basis for the expertize of the reader. And they provide homework exercises so that the reader can learn by actively doing, as well as by the more passive activity of reading.

Provisional Table of Contents

Part 1: Representations

Part 2: Group cohomology

1. Representations, Maschke's Theorem and Semisimplicity

We start by establishing some notation. We let G denote a finite group, and we will work over a commutative ring R with a 1. For example, R could be any of the fields $\mathbb{Q}$, $\mathbb{C}$, $\mathbb{R}$, $\mathbb{F}_p$, $\overline{\mathbb{F}}_p$ etc, where the latter symbol denotes the algebraic closure of $\mathbb{F}_p$, or we could take $R = \mathbb{Z}$ or some other ring. If V is an R-module we denote by $GL(V)$ the group of all invertible R-module homomorphisms $V \to V$. In case $V \cong R^n$ is a free module of rank n this group is isomorphic to the group of all non-singular $n \times n$-matrices over R, and we denote it $GL(n, R)$ or $GL_n(R)$, or in case $R = \mathbb{F}_q$ is the finite field with q elements by $GL(n, q)$ or $GL_n(q)$.

A *(linear) representation* of G (over R) is a homomorphism

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

In a situation where V is free as an R-module, on taking a basis for V we obtain for each element $g \in G$ a matrix $\rho(G)$, and these matrices multiply together in the manner of the group. In this situation the rank of the free R-module V is called the *degree* of the representation. Sometimes by abuse of terminology the module V is called the representation, but it should more properly be called the *representation module* or *representation space* (if R is a field).

(1.1) *Examples.* 1. For any group G and commutative ring R we can take $V = R$ and $\rho(G) = 1$ for all $g \in G$. This representation is called the *trivial representation*, and it is often denoted simply by its representation module R.

2. Let $G = S_n$, the symmetric group on n symbols, $V = R$ and

$$\rho(g) = \text{ multiplication by } \epsilon(g),$$

where $\epsilon(g)$ is the sign of g. This representation is called the *sign representation* of the symmetric group.

3. Let $R = \mathbb{R}$, $V = \mathbb{R}^2$ and $G = S_3$. This group may be realized as the group of automorphisms of V generated by reflections in the three lines

In terms of matrices this gives a representation

$$\begin{aligned}
() &\mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\
(1,2) &\mapsto \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix} \\
(1,3) &\mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\
(2,3) &\mapsto \begin{pmatrix} -1 & 0 \\ -1 & 1 \end{pmatrix} \\
(1,2,3) &\mapsto \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \\
(1,3,2) &\mapsto \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}
\end{aligned}$$

where we have taken basis vectors in the direction of two of the lines of reflection, making an angle of $\frac{2\pi}{3}$ to each other. In fact these matrices define a representation of degree 2 over any ring R, because although the representation was initially constructed over $\mathbb{R}$, in fact the matrices have integer entries which may be interpreted in every ring, and these matrices always multiply together to give a copy of S_3.

4. Let $R = \mathbb{F}_p$, $V = R^2$ and let $G = C_p = \langle g \rangle$ be cyclic of order p generated by an element g. One checks that the assignment

$$\rho(g^r) = \begin{pmatrix} 1 & 0 \\ r & 1 \end{pmatrix}$$

is a representation. In this case the fact that we have a representation is very much dependent on the choice of R as the field $\mathbb{F}_p$: in characteristic 0 it would not work!

We can think of representations in various ways, and one of them is that a representation is the specification of an action of a group on an R-module. Given a representation $\rho : G \to GL(V)$, an element $v \in V$ and a group element $g \in G$ we get another module element $\rho(g)(v)$. Sometimes we write just $g \cdot v$ or gv for this element. This rule for multiplication satisfies

$$\begin{aligned}
g \cdot (\lambda v + \mu w) &= \lambda g \cdot v + \mu g \cdot w \\
(gh) \cdot v &= g \cdot (h \cdot v) \\
1 \cdot v &= v
\end{aligned}$$

for all $g \in G$, $v, w \in V$ and $\lambda, \mu \in R$. A rule for multiplication $G \times V \to V$ satisfying these conditions is called a *linear action* of G on V. To specify a linear action of G on V is the same thing as specifying a representation of G on V, since given a representation we obtain a linear action as indicated above, and evidently given a linear action we may recover the representation.

Another way to define a representation of a group is in terms of the group algebra. We define the *group algebra* RG (or $R[G]$) of G over R to be the free R-module with the elements of G as an R-basis, and with multiplication given on the basis elements by group multiplication. The elements of RG are the (formal) R-linear combinations of group elements, and the multiplication of the basis elements is extended to arbitrary elements using bilinearity of the operation. A typical element of RG may be written $\sum_{g\in G} a_g g$ where $a_g \in R$, and symbolically

$$(\sum_{g\in G} a_g g)(\sum_{h\in G} b_h h) = \sum_{k\in G}(\sum_{gh=k} a_g b_h)k.$$

More concretely, we may exemplify the definition by listing some elements of $\mathbb{Q}S_3$. The elements of S_3 such as $(1,2) = 1\cdot(1,2)$ are also elements of $\mathbb{Q}S_3$ (they appear as basis elements), and $()$ serves as the identity element of $\mathbb{Q}S_3$ (as well as of S_3). In general, elements of $\mathbb{Q}S_3$ may look like $(1,2)-(2,3)$ or $\frac{1}{5}(1,2,3)+6(1,2)-\frac{1}{7}(2,3)$. Here is a computation:

$$((1,2,3)+(1,2))((1,2)-(2,3)) = (1,3)+()-(1,2)-(1,2,3).$$

Having defined the group algebra, we may now define a representation of G over R to be a unital RG-module. The fact that this definition coincides with the previous ones is the content of the next proposition.

(1.2) PROPOSITION. *A representation of G over R has the structure of a unital RG-module; conversely, every unital RG-module provides a representation of G over R.*

Proof. Given a representation $\rho : G \to GL(V)$ we define a module action of RG on V by $(\sum a_g g)v = \sum a_g \rho(g)(v)$.

Given a RG-module V, the linear map $\rho(g) : v \mapsto gv$ is an automorphism of V and $\rho(g_1)\rho(g_2) = \rho(g_1 g_2)$ so $\rho : G \to GL(V)$ is a representation. □

We have defined the group algebra without saying what an algebra is! For the record, an (associative) *R-algebra* is a ring A with a 1, equipped with a (unital) ring homomorphism $R \to A$ whose image lies in the center of A. The group algebra RG is indeed an example of an R-algebra.

The group algebra gives another example of a representation, called the *regular representation*. In fact for any ring A we may regard A itself as a left A-module with the action of A on itself given by multiplication of the elements. We denote this left A-module by ${}_A A$ when we wish to emphasize the module structure, and this is the (left) regular representation of A. When $A = RG$ we may describe action on ${}_{RG}RG$ by observing that each element $g \in G$ acts on ${}_{RG}RG$ by permuting the basis elements in the fashion $g \cdot h = gh$. Thus each g acts by a *permutation matrix*, namely a matrix in which in every row and column there is precisely one non-zero entry, and that non-zero entry is 1. The regular

representation is an example of a *permutation representation*, namely one in which every group element acts by a permutation matrix.

Regarding representations of G as RG-modules has the advantage that many definitions we wish to make may be borrowed from module theory. Thus we may study RG-submodules of an RG-module V, and if we wish we may call them *subrepresentations* of the representation afforded by V. To specify an RG-submodule of V it is necessary to specify an R-submodule W of V which is closed under the action of RG. This is equivalent to requiring that $\rho(g)w \in W$ for all $g \in G$ and $w \in W$. We say that a submodule W satisfying this condition is *stable* under G, or that it is an *invariant submodule* or *invariant subspace* (if R happens to be a field). Such an invariant submodule W gives rise to a homomorphism $\rho_W : G \to GL(W)$ which is the subrepresentation afforded by W.

(1.3) *Examples.* 1. Let $C_2 = \{1, -1\}$ be cyclic of order 2 and consider the representation

$$\begin{aligned} \rho : C_2 &\to GL(\mathbb{R}^2) \\ 1 &\mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ -1 &\mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \end{aligned}$$

One checks that the invariant subspaces are $\{0\}$, $\langle \binom{1}{0} \rangle$, $\langle \binom{0}{1} \rangle$, $\mathbb{R}^2$ and no others. Here $\mathbb{R}^2 = \langle \binom{1}{0} \rangle \oplus \langle \binom{0}{1} \rangle$ is the direct sum of two invariant subspaces.

2. In Example 4 of 1.1 above, an elementary calculation shows that $\langle \binom{0}{1} \rangle$ is the only 1-dimensional invariant subspace, and so it is not possible to write the representation space V as the direct sum of two non-zero invariant subspaces.

We also have the notions of a *homomorphism* and an *isomorphism* of RG-modules. Since RG has as a basis the elements of G, to check that an R-linear homomorphism $f : V \to W$ is in fact a homomorphism of RG modules, it suffices to check that $f(gv) = gf(v)$ for all $g \in G$ — we do not need to check for every $x \in RG$. By means of the identification of RG-modules with representations of G (in the first definition given here) we may refer to homomorphisms and isomorphisms of group representations. In many books the algebraic condition on the representations which these notions entail is written out explicitly, and two representations which are isomorphic are also said to be *equivalent*.

If V and W are RG-modules then we may form their (external) *direct sum* $V \oplus W$, which is the same as the direct sum of V and W as R-modules together with an action of G given by $g(v, w) = (gv, gw)$. We also have the notion of the internal direct sum of RG-modules and write $U = V \oplus W$ to mean that U has RG-submodules V and W satisfying $U = V + W$ and $V \cap W = 0$. In this situation we also say that V and W are *direct summands* of U. We already met this property in (1.3) above, whose first part is an example of a representation which is a direct sum of two non-zero subspaces; however, the second part of (1.3) provides an example of a subrepresentation which is not a direct summand.

We come now to our first non-trivial result, and one which is fundamental to the study of representations over fields of characteristic zero. Here, as in many other places, we require that the ring R be a field, and in this situation we use the symbols R or k instead of R.

(1.4) THEOREM (Maschke). *Let V be a representation of the finite group G over a field F in which $|G|$ is invertible. Let W be an invariant subspace of V. Then there exists an invariant subspace W_1 of V such that $V = W \oplus W_1$ as representations.*

Proof. Let $\pi : V \to W$ be any projection of V onto W as vector spaces, i.e. a linear transformation such that $\pi(w) = w$ for all $w \in W$. Since F is a field, we may always find such a projection by finding a vector space complement to W in V, and projecting off the complementary factor. Then $V = W \oplus \mathrm{Ker}(\pi)$ as vector spaces, but $\mathrm{Ker}(\pi)$ is not necessarily invariant under G. Consider the map

$$\pi' = \frac{1}{|G|} \sum_{g \in G} g\pi g^{-1} : V \to V.$$

Then π' is linear and if $w \in W$ then

$$\begin{aligned} \pi'(w) &= \frac{1}{|G|} \sum_{g \in G} g\pi(g^{-1}w) \\ &= \frac{1}{|G|} \sum_{g \in G} gg^{-1}w \\ &= \frac{1}{|G|}|G|w \\ &= w. \end{aligned}$$

Since $\pi'(v) \in W$ for all $v \in V$, π' is a projection onto W and so $V = W \oplus \mathrm{Ker}(\pi')$. We show finally that $\mathrm{Ker}(\pi')$ is an invariant subspace. If $h \in G$ and $v \in \mathrm{Ker}(\pi')$ then

$$\begin{aligned} \pi'(hv) &= \frac{1}{|G|} \sum_{g \in G} g\pi(g^{-1}hv) \\ &= \frac{1}{|G|} \sum_{g \in G} h(h^{-1}g)\pi((h^{-1}g)^{-1}v) \\ &= h\pi'(v) \\ &= 0 \end{aligned}$$

since as g ranges over the elements of G, so does $h^{-1}g$. This shows that $hv \in \mathrm{Ker}(\pi')$ and so $\mathrm{Ker}(\pi')$ is an invariant subspace. □

Let A be a ring with a 1. An A-module V is said to be *simple* or *irreducible* if V has no A-submodules other than 0 and V. A module which is the direct sum of simple submodules is said to be *semisimple* or *completely reducible* and we saw in (1.3) examples of modules, one of which was semisimple and the other of which was not. We know from the Jordan-Hölder theorem in module theory that in some sense simple modules are the building blocks for arbitrary modules of finite composition length. One way in which these building blocks may be combined is as a direct sum — a construction we feel we understand quite well — giving a semisimple module, but there may be other modules which are not constructed from simple modules in this way.

The next results relate the property of semisimplicity to the property which appears in the statement of Maschke's theorem, namely that every submodule of a module is a direct summand. Our immediate application of this will be an interpretation of Maschke's theorem, but the results have application in greater generality in situations where R is not a field, or when $|G|$ is not invertible in R. To simplify the exposition we have imposed a finiteness condition in the statement of each result, thereby avoiding arguments which use Zorn's lemma. These finiteness conditions can be removed, and we leave the details to the reader in an exercise at the end of this section.

In the special case when the ring A is a field and A-modules are vector spaces the next result is a familiar statement from linear algebra.

(1.5) LEMMA. *Let A be a ring with a 1 and suppose that $U = S_1 + \cdots + S_n$ is an A-module which can be written as the sum of finitely many simple modules $S_1, \ldots, S_n$. If V is any submodule of U there is a subset $I = \{i_1, \ldots, i_r\}$ of $\{1, \ldots, n\}$ such that $U = V \oplus S_{i_1} \oplus \cdots S_{i_r}$. In particular,*

(1) V is a direct summand of U, and

(2) (taking $V = 0$), U is the direct sum of some subset of the S_i, and hence is necessarily semisimple.

Proof. Choose a subset I maximal subject to the condition that the sum $W = V \oplus \bigoplus_{i \in I} S_i$ is a direct sum. Note that $I = \emptyset$ has this property, so we are indeed taking a maximal element of a non-empty set. We show that $W = U$. If $W \neq U$ then $S_j \not\subseteq W$ for some j. Now $S_j \cap W = 0$, being a proper submodule of S_j, so $S_j + W = S_j \oplus W$ and we obtain a contradiction to the maximality of I. Therefore $W = U$. □

(1.6) PROPOSITION. *Let A be a ring with a 1 and let U be an A-module. The following are equivalent.*

(1) U can be expressed as a direct sum of finitely many simple A-submodules.

(2) U can be expressed as a sum of finitely many simple A-submodules.

(3) U has finite composition length and has the property that every submodule of U is a direct summand of U.

When these three conditions hold, every submodule of U and every factor module of U may also be expressed as the direct sum of finitely many simple modules.

Proof. The implication (1) $\Rightarrow$ (2) is immediate and the implications (2) $\Rightarrow$ (1) and (2) $\Rightarrow$ (3) follow from Lemma 1.5. To show that (3) $\Rightarrow$ (1) we argue by induction on the composition length of U, and first observe that hypothesis (3) passes to submodules of U. For if V is a submodule of U and W is a submodule of V then $U = W \oplus X$ for some submodule X, and now $V = W \oplus (X \cap V)$ by the modular law (Exercise 2). Proceeding with the induction argument, when U has length 1 it is a simple module, and so the induction starts. If U has length greater than 1, it has a submodule V and by condition (3), $U = V \oplus W$ for some submodule W. Now both V and W inherit condition (3) and are of shorter length, so by induction they are direct sums of simple modules and hence so is U.

We have already observed that every submodule of U inherits condition (3), and so satisfies condition (1) also. Every factor module of U has the form U/V for some submodule V of U. If condition (3) holds than $U = V \oplus W$ for some submodule W which we have just observed satisfies condition (1), and hence so does U/V since $U/V \cong W$. □

We now present a different statement of Maschke's theorem. The statement remains correct if the words 'finite-dimensional' are removed from it, but we leave the proof of this stronger statement to the exercises.

(1.7) COROLLARY. *Let R be a field in which $|G|$ is invertible. Then every finite-dimensional RG-module is semisimple.*

Proof. This combines Theorem 1.4 with the equivalence of the statements of Proposition 1.6. □

This theorem puts us in very good shape if we want to know about the representations of a finite group over a field in which $|G|$ is invertible — for example any field of characteristic zero. To obtain a description of all possible finite-dimensional representations we need only describe the simple ones, and then arbitrary ones are direct sums of these.

The following corollaries to Lemma 1.5 will not immediately be used, but we present them here because they have the same flavor as the results just considered. They could be omitted at this point, and read as they are needed.

(1.8) COROLLARY. *Let A be a ring with a 1, and let U be an A-module of finite composition length.*

(1) The sum of all the simple submodules of U is a semisimple module, which is the unique largest semisimple submodule of U.

(2) The sum of all submodules of U isomorphic to some given simple module S is a submodule isomorphic to a direct sum of copies of S. It is the unique largest submodule of U with this property.

Proof. The submodules described can be expressed as the sum of finitely many submodules by the finiteness condition on U. They are the unique largest submodules with their respective properties since they contain all simple submodules (in case (1)), and all submodules isomorphic to S (in case (2)). □

The largest semisimple submodule of a module U is called the *socle* of U, and is denoted $\mathrm{Soc}(U)$.

(1.9) COROLLARY. *Let $U = S_1^{a_1} \oplus \cdots \oplus S_r^{a_r}$ be a semisimple module over a ring A with a 1, where the S_i are non-isomorphic simple modules and the a_i are the multiplicities to which they occur as summands of U. Then each submodule $S_i^{a_i}$ is uniquely determined and is characterized as the unique largest submodule of U expressible as a direct sum of copies of S_i.*

Proof. It suffices to show that $S_i^{a_i}$ contains every submodule of U isomorphic to S_i. If T is any non-zero submodule of U not contained in $S_i^{a_i}$ then for some $j \neq i$ its projection to a summand S_j must be non-zero. If we assume that T is simple this projection will be an isomorphism $T \cong S_j$. Thus all simple submodules isomorphic to S_i are contained in the summand $S_i^{a_i}$. □

Exercises for Section 1.

1. In Example 1 of 1.3 prove that there are no more invariant subspaces other than the ones listed.

2. (The modular law.) Let A be a ring and $U = V \oplus W$ an A-module which is the direct sum of A-modules V and W. Show by example that if X is any submodule of U then it need not be the case that $X = (V \cap X) \oplus (W \cap X)$. Show that if we make the assumption that $V \subseteq X$ then it is true that $X = (V \cap X) \oplus (W \cap X)$.

3. Suppose that ρ is a finite-dimensional representation of a finite group G over $\mathbb{C}$. Show that for each $g \in G$ the matrix $\rho(g)$ is diagonalizable.

4. Let

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

be two representations of G on the same R-module V which are injective as homomorphisms. (One says that such a representation is *faithful*.) Consider the three statements

(a) the RG-modules given by ρ_1 and ρ_2 are isomorphic,

(b) the subgroups $\rho_1(G)$ and $\rho_2(G)$ are conjugate in $GL(V)$,

(c) for some automorphism $\alpha \in \mathrm{Aut}(G)$ the representations ρ_1 and $\rho_2\alpha$ are isomorphic.

Show that (a) $\Rightarrow$ (b) and that (b) $\Rightarrow$ (c). Show also that if $\alpha \in \mathrm{Aut}(G)$ is an inner automorphism (i.e. one of the form 'conjugation by g' for some $g \in G$) then ρ_1 and $\rho_1\alpha$ are isomorphic.

5. One form of the Jordan-Zassenhaus theorem states that for each n, $GL(n,\mathbb{Z})$ (that is, $\mathrm{Aut}(\mathbb{Z}^n)$) has only finitely many conjugacy classes of subgroups of finite order. Assuming this, show that for each finite group G and each integer n there are only finitely many isomorphism classes of representations of G on $\mathbb{Z}^n$.

6. (a) Write out a proof of Maschke's theorem in the case of representations over $\mathbb{C}$ along the following lines.

Given a representation $\rho : G \to GL(V)$ where V is a vectorspace over $\mathbb{C}$, let $(\ ,\ )$ be any positive definite Hermitian form on V. Define a new form $(\ ,\ )_1$ on V by

$$(v,w)_1 = \frac{1}{|G|}\sum_{g\in G}(gv,gw).$$

Show that $(\ ,\ )_1$ is a positive definite Hermitian form, preserved under the action of G, i.e. $(v,w)_1 = (gv,gw)_1$ always.

If W is a subrepresentation of V, show that $V = W \oplus W^{\perp}$ as representations.

(b) Show that any finite subgroup of $GL(n,\mathbb{C})$ is conjugate to a subgroup of $U(n,\mathbb{C})$ (the unitary group, consisting of $n \times n$ complex matrices A satisfying $A\bar{A}^T = I$). Show that any finite subgroup of $GL(n,\mathbb{R})$ is conjugate to a subgroup of $O(n,\mathbb{R})$ (the orthogonal group consisting of $n \times n$ real matrices A satisfying $AA^T = I$).

7. Let $U = S_1 \oplus \cdots \oplus S_r$ be an A-module which is the direct sum of finitely many simple modules $S_1, \ldots, S_r$. Show that if T is any simple submodule of U then $T \cong S_i$ for some i.

8. Suppose U is an A-module for which we have two expressions

$$U \cong S_1^{a_1} \oplus \cdots \oplus S_r^{a_r} \cong S_1^{b_1} \oplus \cdots \oplus S_r^{b_r}$$

where $S_1, \ldots, S_r$ are non-isomorphic simple modules. Show that $a_i = b_i$ for all i.

9. Let $G = \langle x, y \mid x^2 = y^2 = 1 = [x,y]\rangle$ be the Klein four-group, $R = \mathbb{F}_2$, and consider the two representations ρ_1 and ρ_2 specified on the generators of G by

$$\rho_1(x) = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \rho_1(y) = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

and

$$\rho_2(x) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \quad \rho_2(y) = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Calculate the socles of these two representations.

10. Let $G = C_p = \langle x \rangle$ and $R = \mathbb{F}_p$ for some prime $p \geq 3$. Consider the two representations ρ_1 and ρ_2 specified by

$$\rho_1(x) = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad \rho_2(x) = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Calculate the socles of these two representations. Show that the second representation is the direct sum of two non-zero subrepresentations.

11. (a) Using 1.6 show that if A is a ring for which the regular representation ${}_AA$ is semisimple, then every finitely generated A-module is semisimple.

(b) Extend the result of part (a), using Zorn's lemma, to show that if A is a ring for which the regular representation ${}_AA$ is semisimple, then every A-module is semisimple.

12. Let U be a module for a ring A with a 1. Show that the following three statements are equivalent.

(1) U is a direct sum of simple A-submodules.

(2) U is a sum of simple A-submodules.

(3) every submodule of U is a direct summand of U.

[Use Zorn's lemma to prove a version of Lemma 1.5 which has no finiteness hypothesis and then copy Proposition 1.6. This deals with all implications except (3) $\Rightarrow$ (2). For that, use the fact that A has a 1 and hence every (left) ideal is contained in a maximal (left) ideal, combined with condition (3), to show that every submodule of U has a simple submodule. Consider the sum of all simple submodules of U and show that it equals U.]

13. Let RG be the group algebra of a finite group G over a commutative ring R with 1. Let S be a simple RG-module and let I be the anihilator in R of S, that is

$$I = \{r \in R \mid rx = 0 \text{ for all } x \in S\}.$$

Show that I is a maximal ideal in R.

[This question requires some familiarity with standard commutative algebra. We conclude from this result that when considering simple RG modules we may reasonably assume that R is a field, since S may naturally be regarded as an $(R/I)G$-module and R/I is a field.]

2. The structure of algebras for which every module is semisimple.

In this section we work with an abstract finite-dimensional algebra A over a field k (unless greater generality is stated). In studying the simple A-modules it is no loss of generality to assume that we are working over a field, as explained in an exercise at the end of the last section. Furthermore, every simple A-module is isomorphic to one of the form A/I where I is some maximal left ideal of A. This is because if $x \in S$ is any non-zero element of a simple module S then the mapping of left modules $A \to S$ specified by $a \mapsto ax$ is surjective, by simplicity of S, and so $S \cong A/I$ where I is the kernel, which is a maximal ideal again by simplicity of S.

The following general result is basic, and will be used time and time again.

(2.1) THEOREM (Schur's Lemma). *Let S_1 and S_2 be simple A-modules where A is a ring with 1. Then $\mathrm{Hom}_A(S_1, S_2) = 0$ unless $S_1 \cong S_2$, in which case $\mathrm{End}_A(S_1)$ is a division ring. In case A is a finite-dimensional algebra over an algebraically closed ground field k, then every endomorphism of S_1 is scalar multiplication by an element of k. Thus $\mathrm{End}_A(S_1) \cong k$.*

Proof. Suppose $\theta : S_1 \to S_2$ is a non-zero morphism. Then $0 \neq \theta(S_1) \subseteq S_2$, so $\theta(S_1) = S_2$ by simplicity of S_2 and θ is surjective. Thus $\mathrm{Ker}\,\theta \neq S_1$, so $\mathrm{Ker}\,\theta = 0$ by simplicity of S_1, and θ is injective. Therefore θ is invertible, $S_1 \cong S_2$ and $\mathrm{End}_A(S_1)$ is a division ring.

If k is algebraically closed, let λ be an eigenvalue of θ. Now $(\theta - \lambda I) : S_1 \to S_1$ is a singular endomorphism of A-modules, so $\theta - \lambda I = 0$ and $\theta = \lambda I$. □

The next result is straightforward and seemingly innocuous, but it has an important consequence for representation theory. It is the main tool in recovering the structure of an algebra from its representations. We use the notation A^{op} to denote the *opposite* ring of A, namely the ring which has the same set and the same addition as A, but in which there is a new multiplication $\cdot$ given by $a \cdot b = ba$.

(2.2) LEMMA. *For any ring A with a 1, $\mathrm{End}_A({}_AA) \cong A^{\mathrm{op}}$.*

Proof. The inverse isomorphisms are

$$\phi \mapsto \phi(1)$$
$$(a \mapsto ax) \leftarrow x.$$

There are several things here which need to be checked: that the second assignment does take values in $\mathrm{End}_A({}_AA)$, that the morphisms are ring homomorphisms, and that they are mutually inverse. We leave most of this to the reader, observing only that under the first homomorphism a composite $\theta\phi$ is sent to $(\theta\phi)(1) = \theta(\phi(1)) = \theta(\phi(1)1) = \phi(1)\theta(1)$, so that this is indeed a homomorphism to A^{op}. □

Observe that the proof of Lemma 2.2 establishes that every endomorphism of the regular representation is of the form 'right multiplication by some element'.

We say that a ring A with 1 is *semisimple* if the regular representation ${}_AA$ is semisimple. There are other equivalent definitions of a semisimple ring which will be explored further in Chapter 6.

A ring A with 1 all of whose modules are semisimple is itself called *semisimple*. By Exercise 1.11 it is equivalent to suppose that the regular representation ${}_AA$ is semisimple. It is also equivalent to suppose that the Jacobson radical of the ring is zero, but we will not deal with this point of view until Chapter 6.

(2.3) THEOREM (Artin-Wedderburn). *Let A be a finite-dimensional algebra over a field with the property that every finite-dimensional module is semisimple. Then A is a direct sum of matrix algebras over division rings. Specifically, if*

$$ {}_AA \cong S_1^{n_1} \oplus \cdots \oplus S_r^{n_r} $$

where the $S_1, \ldots, S_r$ are non-isomorphic simple modules occuring with multiplicities n_i in the regular representation, then

$$ A \cong M_{n_1}(D_1) \oplus \cdots \oplus M_{n_r}(D_r) $$

where $D_i = \mathrm{End}_A(S_i)^{\mathrm{op}}$.

More is true: every such direct sum of matrix algebras is a semisimple algebra, and each matrix algebra over a division ring is a *simple* algebra, namely one which has no 2-sided ideals apart from the zero ideal and the whole ring (see the exercises). Furthermore, the matrix algebra summands are uniquely determined as subsets of A (although the module decomposition of ${}_AA$ is usually only determined up to isomorphism). The uniqueness of the summands will be established in Proposition 3.22. Notice that if k happens to be algebraically closed then by Schur's lemma the division rings D_i which appear must all be equal to k.

Proof. We first observe that if we have a direct sum decomposition $U = U_1 \oplus \cdots \oplus U_r$ of a module U then $\mathrm{End}_A(U)$ is isomorphic to the algebra of $r \times r$ matrices in which the i, j entries lie in $\mathrm{Hom}_A(U_j, U_i)$. This is because any endomorphism $\phi : U \to U$ may be writen as components $\phi = (\phi_{ij})$ where $\phi_{ij} : U_j \to U_i$, and in terms of components these endomorphisms compose in the manner of matrix multiplication. Since $\mathrm{Hom}_A(S_j^{n_j}, S_i^{n_i}) = 0$ if $i \neq j$ by Schur's lemma, the decomposition of ${}_AA$ gives

$$ \mathrm{End}_A({}_AA) \cong \mathrm{End}_A(S_1^{n_1}) \oplus \cdots \oplus \mathrm{End}_A(S_r^{n_r}) $$

and furthermore $\mathrm{End}_A(S_i^{n_i}) \cong M_{n_i}(D_i^{\mathrm{op}})$. By Lemma 2.2 we identify $\mathrm{End}_A({}_AA)$ as A^{op}. □

(2.4) COROLLARY. *Let A be a finite-dimensional semisimple algebra over a field k which is algebraically closed. In any decomposition*

$$ {}_AA = S_1^{n_1} \oplus \cdots \oplus S_r^{n_r} $$

where the S_i are pairwise non-isomorphic simple modules we have that $S_1, \ldots, S_r$ is a complete set of representatives of the isomorphism classes of simple A-modules, $n_i = \dim_k S_i$ and $\dim_k A = n_1^2 + \cdots + n_r^2$.

Proof. All isomorphism types of simple modules must appear in the decomposition because every simple module can be expressed as a homomorphic image of ${}_AA$ (as observed at the start of this section), and so must be a homomorphic image of one of the modules S_i. Since k is algebraically closed all the division rings D_i coincide with k by Schur's lemma, and $\mathrm{End}_A(S_i^{n_i}) \cong M_{n_i}(k)$. The ring decomposition $A = M_{n_1}(k) \oplus \cdots \oplus M_{n_r}(k)$ immediately gives $\dim_k A = n_1^2 + \cdots + n_r^2$. From the way this decomposition was constructed as an endomorphism ring in 2.3 we see that $M_{n_i}(k)$ has non-zero action on the summand $S_i^{n_i}$, and zero action on the other summands $S_j^{n_j}$ with $j \neq i$. It follows that as left A-modules, $M_{n_i}(k) \cong S_i^{n_i}$ since both sides are isomorphic to the quotient of A by the elements which $M_{n_i}(k)$ annihilates. Hence

$$ \dim_k M_{n_i}(k) = n_i^2 = \dim_k S_i^{n_i} = n_i \dim S_i, $$

and so $\dim S_i = n_i$. □

Let us now restate what we have proved specifically in the context of group representations.

(2.5) COROLLARY. *Let G be a finite group and k a field in which $|G|$ is invertible.*

(1) As a ring, kG is a direct sum of matrix algebras over division rings,

(2) Suppose in addition that k is algebraically closed, let $S_1, \ldots, S_r$ be a set of representatives of the simple kG-modules (up to isomorphism) and put $d_i = \dim_k S_i$. Then d_i equals the multiplicity with which S_i is a summand of the regular representation of G, and $|G| = d_1^2 + \cdots + d_r^2$.

Part (2) of this result provides a numerical criterion which enables us to say when we have constructed all the simple modules of a group over an algebraically closed field k in which $|G|$ is invertible. For if we have constructed a set of non-isomorphic simple modules with the property that the squares of their degrees sum to $|G|$, then we have a complete set. While this is an easy condition to verify, it will be superceded later on by the even more straightforward criterion that the number of simple kG-modules (with the same hypotheses on k) equals the number of conjugacy classes of elements of G. Once we have proved this, the formula $\sum d_i^2 = |G|$ allows the degree of the last simple representation to be determined once the others are known.

(2.6) *Example.* Over $\mathbb{R}$ we have constructed for S_3 the trivial representation, the sign representation which is also of dimension 1 but not the same as the trivial representation, and a 2-dimensional representation which is simple because visibly no 1-dimensional subspace of the plane is invariant under the group action. Since $1^2 + 1^2 + 2^2 = |S_3|$ we have constructed all the simple representations.

Exercises for Section 2.

1. Let A be a finite-dimensional semisimple algebra. Show that A has only finitely many isomorphism types of modules in each dimension. [This is not in general true for algebras which are not semisimple: The representations of $C_2 \times C_2 = \langle x, y \rangle$ over $\overline{\mathbb{F}}_2$ specified for each $\lambda \in \overline{\mathbb{F}}_2$ by

$$\rho_\lambda(x) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \qquad \rho_\lambda(y) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & \lambda & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

all have dimension 4 and are non-isomorphic.]

2. Using Exercises 1.5 and 2.1 (which you may assume without proof), show that if k is any field of characteristic 0 then for each natural number m, $GL_n(k)$ has only finitely many conjugacy classes of subgroups of order m. [In view of the comment to problem 1, the same is not true when when $k = \overline{\mathbb{F}}_2$.]

3. Let D be a division ring and n a natural number.

(a) Show that the natural $M_n(D)$-module consisting of column vectors of length n is a simple module.

(b) Show that $M_n(D)$ is semisimple and has up to isomorphism only one simple module.

(c) Show that every algebra of the form

$$M_{n_1}(D_1) \oplus \cdots \oplus M_{n_r}(D_r)$$

is semisimple.

(d) Show that $M_n(D)$ is a *simple* ring, namely one in which the only 2-sided ideals are the zero ideal and the whole ring.

4. Prove the following extension of 2.4:

THEOREM. *Let A be a finite-dimensional semisimple algebra, S a simple A-module and $D = \mathrm{End}_A(S)$. Then S may be regarded as a module over D and the multiplicity of S as a summand of ${}_AA$ equals* $\dim_D S$.

5. Using the fact that $M_n(k)$ has a unique simple module prove the Noether-Skolem theorem, that any algebra automorphism of $M_n(k)$ is inner, i.e. of the form conjugation by some invertible matrix.

6. Show that for any field k we have $M_n(k) \cong M_n(k)^{\mathrm{op}}$, and in general for any division ring D that given any positive integer n, $M_n(D) \cong M_n(D)^{\mathrm{op}}$ if and only if $D \cong D^{\mathrm{op}}$.

7. Let A be any algebra. An element $e \in A$ is called *idempotent* if and only if $e^2 = e$.

(a) Let V be any A-module. Show that an endomorphism $e : V \to V$ is a projection onto a subspace W if and only if e is idempotent as an element of $\mathrm{End}_A(V)$.

(b) Show that direct sum decompositions $V = W_1 \oplus W_2$ as A-modules are in bijection with expressions $1 = e + f$ in $\mathrm{End}_A(V)$, where e and f are idempotent elements with $ef = fe = 0$. (In case $ef = fe = 0$, e and f are called *orthogonal*.)

(c) Let $e_1, e_2 \in \mathrm{End}_A(V)$ be idempotent elements. Show that $e_1(V) \cong e_2(V)$ as A-modules if and only if e_1 and e_2 are conjugate under the unit group $\mathrm{End}_A(V)^*$ (i.e. there exists an A-endomorphism $\alpha : V \to V$ such that $e_2 = \alpha e_1 \alpha^{-1}$).

(d) An idempotent element e is called *primitive* if it cannot be expressed as a sum of orthogonal idempotent elements in a non-trivial way. Show that $e \in \mathrm{End}_A(V)$ is primitive if and only if $e(V)$ has no (non-trivial) direct sum decomposition. (In this case V is said to be *indecomposable*.)

(e) Show that all primitive idempotent elements in $M_n(k)$ are conjugate under the action of the unit group $GL_n(k)$. Write down explicitly any primitive idempotent element in $M_3(k)$.

3. Characters

The characters of a finite group take values in a field of characteristic zero which we may always take to be a subfield of the complex numbers, and so frequently in this section we will restrict our attention to the complex numbers $\mathbb{C}$. When $\rho : G \to GL(V)$ is a finite-dimensional representation of G over $\mathbb{C}$ we define the *character* χ of ρ to be the function

$$\chi : G \to \mathbb{C}$$

given by $\chi(g) = \mathrm{tr}(\rho(g))$, the trace of the linear map $\rho(g)$. We say that the representation ρ and the representation space V *afford* the character χ, and we may write χ_ρ or χ_V when we wish to specify this character more precisely.

(3.1) PROPOSITION.
(1) $\chi(1)$ *is the degree of* ρ.
(2) For every $g \in G$ *we have* $\chi(g^{-1}) = \overline{\chi(g)}$, *the complex conjugate.*
(3) $\chi(hgh^{-1}) = \chi(g)$ *for all* $g, h \in G$.
(4) If V *and* W *are isomorphic* $\mathbb{C}G$*-modules then* $\chi_V(g) = \chi_W(g)$ *for all* $g \in G$.

Proof. (1) is immediate because the identity of the group must act as the identity matrix.

(2) Each element g has finite order so its eigenvalues $\lambda_1, \ldots, \lambda_n$ are roots of unity. The inverse g^{-1} has eigenvalues $\lambda_1^{-1}, \ldots, \lambda_n^{-1} = \overline{\lambda}_1, \ldots, \overline{\lambda}_n$ and so $\chi(g^{-1}) = \overline{\lambda}_1 + \cdots + \overline{\lambda}_n = \overline{\chi(g)}$.

(3) results from the fact that $\mathrm{tr}(ab) = \mathrm{tr}(ba)$ for endomorphisms a and b, so that $\chi(hgh^{-1}) = \mathrm{tr}\,\rho(hgh^{-1}) = \mathrm{tr}(\rho(h)\rho(g)\rho(h^{-1})) = \mathrm{tr}\,\rho(g) = \chi(g)$.

(4) Suppose that ρ_V and ρ_W are the representations of G on V and W, and that we have an isomorphism of $\mathbb{C}G$-modules $\alpha : V \to W$. Then $\alpha\rho_V(g) = \rho_W(g)\alpha$ for all $g \in G$, so that $\chi_W(g) = \mathrm{tr}\,\rho_W(g) = \mathrm{tr}(\alpha\rho_V(g)\alpha^{-1}) = \mathrm{tr}\,\rho_V(g) = \chi_V(g)$. □

Part (4) of the above result is a great convenience since when talking about characters we do not have to worry about the possibility that two modules may be isomorphic but not actually the same.

From part (3) of 3.1 we see that the character of a representation takes the same value on all elements in a conjugacy class of G. The table of complex numbers whose rows are indexed by the isomorphism types of simple representations of G, whose columns are indexed by the conjugacy classes of G and whose entries are the values of the characters of the simple representations on representatives of the conjugacy classes is called the *character table* of G. It is usual to index the first column of a character table by the (conjugacy class of the) identity, and to put the character of the trivial representation as the top row. With this convention the top row of every character table will be a row of 1's, and the first column will list the degrees of the simple representations. At the top of the table it is usual to list two rows, the second of which (immediately above a horizontal line) is a list

of representatives of the conjugacy classes of elements of G, in some notation. The very top row lists the value of $|C_G(g)|$ for the element g underneath.

(3.2) *Example.* We present the character table of S_3. We saw at the end of Section 2 that we already have a complete list of the simple modules for S_3, and the values of their characters on representatives of the conjugacy classes of S_3 are computed from the matrices which give these representations.

Centralizer orders	6	2	3
Conjugacy class representative	1	(12)	(123)
Trivial	1	1	1
Sign	1	-1	1
	2	0	-1

TABLE: The character table of S_3.

We will see that the character table has remarkable properties, among which are that it is always square, and its rows (and also its columns) satisfy certain orthogonality relations. Our next main goal is to state and prove these results. In order to do this we first introduce three ways to construct new representations of a group from existing ones. These constructions have validity no matter what ring R we work over, although in the application to the character table we will suppose that $R = \mathbb{C}$.

Suppose that V and W are representations of G over R. The R-module $V \otimes_R W$ acquires an action of G by means of the formula $g \cdot (v \otimes w) = gv \otimes gw$, thereby making the tensor product into a representation. This is what is called the *tensor product* of the representations V and W, but it is not the only occurrence of tensor products in representation theory, and as the other ones are different this one is sometimes also called the *Kronecker product*. The action of G on the Kronecker product is called the *diagonal* action.

For the second construction we form the R-module $\mathrm{Hom}_R(V, W)$. This acquires an action of G by means of the formula $(g \cdot f)(v) = gf(g^{-1}v)$ for each R-linear map $f : V \to W$ and $g \in G$.

The third construction is the particular case of the second in which we take W to be the trivial module R. We write $V^* = \mathrm{Hom}_R(V, R)$ and the action is $(g \cdot f)(v) = f(g^{-1}v)$. This representation is called the *dual* or *contragredient* representation of V, and it is usually only considered when V is free as an R-module.

If R happens to be a field and we have bases $v_1, \ldots, v_m$ for V and $w_1, \ldots, w_n$ for W then $V \otimes W$ has a basis $\{v_i \otimes w_j \mid 1 \leq i \leq m, 1 \leq j \leq n\}$ and V^* has a dual basis $\hat{v}_1, \ldots, \hat{v}_m$. With respect to these bases an element $g \in G$ acts on $V \otimes W$ with the matrix which is the tensor product of the two matrices giving its action on V and W, and on V^* it acts with the transpose of the inverse of the matrix in its action on V. The tensor product of two matrices is not seen so often these days. If (a_{pq}), (b_{rs}) are an $m \times m$ matrix and an

$n \times n$ matrix their tensor product is the $mn \times mn$ matrix (c_{ij}) where if $i = (p-1)n + r$ and $j = (q-1)n + s$ with $1 \le p, q \le m$ and $q \le r, s \le n$ then $c_{ij} = a_{pq}b_{rs}$. For example,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \otimes \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae & af & be & bf \\ ag & ah & bg & bh \\ ce & cf & de & df \\ cg & ch & dg & dh \end{pmatrix}.$$

If $\alpha : V \to V$ and $\beta : W \to W$ are endomorphisms, then the matrix of

$$\alpha \otimes \beta : V \otimes W \to V \otimes W$$

is the tensor product of the matrices which represent α and β. We see from this that $\operatorname{tr}(\alpha \otimes \beta) = \operatorname{tr}(\alpha)\operatorname{tr}(\beta)$.

In the following result we consider the sum and product of characters, which are defined pointwise by the formulas

$$(\chi_V + \chi_W)(g) = \chi_V(g) + \chi_W(g)$$
$$(\chi_V \cdot \chi_W)(g) = \chi_V(g) \cdot \chi_W(g).$$

(3.3) PROPOSITION. *Let V and W be finite-dimensional representations of G over a field k of characteristic zero.*

(1) $V \oplus W$ has character $\chi_V + \chi_W$.
(2) $V \otimes W$ has character $\chi_V \cdot \chi_W$.
(3) V^* has character $\chi_{V^*}(g) = \chi_V(g^{-1}) = \overline{\chi_V(g)}$.
(4) $\operatorname{Hom}_k(V, W) \cong V^* \otimes_k W$ as kG-modules, and this representation has character equal to $\chi_{V^*} \cdot \chi_W$.

We will see in the proof that the isomorphism of modules in part (4) is in fact valid without restriction on the characteristic of the field k.

Proof. (1), (2) and (3) are immediate on taking matrices for the representations. As for (4), we define a linear map

$$\alpha : V^* \otimes W \to \operatorname{Hom}_k(V, W)$$
$$f \otimes w \mapsto (v \mapsto f(v) \cdot w),$$

this being the specification on basic tensors. We show that α is injective. Assuming that $w_1, \ldots, w_n$ is a basis of W, every element of $V^* \otimes W$ can be written $\sum_{i=1}^n f_i \otimes w_i$ where $f_i : V \to k$. Such an element is sent by α to the map $v \mapsto \sum f_i(v)w_i$, where $v \in V$. If this is the zero mapping then $\sum f_i(v)w_i = 0$ for all $v \in V$, and by independence of the w_i we have $f_i(v) = 0$ for all $v \in V$. Thus $\sum_{i=1}^n f_i \otimes w_i = 0$ which shows that α is injective.

Since $V^* \otimes W$ and $\mathrm{Hom}_k(V,W)$ have the same dimension (equal to $\dim V \cdot \dim W$), α is a vector space isomorphism. It is also a map of kG-modules, since for $g \in G$,

$$\begin{aligned}\alpha(g(f \otimes w)) &= \alpha(gf \otimes gw)\\ &= (v \mapsto (gf)(v) \cdot gw)\\ &= (v \mapsto g(f(g^{-1}v)w))\\ &= g(v \mapsto f(v)w)\\ &= g\alpha(f \otimes w).\end{aligned}$$

□

A fundamental notion in dealing with group actions is that of fixed points. If V is an RG-module we define the *fixed points* $V^G = \{v \in V \mid gv = v \text{ for all } g \in G\}$. This is the largest RG-submodule of V on which G has trivial action.

(3.4) LEMMA. *Over any ring R,* $\mathrm{Hom}_R(V,W)^G = \mathrm{Hom}_{RG}(V,W)$.

Proof. An R-linear map $f : V \to W$ is a morphism of RG-modules precisely if it commutes with the action of G, which is to say $f(gv) = gf(v)$ for all $g \in G$ and $v \in V$, or in other words $gf(g^{-1}v) = f(v)$ always. This is exactly the condition that f is fixed under the action of G. □

The next result is an abstraction of the idea which was used in proving Maschke's theorem, where the application was to the RG-module $\mathrm{Hom}_R(V,V)$. We will use this idea a second time in proving the orthogonality relations for characters.

(3.5) LEMMA. *Let V be an RG-module where R is a ring in which $|G|$ is invertible. Then*

$$\frac{1}{|G|}\sum_{g \in G} g : V \to V^G$$

is a map of RG-modules which is projection onto the fixed points of V. In particular, V^G is a direct summand of V as an RG-module. When R is a field of characteristic zero we have

$$\mathrm{tr}(\frac{1}{|G|}\sum_{g \in G} g) = \dim V^G.$$

Proof. Let $\pi : V \to V$ denote the map 'multiplication by $\frac{1}{|G|}\sum_{g \in G} g$'. We check that π is a linear map, and it commutes with the action of G since for $h \in G$ and $v \in V$ we

have

$$\begin{aligned}\pi(hv) &= (\frac{1}{|G|}\sum_{g\in G} gh)v \\ &= \pi(v) \\ &= (\frac{1}{|G|}\sum_{g\in G} hg)v \\ &= h\pi(v)\end{aligned}$$

since as g ranges through the elements of G so do gh and hg. The same equations show that every vector of the form $\pi(v)$ is fixed by G. Furthermore, if $v \in V^G$ then

$$\pi(v) = \frac{1}{|G|}\sum_{g\in G} gv = \frac{1}{|G|}\sum_{g\in G} v = v$$

so π is indeed projection onto V^G. □

There is one more ingredient we describe before stating the orthogonality relations for characters. We define an inner product on characters, but this does not make sense without some further explanation, because an inner product must be defined on a vector space and characters do not form a vector space. They are, however, elements in a vector space, namely the vector space of class functions on G.

A *class function* on G is a function $G \to \mathbb{C}$ which is constant on each conjugacy class of G. Such functions are in bijection with the functions from the set of conjugacy classes of G to $\mathbb{C}$, a set of functions which we may denote $\mathbb{C}^{\mathrm{cc}(G)}$ where $\mathrm{cc}(G)$ is the set of conjugacy classes of G. These functions become an algebra when we define addition, multiplication and scalar multiplication pointwise on the values of the function. In other words, $(\chi \cdot \psi)(g) = \chi(g)\psi(g)$, $(\chi + \psi)(g) = \chi(g) + \psi(g)$ and $(\lambda\chi)(g) = \lambda\chi(g)$ where χ, ψ are class functions and $\lambda \in \mathbb{C}$. If G has n conjugacy classes, this algebra is isomorphic to $\mathbb{C}^n$, the direct sum of n copies of $\mathbb{C}$, and is semisimple.

We define a Hermitian bilinear form on the complex vector space of class functions on G by means of the formula

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

As well as the usual identities which express bilinearity and the fact that the form is evidently Hermitian, it satisfies

$$\langle \chi\phi, \psi \rangle = \langle \chi, \phi^*\psi \rangle$$

where $\phi^*(g) = \overline{\phi(g)}$ is the class function obtained by complex conjugation. If χ and ψ happen to be characters of a representation we have $\overline{\chi(g)} = \chi(g^{-1})$, ψ^* is the character of

the contragredient representation, and we obtain further expressions for the bilinear form:

$$\begin{aligned}\langle \chi, \psi \rangle &= \frac{1}{|G|} \sum_{g \in G} \chi(g^{-1})\psi(g) \\ &= \frac{1}{|G|} \sum_{g \in G} \chi(g)\psi(g^{-1}) \\ &= \frac{1}{|G|} \sum_{g \in G} \chi(g)\overline{\psi(g)},\end{aligned}$$

where the second equality is obtained by observing that as g ranges over the elements of G, so does g^{-1}.

With all this preparation we can now state and prove the orthogonality relations for the rows of the character table. The picture will be completed once we have shown that the character table is square and deduced the orthogonality relations for columns in 3.16 and 3.17.

(3.6) THEOREM (Row Orthogonality relations).

(1) If χ is the character of a simple representation over $\mathbb{C}$ then $\langle \chi, \chi \rangle = 1$.

(2) If χ and ψ are the characters of non-isomorphic simple representations over $\mathbb{C}$ then $\langle \chi, \psi \rangle = 0$.

Proof. Suppose that V and W are simple complex representations affording characters χ and ψ. By 3.3 the character of $\mathrm{Hom}_{\mathbb{C}}(V, W)$ is $\overline{\chi} \cdot \psi$. By 3.4 and 3.5

$$\begin{aligned}\dim \mathrm{Hom}_{\mathbb{C}G}(V, W) &= \mathrm{tr}(\frac{1}{|G|} \sum_{g \in G} g) \text{ in its action on } \mathrm{Hom}_{\mathbb{C}}(V, W) \\ &= \frac{1}{|G|} \sum_{g \in G} \overline{\chi(g)}\psi(g) \\ &= \langle \chi, \psi \rangle.\end{aligned}$$

Schur's lemma asserts that this number is 1 if $V \cong W$, and 0 if $V \ncong W$. □

We will describe many consequences of the orthogonality relations, and the first is that they provide a way of determining the decomposition of a given representation as a direct sum of simple representations. This procedure is similar to the way of finding the coefficients in the Fourier expansion of a function using orthogonality of the functions $\sin(mx)$ and $\cos(nx)$.

(3.7) COROLLARY. *Let V be a $\mathbb{C}G$-module. In any expression*

$$V = S_1^{n_1} \oplus \cdots \oplus S_r^{n_r}$$

in which $S_1, \ldots, S_r$ are non-isomorphic simple modules, we have

$$n_i = \langle \chi_V, \chi_i \rangle$$

where χ_V is the character of V and χ_i is the character of S_i. In particular n_i is determined by V independently of the choice of decomposition.

(3.8) *Example.* Let $G = S_3$ and denote by $\mathbb{C}$ the trivial representation, ϵ the sign representation and V the 2-dimensional simple representation over $\mathbb{C}$. We decompose the 4-dimensional representation $V \otimes V$ as a direct sum of simple representations. Since the values of the character χ_V give the row of the character table

$$\chi_V : 2 \quad 0 \quad -1,$$

$V \otimes V$ has character values

$$\chi_{V\otimes V} : 4 \quad 0 \quad 1.$$

Thus

$$\langle \chi_{V\otimes V}, \chi_{\mathbb{C}} \rangle = \frac{1}{6}(4 \cdot 1 + 0 + 2 \cdot 1 \cdot 1) = 1$$
$$\langle \chi_{V\otimes V}, \chi_{\epsilon} \rangle = \frac{1}{6}(4 \cdot 1 + 0 + 2 \cdot 1 \cdot 1) = 1$$
$$\langle \chi_{V\otimes V}, \chi_{V} \rangle = \frac{1}{6}(4 \cdot 2 + 0 - 2 \cdot 1 \cdot 1) = 1$$

and we deduce that

$$V \otimes V \cong \mathbb{C} \oplus \epsilon \oplus V.$$

(3.9) COROLLARY. *For finite-dimensional complex representations V and W we have $V \cong W$ if and only if $\chi_V = \chi_W$.*

Proof. We saw in 3.1 that if V and W are isomorphic then they have the same character. Conversely, if they have the same character they both may be decomposed as a direct sum of simple representations by 1.7, and by 3.7 the multiplicities of the simples in these two decompositions must be the same. Hence the representations are isomorphic. □

The next result is a criterion for a representation to be simple. An important step in studying the representation theory of a group is to construct its character table, and one proceeds by compiling a list of the simple characters which at the end of the calculation will be complete. At any stage one has a partial list of simple characters, and considers some (potentially) new character. One finds the multiplicity of each previously obtained simple character as a summand of the new character, and subtracts off the these simple characters to the correct multiplicity. What is left is a character all of whose simple components are new simple characters. This character will itself be simple precisely if the following easily verified criterion is satisfied.

(3.10) COROLLARY. *If χ is the character of a complex representation V then $\langle \chi, \chi \rangle$ is a positive integer, and equals 1 if and only if V is simple.*

Proof. We may write $V \cong S_1^{n_1} \oplus \cdots \oplus S_r^{n_r}$ and then $\langle \chi, \chi \rangle = \sum_{i=1}^{r} n_i^2$ is a positive integer, which equals 1 precisely if one n_i is 1 and the others are 0. □

(3.11) *Example.* We construct the character table of S_4, since it illustrates some techniques in finding simple characters.

24	4	8	4	3
1	(12)	(12)(34)	(1234)	(123)
1	1	1	1	1
1	−1	1	−1	1
2	0	2	0	−1
3	−1	−1	1	0
3	1	−1	−1	0

TABLE: The character table of S_4.

Immediately above the horizontal line we list representatives of the conjugacy classes of elements of S_4, and above them the orders of their centralizers. The first row below the line is the character of the trivial representation, and below that is the character of the sign representation.

There is a homomorphism $\sigma : S_4 \to S_3$ specified by $(12) \mapsto (12)$, $(34) \mapsto (12)$, $(23) \mapsto (23)$, $(123) \mapsto (123)$ which has kernel the normal subgroup $\langle (12)(34), (13)(24) \rangle$. (One way to obtain this homomorphism is to identify S_4 as the group of rotations of a cube and observe that each rotation gives rise to a permutation of the three pairs of opposite faces.) Any representation $\rho : S_3 \to GL(V)$ gives rise to a representation $\rho\sigma$ of S_4 obtained by composition with σ, and if we start with a simple representation of S_3 we will obtain a simple representation of S_4 since σ is surjective and the invariant subspaces for ρ and $\rho\sigma$ are the same. Thus the simple characters of S_3 give a set of simple characters of S_4 obtained by applying σ and evaluating the character of S_3. This procedure, which in general works whenever one group is a homomorphic image of another, gives the trivial, sign and 2-dimensional representations of S_4.

There is an isomorphism between S_4 and the group of rotations of $\mathbb{R}^3$ which preserve a cube. One sees this from the fact that the group of such rotations permutes the four diagonals of the cube. This action is faithful and since every transposition of diagonals may be realized through some rotation, so can every permutation of the diagonals. Hence the full group of such rotations is isomorphic to S_4. The character of this action of S_4 on $\mathbb{R}^3$ is the fourth row of the character table. To compute the traces of the matrices which represent the different elements we do not actually have to work out what those matrices are, relying instead on the observation that every rotation of $\mathbb{R}^3$ has matrix conjugate to a matrix

$$\begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Thus, for example, (12) and (123) must act as rotations through π and $\frac{2\pi}{3}$, respectively, so act via matrices which are conjugates of

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad \text{and} \qquad \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} & 0 \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

which have traces -1 and 0.

There is an action of S_4 on $\mathbb{C}^4$ given by the permutation action of S_4 on four basis vectors. Since the trace of a permutation matrix equals the number of points fixed by the permutation, this has character

$$\chi: \quad 4 \quad 2 \quad 0 \quad 0 \quad 1$$

and we compute

$$\langle \chi, 1 \rangle = \frac{4}{24} + \frac{2}{4} + 0 + 0 + \frac{1}{3} = 1.$$

Thus $\chi = 1 + \psi$ where ψ is the character of a 3-dimensional representation:

$$\psi: \quad 3 \quad 1 \quad -1 \quad -1 \quad 0.$$

Again we have

$$\langle \psi, \psi \rangle = \frac{9}{24} + \frac{1}{4} + \frac{1}{8} + \frac{1}{4} + 0 = 1$$

so ψ is simple by 3.10, and this is the bottom row of the character table.

There are other ways to complete the calculation of the character table. Having computed four of the five rows, the fifth is determined by the facts that it is orthogonal to the other four, and that the sum of the squares of the degrees of the characters equals 24. Equally we could have constructed the bottom row as $\chi \otimes \epsilon$ where χ is the other character of degree 3 and ϵ is the sign character.

Our next immediate goal is to prove that the character table of a finite group is square, and to deduce the column orthogonality relations. Before doing this we show in the next two results how part of the column orthogonality relations may be derived in a direct way.

Consider the regular representation of G on $\mathbb{C}G$, and let $\chi_{\mathbb{C}G}$ denote the character of this representation.

(3.12) LEMMA.

$$\chi_{\mathbb{C}G}(g) = \begin{cases} |G| & \text{if } g = 1 \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Each $g \in G$ acts by the permutation matrix corresponding to the permutation $h \mapsto gh$. Now $\chi_{\mathbb{C}G}(g)$ equals the number of 1's down the diagonal of this matrix, which equals $|\{h \in G \mid gh = h\}|$. □

We may deduce an alternative proof of 2.5 (in case $k = \mathbb{C}$), and also a way to do the computation of the final row of the character table once the others have been determined.

(3.13) COROLLARY. *Let $\chi_1, \ldots, \chi_r$ be the simple complex characters of G, with degrees $d_1, \ldots, d_r$. Then $\langle \chi_{\mathbb{C}G}, \chi_i \rangle = d_i$, and hence*
(1) $\sum_{i=1}^{r} d_i^2 = |G|$, *and*
(2) $\sum_{i=1}^{r} d_i \chi_i(g) = 0$ *if* $g \neq 1$.

Proof. Direct evaluation gives

$$\langle \chi_{\mathbb{C}G}, \chi_i \rangle = \frac{1}{|G|} |G| \chi_i(1) = d_i$$

and hence $\chi_{\mathbb{C}G} = d_1\chi_1 + \cdots + d_r\chi_r$. Evaluating at 1 gives (1), and at $g \neq 1$ gives (2). □

It is an immediate deduction from the fact that the rows of the character table are orthogonal that the number of simple complex characters of a group is at most the number of conjugacy classes of elements in the group. We shall now prove that there is always equality here. For any ring A we denote by $Z(A)$ the *center* of A.

(3.14) LEMMA.
(1) For any ring R, $Z(M_n(R)) = \{\lambda I \mid \lambda \in R\} \cong R$.
(2) The number of simple complex characters of G equals $\dim Z(\mathbb{C}G)$.

Proof. (1) Let E_{ij} denote the matrix which is 1 in place i, j and 0 elsewhere. If $X = (x_{ij})$ is any matrix then

$$E_{ij}X = \text{the matrix with row } j \text{ of } X \text{ moved to row } i, \text{ 0 elsewhere,}$$
$$XE_{ij} = \text{the matrix with column } i \text{ of } X \text{ moved to column } j, \text{ 0 elsewhere.}$$

If $X \in Z(M_n(k))$ these two are equal, and we deduce that $x_{ii} = x_{jj}$ and all other entries in row j and column i are 0. Therefore $X = x_{11}I$.

(2) In 2.3 we constructed an isomorphism

$$\mathbb{C}G \cong M_{n_1}(\mathbb{C}) \oplus \cdots \oplus M_{n_r}(\mathbb{C})$$

where the matrix summands are in bijection with the isomorphism classes of simple modules. On taking centres, each matrix summand contributes 1 to $\dim Z(\mathbb{C}G)$. □

(3.15) LEMMA. *Let $x_1, \dots, x_t$ be representatives of the conjugacy classes of elements of G and let R be any ring. For each i let $\overline{x}_i \in RG$ denote the sum of the elements in the same conjugacy class as x_i. Then $Z(RG)$ is free as an R-module, with basis $\overline{x}_1, \dots, \overline{x}_t$.*

Proof. We first show that $\overline{x}_i \in Z(RG)$. Write $\overline{x}_i = \sum_{y \sim x_i} y$, where $\sim$ denotes conjugacy. Then

$$g\overline{x}_i = \sum_{y \sim x_i} gy = (\sum_{y \sim x_i} gyg^{-1})g = \overline{x}_i g$$

since as y runs through the elements of G conjugate to x_i, so does gyg^{-1}, and from this it follows that $\overline{x}_i$ is central.

Next suppose $\sum_{g \in G} a_g g \in Z(RG)$. We show that if $g_1 \sim g_2$ then $a_{g_1} = a_{g_2}$. Suppose that $g_2 = hg_1h^{-1}$. The coefficient of g_2 in $h(\sum_{g \in G} a_g g)h^{-1}$ is a_{g_1} and in $(\sum_{g \in G} a_g g)$ is a_{g_2}. Since elements of G are independent in RG, these coefficients must be equal. From this we see that every element of $Z(RG)$ can be expressed as an R-linear combination of the $\overline{x}_i$.

Finally we observe that the $\overline{x}_i$ are independent over R, since each is a sum of group elements with support disjoint from the supports of the other $\overline{x}_j$. □

(3.16) THEOREM. *The number of simple complex characters of G equals the number of conjugacy classes of elements of G.*

Proof. In 3.14 we showed that the number of simple characters equals the dimension of the centre, and 3.15 we showed that this is equal to the number of conjugacy classes. □

We conclude that the character table of a finite group is always square. From this we get orthogonality relations between the columns of the character table.

(3.17) COROLLARY (Column orthogonality relations). *Let X be the character table of G as a matrix, and let*

$$C = \begin{pmatrix} |C_G(x_1)| & 0 & \cdots & 0 \\ 0 & |C_G(x_2)| & & \\ \vdots & & \ddots & \vdots \\ 0 & & \cdots & |C_G(x_r)| \end{pmatrix}$$

where $x_1, \dots, x_r$ are representatives of the conjugacy classes of elements of G. Then

$$X^T \overline{X} = C,$$

where the bar denotes complex conjugation.

Proof. The orthogonality relations between the rows may be stated $\overline{X}C^{-1}X^T = I$. Since all these matrices are square, they are invertible, and in fact $(\overline{X}C^{-1})^{-1} = X^T = C\overline{X}^{-1}$. Therefore $X^T\overline{X} = C$. □

A less intimidating way to state the column orthogonality relations is

$$\sum_{i=1}^{r} \chi_i(g)\overline{\chi_i(h)} = \begin{cases} |C_G(g)| & \text{if } g \sim h, \\ 0 & \text{if } g \not\sim h. \end{cases}$$

The special case of this in which $g = 1$ has already been seen in Corollary 3.13.

We conclude this section on the properties of characters with the result which states that the degrees of the simple complex characters of a finite group G divide $|G|$. This is, of course, a big restriction on the possible degrees which may occur, and it is proved by means of an algebraic excursion which otherwise will not be used in the immediate development of the theory. This means that it is quite a good idea to skip the proof on first reading.

We need to use the notion of integrality. Suppose that S is a commutative ring with 1 and R is a subring of S with the same 1. An element $s \in S$ is said to be *integral* over R if $f(s) = 0$ for some monic polynomial $f \in R[X]$. Here, a *monic* polynomial is one in which the coefficient of the highest power of X is 1. We say that the ring S is integral over R if every element of S is integral over R. An element of $\mathbb{C}$ integral over $\mathbb{Z}$ is called an *algebraic integer*. We summarize the properties of integers which we will need.

(3.18) THEOREM. *Let R be a subring of a commutative ring S.*

(1) The following are equivalent for an element $s \in S$:
  (a) s is integral over R,
  (b) $R[s]$ is contained in some finitely generated R-submodule M of S such that $sM \subseteq M$.

(2) The elements of S integral over R form a subring of S.

(3) $\{x \in \mathbb{Q} \mid x \text{ is integral over } \mathbb{Z}\} = \mathbb{Z}$.

(4) Let g be any element of a finite group G and χ any character of G. Then $\chi(g)$ is an algebraic integer.

In the statement of this result, $R[s]$ denotes the subring of S generated by R and s.

Proof. (1) (a) $\Rightarrow$ (b). Suppose s is an element integral over R, satisfying the equation

$$s^n + a_{n-1}s^{n-1} + \cdots + a_1 s + a_0 = 0$$

where $a_i \in R$. Then $R[s]$ is generated as an R-module by $1, s, s^2, \ldots, s^{n-1}$. This is because the R-span of these elements is also closed under multiplication by s, using the fact that

$$s \cdot s^{n-1} = -a_{n-1}s^{n-1} - \cdots - a_1 s - a_0.$$

Thus we may take $M = R[s]$.

(b) $\Rightarrow$ (a). Suppose $R[s] \subseteq M = Rx_1 + \cdots Rx_n$ with $sM \subseteq M$. Thus for each i we have $sx_i = \sum_{j=1}^{n} \lambda_{ij}x_j$ for certain $\lambda_{ij} \in R$. Consider the $n \times n$ matrix $A = sI - (\lambda_{ij})$ with entries in S, where I is the identity matrix. We have $Ax = 0$ where x is the vector

$(x_1, \ldots, x_n)^T$, and so $\mathrm{adj}(A)Ax = 0$ where $\mathrm{adj}(A)$ is the adjugate matrix of A satisfying $\mathrm{adj}(A)A = \det(A) \cdot I$. Hence $\det(A) \cdot x_i = 0$ for all i. Since $1 \in R \subseteq M$ is a linear combination of the x_i we have $\det(A) = 0$ and so s is a root of the monic polynomial $\det(X \cdot I - (\lambda_{ij}))$.

(2) We show that if $a, b \in S$ are integral over R then $a + b$ and ab are also integral over R. These lie in $R[a, b]$, and we show that this is finitely generated as an R-module. We see from the proof of part (1) that each of $R[a]$ and $R[b]$ is finitely generated as an R-module. If $R[a]$ is generated by $x_1, \ldots, x_m$ and $R[b]$ is generated by $y_1, \ldots, y_n$, then $R[a, b]$ is evidently generated as an R-module by all the products $x_i y_j$. Now $R[a, b]$ also satisfies the remaining condition of part (b) of (1), and we deduce that $a + b$ and ab are integral over R.

(3) Suppose that $\frac{a}{b}$ is integral over $\mathbb{Z}$, where a, b are coprime integers. Then

$$\left(\frac{a}{b}\right)^n + c_{n-1}\left(\frac{a}{b}\right)^{n-1} + \cdots + c_1\frac{a}{b} + c_0 = 0$$

for certain integers c_i, and so

$$a^n + c_{n-1}a^{n-1}b + \cdots + c_1 ab^{n-1} + c_0 b^n = 0.$$

Since b divides all terms in this equation except perhaps the term a^n, b must also be a factor of a^n. Since a and b are coprime, this is only possible if $b = \pm 1$, and we deduce that $\frac{a}{b} \in \mathbb{Z}$.

(4) $\chi(g)$ is the sum of the eigenvalues of g in its action on the representation which affords χ. Since $g^n = 1$ for some n these eigenvalues are all roots of $X^n - 1$ and so are integers. □

(3.19) PROPOSITION. *The centre $Z(\mathbb{Z}G)$ is integral over $\mathbb{Z}$. Hence if $x_1, \ldots, x_r$ are representatives of the conjugacy classes of G, $\overline{x}_i \in \mathbb{Z}G$ is the sum of the elements conjugate to x_i, and $\lambda_1, \ldots, \lambda_r \in \mathbb{C}$ are algebraic integers then $\sum_{i=1}^r \lambda_i \overline{x}_i$ is integral over $\mathbb{Z}$.*

Proof. In the statement of this result we are identifying $\mathbb{Z}$ with the scalar multiples of the identity $\mathbb{Z} \cdot 1 \subseteq Z(\mathbb{Z}G)$. We also regard $\mathbb{Z}G$ as a subset of $\mathbb{C}G$ when we form the linear combination $\sum_{i=1}^r \lambda_i \overline{x}_i$.

It is the case that every commutative subring of $\mathbb{Z}G$ is integral over $\mathbb{Z}$, using condition 1(b) of 3.18, since such a subring is in particular a subgroup of the finitely-generated free abelian group $\mathbb{Z}G$, and hence is finitely generated as a $\mathbb{Z}$-module.

We have seen in 3.15 that the elements $\overline{x}_1, \ldots, \overline{x}_r$ lie in $Z(\mathbb{Z}G)$, so they are integral over $\mathbb{Z}$, and by part (2) of 3.18 the linear combination $\sum_{i=1}^r \lambda_i \overline{x}_i$ is integral also. (We note that the $\overline{x}_i$ are in fact a finite set of generators for $Z(\mathbb{Z}G)$ as an abelian group, but we did not need to know this for the proof.) □

Let $\rho_1, \ldots, \rho_r$ be the simple representations of G over $\mathbb{C}$ with degrees $d_1, \ldots, d_r$ and characters $\chi_1, \ldots, \chi_r$. Then each $\rho_i : G \to M_{d_i}(\mathbb{C})$ extends by linearity to a $\mathbb{C}$-algebra homomorphism

$$\rho_i : \mathbb{C}G = \bigoplus_{i=1}^{r} M_{d_i}(\mathbb{C}) \to M_{d_i}(\mathbb{C})$$

projecting onto the ith matrix summand. The fact that the group homomorphism ρ_i extends to an algebra homomorphism in this way comes formally from the construction of the group algebra. The fact that this algebra homomorphism is projection onto the ith summand arises from the way we decomposed $\mathbb{C}G$ as a sum of matrix algebras, in which each matrix summand acts on the corresponding simple module as matrices on the space of column vectors.

(3.20) PROPOSITION. *If $x \in Z(\mathbb{C}G)$ then $\rho_i(x) = \lambda I$ for some $\lambda \in \mathbb{C}$. In fact*

$$\rho_i(x) = \frac{1}{d_i} \cdot \textit{trace of } \rho_i(x) \cdot I.$$

Writing $x = \sum_{g \in G} a_g g$ we have

$$\rho_i(x) = \frac{1}{d_i} \sum_{g \in G} a_g \chi_i(g) \cdot I.$$

Proof. Since x is central the matrix $\rho_i(x)$ commutes with the matrices $\rho_i(g)$ for all $g \in G$. Therefore by Schur's lemma, since ρ_i is a simple complex representation, $\rho_i(x) = \lambda I$, some scalar multiple of the identity matrix. Evidently $\lambda = \frac{1}{d_i} \operatorname{tr}(\lambda I)$. Substituting into this expression we obtain

$$\begin{aligned} \frac{1}{d_i} \operatorname{tr}(\rho_i(\sum_{g \in G} a_g g)) &= \frac{1}{d_i} \sum_{g \in G} a_g \operatorname{tr}(\rho_i(g)) \\ &= \frac{1}{d_i} \sum_{g \in G} a_g \chi_i(g). \end{aligned}$$

□

(3.21) THEOREM. *The degrees d_i of the simple complex representations of G all divide $|G|$.*

Proof. Let $x = \sum_{g \in G} \chi_i(g^{-1}) g$. This element is central in $\mathbb{C}G$ since the coefficients of group elements are constant on conjugacy classes. By 3.20

$$\begin{aligned} \rho_i(x) &= \frac{1}{d_i} \sum_{g \in G} \chi_i(g^{-1}) \chi_i(g) \cdot I \\ &= \frac{|G|}{d_i} \cdot I \end{aligned}$$

the second equality arising from the fact that $\langle \chi_i, \chi_i \rangle = 1$. Now x is integral over $\mathbb{Z} \cdot 1$ so $\rho_i(x)$ is integral over $\rho_i(\mathbb{Z} \cdot 1) = \mathbb{Z} \cdot I$. Thus $\frac{|G|}{d_i}$ is integral over $\mathbb{Z}$, hence $\frac{|G|}{d_i} \in \mathbb{Z}$ so $d_i \mid |G|$. □

At this point we may very quickly deduce a formula for the central primitive idempotent elements in $\mathbb{C}G$. We use some of the same ideas that arose in proving Theorem 3.21 and for that reason we present this further application here. However, the formula has no immediate use in this text and can be omitted without loss of understanding at this point. We start with some generalities about central primitive idempotent elements.

An element e of an algebra A is said to be *idempotent* if $e^2 = e$, and we say it is a *central idempotent element* if it lies in the centre $Z(A)$. Two idempotent elements e and f are *orthogonal* if $ef = fe = 0$. An idempotent element e is called *primitive* if whenever $e = e_1 + e_2$ where e_1 and e_2 are orthogonal idempotent elements then either $e_1 = 0$ or $e_2 = 0$. We say that e is a *primitive central idempotent element* if it is primitive as an idempotent element in $Z(A)$, that is, e is central and has no proper decomposition as a sum of orthogonal central idempotent elements. Some properties of idempotent elements relating to these definitions are described in the exercises to Section 2.

Given a set of rings with identity $A_1, \ldots, A_r$ we may form their direct sum $A = A_1 \oplus \cdots \oplus A_r$ which acquires the structure of a ring with componentwise addition and multiplication. In this situation each ring A_i may be identified as the subset of A consisting of elements which are zero except in component i, but this subset is not a subring of A because it does not contain the identity element of A. It is, however, a 2-sided ideal. Equally, in any decomposition of a ring A as a direct sum of 2-sided ideals, these ideals have the structure of rings with identity.

(3.22) PROPOSITION. *Let A be a ring with identity. Decompositions*

$$A = A_1 \oplus \cdots \oplus A_r$$

as direct sums of 2-sided ideals A_i biject with expressions

$$1 = e_1 + \cdots + e_r$$

as a sum of orthogonal central idempotent elements, where e_i is the identity element of A_i and $A_i = Ae_i$. The A_i are indecomposable as rings if and only if the e_i are primitive central idempotent elements. If every A_i is indecomposable as a ring then the A_i, and also the primitive central idempotents e_i, are uniquely determined as subsets of A, and every central idempotent can be written as a sum of certain of the e_i.

Proof. Given any ring decomposition $A = A_1 \oplus \cdots \oplus A_r$ we may write $1 = e_1 + \cdots + e_r$ where $e_i \in A_i$ and now it is clear that the e_i are orthogonal central idempotent elements. Conversely, given an expression $1 = e_1 + \cdots + e_r$ where the e_i are orthogonal central idempotent elements we have $A = Ae_1 \oplus \cdots \oplus Ae_r$ as rings.

To say that the ring A_i is indecomposable means that it cannot be expressed as a direct sum of rings, except in the trivial way, and evidently this happens precisely if the corresponding idempotent element cannot be decomposed as a sum of orthogonal central idempotent elements.

What is perhaps surprising is that there is at most one decomposition of A as a sum of indecomposable rings. Suppose we have two such decompositions, and that the corresponding primitive central idempotent elements are labelled e_i and f_j, so that

$$1 = e_1 + \cdots + e_r = f_1 + \cdots + f_s.$$

We have

$$e_i = e_i \cdot 1 = \sum_{j=1}^{s} e_i f_j,$$

and so $e_i = e_i f_j$ for some unique j and $e_i f_k = 0$ if $k \neq j$, by primitivity of e_i. Also

$$f_j = 1 \cdot f_j = \sum_{k=1}^{r} e_k f_j$$

so that $e_k f_j \neq 0$ for some unique k. Since $e_i f_j \neq 0$ we have $k = i$ and $e_i f_j = f_j$. Thus $e_i = f_j$. We proceed by induction on r, starting at $r = 1$. If $r > 1$ we now work with the ring $A \cdot \sum_{k \neq i} e_k = A \cdot \sum_{k \neq j} f_k$ in which the identity is expressible as sums of primitive central idempotent elements $\sum_{k \neq i} e_k = \sum_{k \neq j} f_k$. The first of these expressions has $r - 1$ terms, so by induction the e_k's are the same as the f_k's after some permutation.

If e is any central idempotent and the e_i are primitive then ee_i is either e_i or 0 since $e = ee_i + e(1 - e_i)$ is a sum of orthogonal central idempotents. Thus

$$e = e \sum_{k=1}^{r} e_i = \sum_{k=1}^{r} ee_i$$

is a sum of certain of the e_i. □

In view of the last result when we speak of the primitive central idempotent elements of an algebra we are referring to the set which determines the unique decomposition of the algebra as a direct sum of indecomposable rings.

(3.23) THEOREM. *Let $\chi_1, \ldots, \chi_r$ be the simple complex characters of G with degrees $d_1, \ldots, d_r$. The primitive central idempotent elements in $\mathbb{C}G$ are the elements*

$$\frac{d_i}{|G|} \sum_{g \in G} \chi_i(g^{-1}) g$$

where $1 \leq i \leq r$, the corresponding indecomposable ring summand of $\mathbb{C}G$ having a simple representation which affords the character χ_i.

Proof. Using the notation of 3.20 we have that the representation ρ_i which affords χ_i yields an algebra map $\rho_i : \mathbb{C}G \to M_{d_i}(\mathbb{C})$ which is projection onto the ith matrix summand in a decomposition of $\mathbb{C}G$ as a sum of matrix rings. For any field k the matrix ring $M_n(k)$ is indecomposable, since we have seen in 3.14 that $Z(M_n(k)) \cong k$ and the only non-zero idempotent element in a field is 1. Thus the decomposition of $\mathbb{C}G$ as a direct sum of matrix rings is the unique decomposition of $\mathbb{C}G$ as a sum of indecomposable ring summands. The corresponding primitive central idempotent elements are the identity matrices in the various summands, and so they are the elements $e_i \in \mathbb{C}G$ such that $\rho_i(e_i) = I$ and $\rho_j(e_i) = 0$ if $i \neq j$. From the formula of 3.20 and the orthogonality relations we have

$$\begin{aligned}
\rho_j\left(\frac{d_i}{|G|}\sum_{g\in G}\chi_i(g^{-1})g\right) &= \frac{d_i}{|G|d_j}\sum_{g\in G}\chi_i(g^{-1})\chi_j(g)\cdot I \\
&= \frac{d_i}{d_j}\langle\chi_i,\chi_j\rangle\cdot I \\
&= \frac{d_i}{d_j}\delta_{i,j}\cdot I \\
&= \delta_{i,j}\cdot I,
\end{aligned}$$

so that the elements specified in the statement of the theorem do indeed project correctly onto the identity matrices, and are therefore the primitive central idempotent elements. □

While the identity matrix is a primitive *central* idempotent element in the matrix ring $M_n(k)$, where k is a field, it is never a primitive idempotent element if $n > 1$ since it is the sum of the orthogonal (non-central) primitive idempotent elements $I = E_{1,1} + \cdots + E_{n,n}$. Furthermore, removing the hypothesis of centrality we can no longer say that decompositions of the identity as a sum of primitive idempotent elements are unique; indeed, any conjugate expression by an invertible matrix will also be a sum of orthogonal primitive idempotent elements. Applying these comments to a matrix summand of $\mathbb{C}G$, the primitive idempotent decompositions of 1 will never be unique if we have a non-abelian matrix summand — which, of course, happens precisely when G is non-abelian. It is unfortunately the case that in terms of the group elements there is in general no known formula for primitive idempotent elements of $\mathbb{C}G$ lying in a non-abelian matrix summand.

We conclude this section with Burnside's remarkable 'p^aq^b theorem', which establishes a group-theoretic result using the ideas of representation theory we have so far developed, together with some admirable ingenuity. In the course of the proof we again make use of the idea of integrality, but this time we also require Galois theory at one point. This is needed to show that if ζ is a field element which is expressible as a sum of roots of unity,

then every algebraic conjugate of ζ is again expressible as a sum of roots of unity. We present Burnside's theorem here because of its importance as a theorem in its own right, not because anything later depends on it. In view of this the proof (which is fairly long) can be omitted without subsequent loss of understanding.

Recall that a group G is *soluble* if it has a composition series in which all of the composition factors are cyclic. Thus a group is not soluble precisely if it has a non-abelian composition factor.

(3.24) THEOREM (Burnside's p^aq^b theorem). *Let G be a group of order p^aq^b where p and q are primes. Then G is soluble.*

Proof. We suppose the result is false, and consider a group G of minimal order subject to being not soluble and of order p^aq^b.

Step 1. The group G is simple, not abelian and not of prime-power order; for if it were abelian or of prime-power order it would be soluble, and if G had a normal subgroup N then one of N and G/N would be a smaller group of order $p^\alpha q^\beta$ which was not soluble.

Step 2. We show that G contains an element g whose conjugacy class has size q^d for some $d > 0$. Let P be a Sylow p-subgroup, $1 \neq g \in Z(P)$. Then $C_G(g) \supseteq P$ so $|G : C_G(g)| = q^d$ for some $d > 0$, and this is the number of conjugates of g.

Step 3. We show that there is a simple non-identity character χ of G such that $q \not| \chi(1)$ and $\chi(g) \neq 0$. To prove this, suppose to the contrary that whenever $\chi \neq 1$ and $q \not| \chi(1)$ then $\chi(g) = 0$. Let R denote the ring of algebraic integers in $\mathbb{C}$. Consider the orthogonality relation between the column of 1 (consisting of character degrees) and the column of g:

$$1 + \sum_{\chi \neq 1} \chi(1)\chi(g) = 0.$$

Then q divides every term apart from 1 in the sum on the left, and so $1 \in qR$. Thus $q^{-1} \in R$. But $q^{-1} \in \mathbb{Q}$ and so $q^{-1} \in \mathbb{Z}$ by 3.18, a contradiction. We now fix a non-identity character χ for which $q \not| \chi(1)$ and $\chi(g) \neq 0$.

Step 4. Recall that the number of conjugates of g is q^d. We show that

$$\frac{q^d\chi(g)}{\chi(1)}$$

is an algebraic integer. To do this we use results 3.15 and 3.20. These imply that if $\overline{g} = \sum_{h \sim g} h \in \mathbb{C}G$ is the sum of the elements conjugate to g and ρ is a representation affording the character χ then $\overline{g} \in Z(\mathbb{C}G)$ and

$$\begin{aligned}\rho(\overline{g}) &= \frac{1}{\chi(1)} \sum_{h \sim g} \chi(h) \cdot I \\ &= \frac{q^d\chi(g)}{\chi(1)} \cdot I,\end{aligned}$$

where I is the identity matrix. Now by 3.19 this is integral over $\rho(\mathbb{Z}) = \mathbb{Z} \cdot I$, which proves what we want.

Step 5. We deduce that $\frac{\chi(g)}{\chi(1)}$ is an algebraic integer. This arises from the fact that $q \not| \chi(1)$. We can find $\lambda, \mu \in \mathbb{Z}$ so that $\lambda q^d + \mu\chi(1) = 1$. Now

$$\frac{\chi(g)}{\chi(1)} = \lambda \frac{q^d \chi(g)}{\chi(1)} + \mu\chi(g)$$

is a sum of algebraic integers.

Step 6. We show that $|\chi(g)| = \chi(1)$ and put $\zeta = \chi(g)/\chi(1)$. We consider the algebraic conjugates of ζ, which are the roots of the minimal polynomial of ζ over $\mathbb{Q}$. They are all algebraic integers, since ζ and its algebraic conjugates are all roots of the same polynomials over $\mathbb{Q}$. Thus the product $N(\zeta)$ of the algebraic conjugates is an algebraic integer. Since it is also $\pm$ the constant term of the minimal polynomial of ζ, it is rational and non-zero. Therefore $0 \neq N(\zeta) \in \mathbb{Z}$ by 3.18.

Now $\chi(g)$ is the sum of the eigenvalues of $\chi(g)$, of which there are $\chi(1)$, each of which is a root of unity. Hence by the triangle inequality, $|\chi(g)| \leq \chi(1)$. By Galois theory the same is true and a similar inequality holds for each algebraic conjugate of $\chi(g)$. We conclude that all algebraic conjugates of ζ have absolute value at most 1. Therefore $|N(\zeta)| \leq 1$. The only possibility is $|N(\zeta)| = 1$ and $|\zeta| = 1$.

Step 7. We deduce that G has a proper normal subgroup by considering

$$H = \{h \in G \mid |\chi(h)| = \chi(1)\}$$

where χ is the simple non-identity character introduced in Step 3. We argue first that H is a normal subgroup. If the eigenvalues of $\rho(h)$ are $\lambda_1, \ldots, \lambda_n$ then, since these are roots of unity, $|\lambda_1 + \cdots + \lambda_n| = n$ if and only if $\lambda_1 = \cdots = \lambda_n$. Thus $|\chi(h)| = \chi(1)$ if and only if $\rho(h)$ is multiplication by some scalar, and from this we see immediately that H is a normal subgroup. It also implies that $H/\operatorname{Ker}\rho$ is abelian. From Step 6 we see that $|H/\operatorname{Ker}\rho| > 1$, but this forces a contradiction since simplicity of G implies that $H = G$ and $\operatorname{Ker}\rho = 1$, from which we deduce that G is abelian. This contradiction terminates the proof. □

Exercises for Section 3.

1. Suppose that V is a representation of G over $\mathbb{C}$ for which $\chi_V(g) = 0$ if $g \neq 1$. Show that $\dim V$ is a multiple of $|G|$. Deduce that $V \cong \mathbb{C}G^n$ for some n. Show that if W is any representation of G over $\mathbb{C}$ then $\mathbb{C}G \otimes_{\mathbb{C}} W \cong \mathbb{C}G^{\dim W}$ as $\mathbb{C}G$-modules.

2. (a) By using characters show that if V and W are any $\mathbb{C}G$-modules then $(V \otimes_{\mathbb{C}} W)^* \cong V^* \otimes_{\mathbb{C}} W^*$, and $({}_{\mathbb{C}G}\mathbb{C}G)^* \cong {}_{\mathbb{C}G}\mathbb{C}G$.

(b) If k is any field and V, W are kG-modules, show that $(V \otimes_k W)^* \cong V^* \otimes_k W^*$, and $({}_{kG}kG)^* \cong {}_{kG}kG$.

3. Consider a ring with identity which is the direct sum (as a ring) of subrings $A = A_1 \oplus \cdots \oplus A_r$. Suppose that A has exactly n isomorphism types of simple modules. Show that $r \leq n$.

4. Let g be any non-identity element of a group G. Show that G has a simple complex character χ for which $\chi(g)$ has negative real part.

5. Show that if every element of a finite group G is conjugate to its inverse, then every character on G is real-valued.

Conversely, show that if every character on G is real-valued, then every element of G is conjugate to its inverse.

[Note here that the quaternion group of order 8 in its action on the algebra of quaternions provides an example of a complex representation which is not equivalent to a real representation, but whose character is real-valued. In this example, the representation has complex dimension 2, but there is no basis over $\mathbb{C}$ for the representation space such that the group acts by matrices with real entries.]

6. (Jozsef Pelikan) While walking down the street you find a scrap of paper with the following character table on it:

$$\begin{array}{ccccc} \hline & 1 & & 1 & \\ & 1 & & -1 & \\ \cdots & 2 & \cdots & -1 & \cdots \\ & 3 & & 1 & \\ & 3 & & -1 & \\ \hline \end{array}$$

All except two of the columns are obscured, and while it is clear that there are five rows you cannot read anything of the other columns, including their position. Prove that there is an error in the table. Given that there is exactly *one* error, determine where it is, and what the correct entry should be.

7. A finite group has seven conjugacy classes with representatives $c_1, \ldots, c_7$ (where $c_1 = 1$), and the values of five of its irreducible characters are given by the following table:

c_1	c_2	c_3	c_4	c_5	c_6	c_7
1	1	1	1	1	1	1
1	1	1	1	−1	−1	−1
4	1	−1	0	2	−1	0
4	1	−1	0	−2	1	0
5	−1	0	1	1	1	−1

Calculate the numbers of elements in the various conjugacy classes and the remaining simple characters.

8. Let $g \in G$. Prove that g lies in the centre of G if and only if $|\chi(g)| = |\chi(1)|$ for every simple complex character χ of G.

9. Here is a column of a character table:

g
1
-1
0
-1
-1
$\frac{-1+i\sqrt{11}}{2}$
$\frac{-1-i\sqrt{11}}{2}$
0
1
0

(a) Find the order of g.
(b) Prove that $g \notin Z(G)$.
(c) Show that there exists an element $h \in G$ with the same order as g but not conjugate to g.
(d) Show that there exist two distinct simple characters of G of the same degree.

4. The Construction of Modules and Characters

We start with the particular case of cyclic groups over $\mathbb{C}$.

(4.1) PROPOSITION. *Let $G = \langle x \mid x^n = 1 \rangle$ be a cyclic group of order n, and let $\zeta \in \mathbb{C}$ be a primitive nth root of unity. Then the simple complex characters of G are the n functions*

$$\chi_r(x^s) = \zeta^{rs}$$

where $0 \leq r \leq n-1$.

Proof. We merely observe that the mapping

$$x^s \mapsto \zeta^{rs}$$

is a group homomorphism

$$G \to GL(1, \mathbb{C}) = \mathbb{C}^*$$

giving a 1-dimensional representation with character χ_r, which must necessarily be simple. These characters are all distinct, and since the number of them equals the group order we have them all. □

We next show how to obtain the simple characters of a product of groups in terms of the characters of the groups in the product. Combining this with the last result we obtain the character table of any finite abelian group. We describe a construction which works over any ring R. Suppose that $\rho_1 : G_1 \to GL(V_1)$ and $\rho_2 : G_2 \to GL(V_2)$ are representations of groups G_1 and G_2. We may define an action of $G_1 \times G_2$ on $V_1 \otimes_R V_2$ by the formula

$$(g_1, g_2)(v_1 \otimes v_2) = g_1 v_1 \otimes g_2 v_2$$

where $g_i \in G_i$ and $v_i \in V_i$. When R is a field we may choose bases for V_1 and V_2, and now (g_1, g_2) acts via the tensor product of the matrices by which g_1 and g_2 act. It follows when $R = \mathbb{C}$ that

$$\chi_{V_1 \otimes V_2}(g_1, g_2) = \chi_{V_1}(g_1)\chi_{V_1}(g_1).$$

(4.2) THEOREM. *Let $V_1, \ldots, V_m$ and $W_1, \ldots, W_n$ be complete lists of the simple complex representations of groups G_1 and G_2. Then the representations $V_i \otimes W_j$ with $1 \leq i \leq n$ and $1 \leq j \leq m$ form a complete list of the simple complex $G_1 \times G_2$ representations.*

Remark. The statement of this theorem actually works over an arbitrary field, which need not be $\mathbb{C}$. There is a still more general statement to do with representations of finite-dimensional algebras A and B over a field k, which is that the simple representations of $A \otimes_k B$ are precisely the $S \otimes_k T$, where S is a simple A-module and T is a simple B-module. The connection with groups is that the group algebra $R[G_1 \times G_2]$ over any commutative

ring R is isomorphic to $RG_1 \otimes_R RG_2$, which we may see by observing that the basis of $RG_1 \otimes_R RG_2$ consisting of elements $g_1 \otimes g_2$ with $g_i \in G_i$ multiplies the same way as the group $G_1 \times G_2$.

Proof. We first verify that the representations $V_i \otimes W_j$ are simple using the criterion of 3.10:

$$\begin{aligned}\langle \chi_{V_i\otimes W_j}, \chi_{V_i\otimes W_j}\rangle &= \frac{1}{|G_1\times G_2|}\sum_{(g_1,g_2)\in G_1\times G_2} \overline{\chi_{V_i\otimes W_j}(g_1,g_2)}\chi_{V_i\otimes W_j}(g_1,g_2)\\ &= \frac{1}{|G_1||G_2|}\sum_{(g_1,g_2)\in G_1\times G_2} \overline{\chi_{V_1}(g_1)}\chi_{V_1}(g_1)\overline{\chi_{V_2}(g_2)}\chi_{V_2}(g_2)\\ &= \frac{1}{|G_1|}\sum_{g_1\in G_1}\overline{\chi_{V_1}(g_1)}\chi_{V_1}(g_1)\cdot\frac{1}{|G_2|}\sum_{g_2\in G_2}\overline{\chi_{V_2}(g_2)}\chi_{V_2}(g_2)\\ &= 1.\end{aligned}$$

The characters of these representations are distinct, since by a similar calculation if $(i,j)\neq(r,s)$ then $\langle \chi_{V_i\otimes W_j}, \chi_{V_r\otimes W_s}\rangle = 0$. To show that we have the complete list, we observe that if $\dim V_i = d_i$ and $\dim W_j = e_j$ then $V_i \otimes W_j$ is a representation of degree d_ie_j and

$$\sum_{i=1}^{m}\sum_{j=1}^{n}(d_ie_j)^2 = \sum_{i=1}^{m} d_i^2 \cdot \sum_{j=1}^{n} e_j^2 = 1.$$

This establishes what we need, using 2.5 or 3.13. □

Putting the last two results together enables us to compute the character table of any finite abelian group. To give a very small example, let

$$G = \langle x, y \mid x^2 = y^2 = [x,y] = 1\rangle \cong C_2 \times C_2.$$

The character tables of $\langle x\rangle$ and $\langle y\rangle$ are

	2	2
	1	x
χ_1	1	1
χ_2	1	-1

	2	2
	1	y
ψ_1	1	1
ψ_2	1	-1

TABLE: Two copies of the character table of C_2.

and the character table of $C_2 \times C_2$ is

	4	4	4	4
	1	x	y	xy
$\chi_1\psi_1$	1	1	1	1
$\chi_2\psi_1$	1	-1	1	-1
$\chi_1\psi_2$	1	1	-1	-1
$\chi_2\psi_2$	1	-1	-1	1

TABLE: The character table of $C_2 \times C_2$.

We immediately notice that this construction gives the character table of $C_2 \times C_2$ as the tensor product of the character tables of C_2 and C_2, and without further argument we see that this is true in general.

(4.3) COROLLARY. *The character table of a direct product $G_1 \times G_2$ is the tensor product of the character tables of G_1 and G_2.*

We see from this that all simple complex characters of an abelian group have degree 1, and in fact this property characterizes abelian groups.

(4.4) THEOREM. *The following are equivalent for a finite group G:*
(1) G is abelian,
(2) all simple complex representations of G have degree 1.

Proof. Since the simple representations of every finite cyclic group all have degree 1, and since every finite abelian group is a direct product of cyclic groups, the last result shows that all simple representations of a finite abelian group have degree 1.

Conversely, we may use the fact that $|G| = \sum_{i=1}^{r} d_i^2$ where $d_1, \ldots, d_r$ are the degrees of the simple representations. We deduce that $d_i = 1$ for all $i \Leftrightarrow r = |G| \Leftrightarrow$ every conjugacy class has size $1 \Leftrightarrow$ every element is central $\Leftrightarrow G$ is abelian.

Another proof of this result may be obtained from the fact that $\mathbb{C}G$ is a direct sum of matrix algebras over $\mathbb{C}$, a summand $M_n(\mathbb{C})$ appearing precisely if there is a simple module of dimension n. The group and hence the group ring are abelian if and only if n is always 1. □

We may construct the part of the character table of any finite group which consists of characters of degree 1 by combining the previus results with the next one.

(4.5) PROPOSITION. *The degree 1 representations of any finite group G over any field are precisely the degree 1 representations of G/G', lifted to G via the homomorphism $G \to G/G'$.*

Proof. We only have to observe that a degree 1 representation of G over a field k is a homomorphism $G \to GL(1,k) = k^\times$ which takes values in an abelian group, and so has kernel containing G'. Thus such a homomorphism is always a composite $G \to G/G' \to GL(1,k)$ obtained from a degree 1 representation of G/G'. □

(4.6) *Example.* Neither implication of 4.4 holds if we do not assume that our representations are defined over $\mathbb{C}$ (or more generally, an algebraically closed field in characteristic prime to $|G|$). Over $\mathbb{R}$ the cyclic group $\langle x \mid x^3 = 1 \rangle$ of order 3 has a 2-dimensional representation in which x acts as rotation through $\frac{2\pi}{3}$. This representation is simple since there is no 1-dimensional subspace stable under the group action. We need to pass to $\mathbb{C}$ to split it as a sum of two representations of degree 1. This is an example of an abelian group not all of whose simple representations have degree 1, and equally one may find a non-abelian group all of whose simple representations do have degree 1. As we shall see later, this happens whenever G is a p-group and we consider representations in characteristic p.

Induction and Restriction

We now consider an extremely important way of constructing representations of a group from representations of its subgroups. Let H be a subgroup of G and V an RH-module where R is a commutative ring with 1. We define an RG-module

$$V \uparrow_H^G = RG \otimes_{RH} V$$

with the action of G coming from the left module action on RG:

$$x \cdot (\sum_{g \in G} a_g g \otimes v) = (x \sum_{g \in G} a_g g) \otimes v$$

where $x, g \in G$, $a_g \in R$ and $v \in V$. We refer to this module as V *induced* from H to G, and say that $V \uparrow_H^G$ is an induced module. In many books the notation V^G is used for this induced module, but for us this conflicts with the notation for fixed points.

We denote the set of left cosets $\{gH \mid g \in G\}$ by G/H.

(4.7) PROPOSITION. *Let V be an RH-module and let $g_1H, \ldots, g_{|G:H|}H$ be a list of the left cosets G/H. Then*

$$V \uparrow_H^G = \bigoplus_{i=1}^{|G:H|} g_i \otimes V$$

as R-modules, where $g_i \otimes V = \{g_i \otimes v \mid v \in V\} \subseteq RG \otimes_{RH} V$. Each $g_i \otimes V$ is isomorphic to V as an R-module, and in case V is free as an R-module we have

$$\operatorname{rank}_R V \uparrow_H^G = |G : H| \operatorname{rank}_R V.$$

If $x \in G$ then $x(g_i \otimes V) = g_j \otimes V$ where $xg_i = g_j h$ for some $h \in H$. Thus the R-submodules $g_i \otimes V$ of $V \uparrow_H^G$ are permuted under the action of G. This action is transitive, and if $g_1 \in H$ then $\operatorname{Stab}_G(g_1 \otimes V) = H$.

Proof. We have $RG_{RH} = \bigoplus_{i=1}^{|G:H|} g_i RH \cong RH^{|G:H|}$ as right RH-modules, since H has a permutation action on the basis of RG with $|G : H|$ orbits $g_1H, \ldots, g_{|G:H|}H$, and each orbit spans a right RH-submodule $R[g_iH]$ of RG, which is isomorphic to RH_{RH} as right RH-modules via the isomorphism specified by $g_ih \mapsto h$, where $h \in H$. Now

$$\begin{aligned} RG \otimes_{RH} V &= (\bigoplus_{i=1}^{|G:H|} g_i RH) \otimes_{RH} V \\ &= \bigoplus_{i=1}^{|G:H|} (g_i RH \otimes_{RH} V) \\ &= \bigoplus_{i=1}^{|G:H|} g_i \otimes_{RH} V \end{aligned}$$

and as R-modules $g_iRH \otimes_{RH} V \cong RH \otimes_{RH} V \cong V$.

We next show that with its left action on $RG \otimes_{RH} V$ coming from the left action on RG, G permutes these R-submodules. If $x \in G$ and $xg_i = g_j h$ with $h \in H$ then

$$\begin{aligned} x(g_i \otimes v) &= xg_i \otimes v \\ &= g_j h \otimes v \\ &= g_j \otimes hv, \end{aligned}$$

so that $x(g_i \otimes v) \subseteq g_j \otimes V$. We argue that we have equality using the invertibility of x. For, by a similar argument to the one above, we have $x^{-1}g_j \otimes V \subseteq g_i \otimes V$, and so $g_j \otimes V = xx^{-1}(g_j \otimes V) \subseteq x(g_i \otimes V)$. This action of G on the subspaces is transitive since given two subspaces $g_i \otimes V$ and $g_j \otimes V$ we have $(g_j g_i^{-1})g_i \otimes V = g_j \otimes V$.

Now to compute the stabilizer of $g_1 \otimes V$ where $g_1 \in H$, if $x \in H$ then $x(g_1 \otimes V) = g_1(g_1^{-1}xg_1) \otimes V = g_1 \otimes V$, and if $x \notin H$ then $x \in g_iH$ for some $i \neq 1$ and so $x(g_1 \otimes V) = g_i \otimes V$. Thus $\mathrm{Stab}_G(g_1 \otimes V) = H$. □

The structure of induced modules described in the last result in fact characterizes these modules, giving an extremely useful criterion for a module to be of this form which we will use several times later on.

(4.8) PROPOSITION. *Let M be an RG-module which has an R-submodule V with the property that M is the direct sum of the R-submodules $\{gV \mid g \in G\}$. Let $H = \{g \in G \mid gV = V\}$. Then $M \cong V \uparrow_H^G$.*

Proof. We define a map of R-modules

$$\begin{aligned} RG \otimes_{RH} V &\to M \\ g \otimes v &\mapsto gv \end{aligned}$$

extending this specification from the generators to the whole of $RG \otimes_{RH} V$ by R-linearity. This is in fact a map of RG-modules. The R-submodules gV of M are in bijection with the cosets G/H, since G permutes them transitively, and the stabilizer of one of them is H. Thus each of $RG \otimes_{RH} V$ and M is the direct sum of $|G : H|$ R-submodules $g \otimes V$ and gV respectively, each isomorphic to V via isomorphisms $g \otimes v \leftrightarrow v$ and $gv \leftrightarrow v$. Thus on each summand the map $g \otimes v \mapsto gv$ is an isomorphism, and so $RG \otimes_{RH} V \to M$ is itself an isomorphism. □

(4.9) *Examples.* 1. Immediately from the definitions we have $RG = R\uparrow_1^G$.

2. More generally, suppose that Ω is a G-set, that is a set with an action of G. We may form $R\Omega$, the free R-module with the elements of Ω as a basis, and it acquires the structure of an RG-module via the permutation action of G on this basis. This is the *permutation module* determined by Ω. Now $R\Omega = \bigoplus_{\omega\in\Omega} R\omega$ is the direct sum of rank 1 R-submodules, each generated by a basis vector. In case G acts transitively on Ω these are permuted transitively by G. If we pick any $\omega \in \Omega$ and let $H = \operatorname{Stab}\omega$ then H is also the stabilizer of the space $R\omega$ and $R\Omega \cong R\uparrow_H^G$. This shows that permutation modules on transitive G-sets are induced modules.

The general function of induced representations is that they are a mechanism which relates the representations of a group to those of a subgroup. When working over $\mathbb{C}$ they provide a way of constructing new characters, and with this in mind we give the formula for the character of an induced representation. If χ is the character of a representation V of a subgroup H, let us simply write $\chi\uparrow_H^G$ for the character of $V\uparrow_H^G$. We will also write $[G/H]$ to denote a set of representatives of the left cosets of H in G.

(4.10) PROPOSITION. *Let H be a subgroup of G and let V be a $\mathbb{C}H$-module with character χ. Then the character of $V\uparrow_H^G$ is*

$$\begin{aligned}\chi\uparrow_H^G(g) &= \frac{1}{|H|}\sum_{\substack{t\in G\\ t^{-1}gt\in H}} \chi(t^{-1}gt)\\ &= \sum_{\substack{t\in[G/H]\\ t^{-1}gt\in H}} \chi(t^{-1}gt).\end{aligned}$$

Proof. The two formulas on the right are in fact the same, since if $t^{-1}gt \in H$ and $h \in H$ then $(th)^{-1}gth \in H$ also, and so $\{t \in G \mid t^{-1}gt \in H\}$ is a union of left cosets of H. Since $\chi(t^{-1}gt) = \chi((th)^{-1}gth)$ the terms in the first sum are constant on the cosets of H, and we obtain the second sum by choosing one representative from each coset and multiplying by $|H|$.

Using the vector space decomposition of 4.7 we obtain that the trace of g on $V\uparrow_H^G$ is the sum of the traces of g on the spaces $t\otimes V$ which are invariant under g, where $t \in [G/H]$. This is because if g does not leave $t\otimes V$ invariant, we get a matrix of zeros on the diagonal at that point in the block matrix decomposition for the matrix of g. Thus we only get a non-zero contribution from subspaces $t\otimes V$ with $gt\otimes V = t\otimes V$. This happens if and only if $t^{-1}gt\otimes V = 1\otimes V$, that is $t^{-1}gt \in H$. We have

$$\chi\uparrow_H^G(g) = \sum_{\substack{t\in[G/H]\\ t^{-1}gt\in H}} \text{trace of } g \text{ on } t\otimes V.$$

Now g acts on $t \otimes V$ as

$$g(t \otimes v) = t(t^{-1}gt) \otimes v = t \otimes (t^{-1}gt)v$$

and so the trace of g on this space is $\chi(t^{-1}gt)$. Combining this with the last expression gives the result. □

We see in the above proof that g leaves invariant $t \otimes V$ if and only if $t^{-1}gt \in H$, or in other words $g \in tHt^{-1}$. Thus $\mathrm{Stab}_G(t \otimes V) = tHt^{-1}$. Furthermore, if we identify $t \otimes V$ with V by means of the bijection $t \otimes v \leftrightarrow v$, then g acts on $t \otimes V$ via the composite homomorphism

$$\langle g \rangle \xrightarrow{c_{t^{-1}}} H \xrightarrow{\rho} GL(V)$$

where ρ is the homomorphism associated to V and $c_a(x) = axa^{-1}$ is the automorphism of G which is conjugation by $a \in G$.

(4.11) *Example.* To make clearer what the terms in the expression for the induced character are, consider $G = S_3$ and $H = \langle (123) \rangle$ the normal subgroup of order 3. To avoid expressions such as $(())$ we will write the identity element of S_3 as e. We may take the coset representatives $[G/H]$ to be $\{e, (12)\}$. If χ is the trivial character of H then

$$\begin{aligned} \chi \uparrow_H^G (e) &= \chi(e^e) + \chi(e^{(12)}) = 2 \\ \chi \uparrow_H^G ((12)) &= \text{the empty sum} = 0 \\ \chi \uparrow_H^G ((123)) &= \chi((123)^e) + \chi((123)^{(12)}) = 2 \end{aligned}$$

Recalling the character table of S_3 we find that $\chi \uparrow_H^G$ is the sum of the trivial character and the sign character of S_3.

Before giving examples of how induced characters may be used in the construction of character tables, we describe some formalism of the relationship between a group and its subgroups which will allow us to compute more easily with induced representations. The companion notion to induction is that of *restriction* of representations. If H is a subgroup of G and W is a representation of G we denote by $W \downarrow_H^G$ the representation of H obtained by letting the elements of H the way they do when regarded as elements of G. Restriction and induction are a particular case of the following more general situation. Whenever we have a (unital) homomorphism of rings $A \to B$, an A-module V and an B-module W we may form the B-module $B \otimes_A V$ and the A-module $W \downarrow_A^B$. On taking $A = RH$ and $B = RG$ we obtain the induction and restriction we have been studying.

(4.12) LEMMA. *Let $A \to B$ be a homomorphism of rings, V an A-module and W a B-module.*

(1) (Adjointness of $\otimes$ and Hom*)* $\mathrm{Hom}_B(B \otimes_A V, W) \cong \mathrm{Hom}_A(V, W \downarrow_A)$.

(2) If $\phi : B \to C$ is another ring homomorphism then $C \otimes_B (B \otimes_A V) \cong C \otimes_A V$.

Proof. In the case of (1) the mutually inverse isomorphisms are

$$f \mapsto (v \mapsto f(1 \otimes v))$$

and

$$(b \otimes v \mapsto bg(v)) \leftarrow g.$$

In the case of (2) the mutually inverse isomorphisms are

$$c \otimes b \otimes v \mapsto c\phi(b) \otimes v$$

and

$$c \otimes 1 \otimes v \leftarrow c \otimes v.$$

□

(4.13) COROLLARY. *Let $H \leq K \leq G$ be subgroups of G, let V be an RH-module and W an RG-module.*

(1) (Frobenius reciprocity) $\mathrm{Hom}_{RG}(V \uparrow_H^G, W) \cong \mathrm{Hom}_{RH}(V, W \downarrow_H^G)$.

(2) (Transitivity of induction) $(V \uparrow_H^K) \uparrow_K^G \cong V \uparrow_H^G$.

(3) (Transitivity of restriction) $(W \downarrow_K^G) \downarrow_H^K = W \downarrow_H^G$.

(4) $V \uparrow_H^G \otimes_R W \cong (V \otimes_R W \downarrow_H^G) \uparrow_H^G$.

Proof. The first two are the translation of 4.12 into the language of group representations and the third statement is clear. Part (4) is the statement

$$(RG \otimes_{RH} V) \otimes_R W \cong RG \otimes_{RH} (V \otimes_R W)$$

and is not a corollary of 4.12. Here the mutually inverse isomorphisms are

$$(g \otimes v) \otimes w \mapsto g \otimes (v \otimes g^{-1}w)$$

and

$$(g \otimes v) \otimes gw \leftarrow g \otimes (v \otimes w).$$

□

In the case of representations in characteristic zero all of these results may be translated into the language of characters. By analogy with the notation $\chi \uparrow_K^G$ for the character of an induced representation $V \uparrow_K^G$, let us write $\chi \downarrow_H^K$ for the character of $V \downarrow_H^K$.

(4.14) COROLLARY. *Let $H \leq K \leq G$ be subgroups of G, let χ be a complex character of H and ψ a character of G.*

(1) (Frobenius reciprocity)

$$\langle \chi \uparrow_H^G, \psi \rangle_G = \langle \chi, \psi \downarrow_H^G \rangle_H$$

and

$$\langle \psi, \chi \uparrow_H^G \rangle_G = \langle \psi \downarrow_H^G, \chi \rangle_H.$$

In fact all four numbers are equal.

(2) (Transitivity of induction) $(\chi \uparrow_H^K) \uparrow_K^G = \chi \uparrow_H^G$.

(3) (Transitivity of restriction) $(\psi \downarrow_K^G) \downarrow_H^K = \psi \downarrow_H^G$.

(4) $\chi \uparrow_H^G \cdot \psi = (\chi \cdot \psi \downarrow_H^G) \uparrow_H^G$.

Proof. In (1) we write $\langle \quad , \quad \rangle_G$ and $\langle \quad , \quad \rangle_H$ to denote the inner product of characters of G and H, respectively. The four parts are translations of the four parts of 4.13 into the language of characters. In part (1) we use the fact that the inner products are the dimensions of the Hom groups in 4.13(1) and that the inner product is symmetric. □

The statement of Frobenius reciprocity for complex characters is equivalent to the statement that if ψ and χ are simple characters of G and H respectively then the multiplicity of ψ as a summand of $\chi \uparrow_H^G$ equals the multiplicity of χ as a summand of $\psi \downarrow_H^G$.

At a slightly more sophisticated level we may interpret induction, restriction and Frobenius reciprocity in terms of the space $\mathbb{C}^{\mathrm{cc}(G)}$ of class functions introduced in Section 3, that is, the vector space of functions $\mathrm{cc}(G) \to \mathbb{C}$ where $\mathrm{cc}(G)$ is the set of conjugacy classes of G. Since each conjugacy class of H is contained in a unique conjugacy class of G we have a mapping $\mathrm{cc}(H) \to \mathrm{cc}(G)$ and this gives rise by composition to a linear map $\downarrow_H^G \colon \mathbb{C}^{\mathrm{cc}(G)} \to \mathbb{C}^{\mathrm{cc}(H)}$ which on characters is the restriction operation we have already defined. We may also define a linear map $\uparrow_H^G \colon \mathbb{C}^{\mathrm{cc}(H)} \to \mathbb{C}^{\mathrm{cc}(G)}$ which on characters sends a character χ of H to the character $\chi \uparrow_H^G$. It would be possible to define this on arbitrary class functions of H by means of the explicit formula given in 4.10, but the trouble with this is that transitivity of induction is not entirely obvious. It is perhaps easier to observe that the characters of simple representations of H form a basis of $\mathbb{C}^{\mathrm{cc}(H)}$. We have defined $\chi \uparrow_H^G$ on these basis elements, and we may define $\uparrow_H^G$ on arbitrary class functions so that it is a linear map. With these definitions the formulas of 4.14 hold for arbitrary class functions. We may also interpret Frobenius reciprocity within this framework. The inner products $\langle \quad , \quad \rangle_G$ and $\langle \quad , \quad \rangle_H$ provide us with the notion of the transpose of a linear map between the vector spaces $\mathbb{C}^{\mathrm{cc}(H)}$ and $\mathbb{C}^{\mathrm{cc}(G)}$. Now Frobenius reciprocity states that induction and restriction are the transpose of each other. We know that the characters

of simple modules form orthonormal bases of these vector spaces. Taking matrices with respect to these bases, the matrix of induction is the transpose of the matrix of restriction.

(4.15) *Examples.* 1. Frobenius reciprocity is a most useful tool in calculating with induced characters. In the special case that V and W are simple representations over $\mathbb{C}$ of H and G, respectively, where $H \leq G$, it says that the multiplicity of W as a summand of $V\uparrow_H^G$ equals the multiplicity of V as a summand of $W\downarrow_H^G$. As an example we may take both V and W to be the trivial representations of their respective groups. As explained in 4.9, $\mathbb{C}\uparrow_H^G$ is a permutation module. We deduce from Frobenius reciprocity that as representations of G, $\mathbb{C}$ is a direct summand of $\mathbb{C}\uparrow_H^G$ with multiplicity one.

2. Let $G = \langle x, y \mid x^n = y^2 = 1, yxy^{-1} = x^{-1}\rangle = D_{2n}$, the dihedral group of order $2n$. Suppose that n is odd. We compute that the commutator $[y, x] = x^{n-2}$, and since n is odd we have $G' = \langle x^{n-2}\rangle = \langle x\rangle \cong C_n$ and $G/G' \cong C_2$. Thus G has two complex characters of degree 1 which we denote 1 and -1.

Let χ_s denote the degree 1 character of $\langle x\rangle$ specified by $\chi_s(x^r) = \zeta^{rs}$ where $\zeta = e^{\frac{2\pi i}{n}}$. Then $\chi_s\uparrow_{\langle x\rangle}^G$ has values given in the following table.

	$2n$	n	n		n	2
	1	x	x^2	$\cdots$	$x^{\frac{n-1}{2}}$	y
1	1	1	1	$\cdots$	1	1
-1	1	1	1	$\cdots$	1	-1
$\chi_s\uparrow_{\langle x\rangle}^G$	2	$\zeta^s + \overline{\zeta^s}$	$\zeta^{2s} + \overline{\zeta^{2s}}$	$\cdots$	$\zeta^{\frac{n-1}{2}s} + \overline{\zeta^{\frac{n-1}{2}s}}$	0
$(1 \leq s \leq \frac{n-1}{2})$						

TABLE: The character table of D_{2n}, n odd.

We verify that

$$\langle \chi_s\uparrow_{\langle x\rangle}^G, \pm 1\rangle_G = \langle \chi_s, \pm 1\downarrow_{\langle x\rangle}^G\rangle_{\langle x\rangle} = 0$$

if $n \not| s$, using Frobenius reciprocity (or a direct calculation), and hence the characters χ_s are simple when $n \not| s$. For $1 \leq s \leq \frac{n-1}{2}$ they are distinct, and so we have constructed $\frac{n-1}{2} + 2 = \frac{n+3}{2}$ simple characters. This equals the number of conjugacy classes of G, so we have the complete character table.

Symmetric and Exterior Powers

As further ways of constructing new representations from old ones we describe the symmetric powers and exterior powers of a representation. If V is a vector space over a field k its *nth symmetric power* is the vector space

$$S^n(V) = V^{\otimes n}/I$$

where $V^{\otimes n} = V \otimes \cdots \otimes V$ with n factors, and I is the subspace spanned by tensors $(\cdots \otimes v_i \otimes \cdots \otimes v_j \otimes \cdots - \cdots \otimes v_j \otimes \cdots \otimes v_i \otimes \cdots)$ where $v_i, v_j \in V$. We write the image of the tensor $v_1 \otimes \cdots \otimes v_n$ in $S^n(V)$ as a (commutative) product $v_1 \cdots v_n$, noting that in $S^n(V)$ it does not matter in which order we write the terms. A good way to think of $S^n(V)$ is as the space of homogeneous polynomials of degree n in a polynomial ring. Indeed, if $u_1, \ldots, u_r$ is any basis of V and we let $k[u_1, \ldots, u_r]_n$ denote the vector space of homogeneous polynomials of degree n in the u_i as indeterminates, there is a surjective linear map

$$V^{\otimes n} \to k[u_1, \ldots, u_r]_n$$
$$u_{i_1} \otimes \cdots \otimes u_{i_n} \mapsto u_{i_1} \cdots u_{i_n}$$

(extended by linearity to the whole of $V^{\otimes n}$). This map contains I in its kernel, so there is induced a map

$$S^n(V) \to k[u_1, \ldots, u_r]_n.$$

This is now an isomorphism since, modulo I, the tensors $u_1^{\otimes a_1} \otimes u_2^{\otimes a_2} \otimes \cdots \otimes u_r^{\otimes a_r}$ where $\sum_{i-1}^r a_i = n$, span $V^{\otimes n}$, and they map to the monomials which form a basis of $\dim_k k[u_1, \ldots, u_r]_n$. As is well-known, $\dim_k k[u_1, \ldots, u_r]_n = \binom{n+r-1}{n}$.

The *nth exterior power* of V is the vector space

$$\Lambda^n(V) = V^{\otimes n}/J$$

where J is the subspace spanned by tensors $(\cdots \otimes v_i \otimes \cdots \otimes v_j \otimes \cdots + \cdots \otimes v_j \otimes \cdots \otimes v_i \otimes \cdots)$ and $(\cdots \otimes v_i \otimes \cdots \otimes v_i \otimes \cdots)$ where $v_i, v_j \in V$. We write the image of $v_1 \otimes \cdots \otimes v_n$ in $\Lambda^n(V)$ as $v_1 \wedge \cdots \wedge v_n$, so that interchanging v_i and v_j changes the sign of the symbol, and if two of v_i and v_j are equal the symbol is zero. If the characteristic of k is not 2 the second of these properties follows from the first, but for the sake of characteristic 2 we impose it anyway. By an argument similar to the one used for symmetric powers we see that $\Lambda^n(V)$ has as a basis $\{u_{i_1} \wedge \cdots \wedge u_{i_n} \mid 1 \leq i_1, \cdots i_n \leq r\}$, and its dimension is $\binom{n}{r}$. In particular, $\Lambda^n(V) = 0$ if $n > \dim V$.

Suppose now that a group G acts on V and consider the diagonal action of G on $V^{\otimes n}$. The subspaces of relations I and J are preserved by this action, and so there arise actions of G on $S^n(V)$ and $\Lambda^n(V)$:

$$g \cdot (v_1 v_2 \cdots v_n) = (gv_1)(gv_2) \cdots (gv_n)$$
$$g \cdot (v_1 \wedge \cdots \wedge v_n) = (gv_1) \wedge \cdots \wedge (gv_n).$$

Because we substitute the expressions for gv_i into the monomials which form the bases of $S^n(V)$ and $\Lambda^n(V)$, we say that G acts on these spaces by *linear substitutions*. With these actions we have described the symmetric and exterior powers of the representation V.

(4.16) *Example.* Consider the representation of $G = \langle x \mid x^3 = 1\rangle$ on the vector space V with basis $\{u_1, u_2\}$ given by

$$\begin{aligned} xu_1 &= u_2 \\ xu_2 &= -u_1 - u_2. \end{aligned}$$

Then $S^2(V)$ has a basis $\{u_1^2, u_1u_2, u_2^2\}$ and

$$\begin{aligned} x \cdot u_1^2 &= u_2^2 \\ x \cdot (u_1u_2) &= u_2(-u_1 - u_2) = -u_1u_2 - u_2^2 \\ x \cdot u_2^2 &= (-u_1 - u_2)^2 = u_1^2 + 2u_1u_2 + u_2^2. \end{aligned}$$

Similarly $\Lambda^2(V)$ has basis $\{u_1 \wedge u_2\}$ and

$$x \cdot (u_1 \wedge u_2) = u_2 \wedge (-u_1 - u_2) = u_1 \wedge u_2.$$

The symmetric and exterior powers fit into a more general framework where we consider tensors with different symmetry properties. There is an action of the symmetric group S_n on the n-fold tensor power $V^{\otimes n}$ given by permuting the positions of vectors in a tensor, so that for example if α, β, γ are vectors in V then

$$\begin{aligned} (1,2)(\alpha \otimes \beta \otimes \gamma) &= \beta \otimes \alpha \otimes \gamma, \\ (1,3)(\beta \otimes \alpha \otimes \gamma) &= \gamma \otimes \alpha \otimes \beta. \end{aligned}$$

From the above very convincing formulas and the fact that $(1,2,3) = (1,3)(1,2)$ we deduce that

$$(1,2,3)(\alpha \otimes \beta \otimes \gamma) = \gamma \otimes \alpha \otimes \beta$$

which is evidence that if $\sigma \in S_n$ then

$$\sigma(v_1 \otimes \cdots \otimes v_n) = v_{\sigma^{-1}(1)} \otimes v_{\sigma^{-1}(2)} \otimes \cdots \otimes v_{\sigma^{-1}(n)},$$

a formula which is not quite so obvious. With this action it is evident that $S^n(V)$ is the largest quotient of $V^{\otimes n}$ on which S_n acts trivially, and when $\mathrm{char}(k) \neq 2$, $\Lambda^n(V)$ is the largest quotient of $V^{\otimes n}$ on which S_n acts as a sum of copies of the sign representation.

We define the *symmetric tensors* to be the fixed points $(V^{\otimes n})^{S_n}$, and when $\mathrm{char}\, k \neq 2$ we define the *skew-symmetric tensors* to be the largest kS_n-submodule of $V^{\otimes n}$ which is a sum of modules isomorphic to the sign representation. Thus

$$\begin{aligned} \text{symmetric tensors} &= \{w \in V^{\otimes n} \mid \sigma(w) = w \text{ for all } \sigma \in S_n\}, \\ \text{skew-symmetric tensors} &= \{w \in V^{\otimes n} \mid \sigma(w) = \mathrm{sign}(\sigma) w \text{ for all } \sigma \in S_n\}. \end{aligned}$$

When we let G act diagonally on $V^{\otimes n}$ the symmetric tensors, the skew-symmetric tensors, as well as the subspaces I and J defined earlier remain invariant for the action of G. We easily see this directly, but at a more theoretical level the reason is that the actions of G and S_n on $V^{\otimes n}$ commute with each other (as is easily verified), so that $V^{\otimes n}$ acquires the structure of a $k[G \times S_n]$-module, and elements of G act as endomorphisms of $V^{\otimes n}$ as a kS_n-module, and vice-versa. Every endomorphism of the kS_n-module $V^{\otimes n}$ must send the S_n-fixed points to themselves, for example, and so the symmetric tensors are invariant under the action of G. One sees similarly that the other subspaces are also invariant under the action of G.

We remark that, in general, the symmetric power $S^n(V)$ and the symmetric tensors provide non-isomorphic representations of G, as do $\Lambda^n(V)$ and the skew-symmetric tensors. This phenomenon is investigated in the exercises at the end of this section. However these pairs of kG-modules are isomorphic in characteristic zero, and we now consider in detail the case of the symmetric and exterior square. Suppose that k is a field whose characteristic is not 2. In this situation the only tensor which is both symmetric and skew-symmetric is 0, and furthermore any tensor may be written as the sum of a symmetric tensor and a skew-symmetric tensor in the following way:

$$\sum \lambda_{ij} v_i \otimes v_j = \frac{1}{2} \sum \lambda_{ij} (v_i \otimes v_j + v_j \otimes v_i) + \frac{1}{2} \sum \lambda_{ij} (v_i \otimes v_j - v_j \otimes v_i).$$

We deduce from this that

$$V \otimes V = \text{symmetric tensors} \oplus \text{skew-symmetric tensors}$$

as kG-modules. The subspace I which appeared in the definition $S^2(V) = (V \otimes V)/I$ is contained in the space of skew-symmetric tensors, and the subspace J for which $\Lambda^2(V) = (V \otimes V)/J$ is contained in the space of symmetric tensors. By counting dimensions we see that $\dim I + \dim J = \dim V \otimes V$ and putting this together we see that

$$\begin{aligned} I &= \text{ skew-symmetric tensors} \\ J &= \text{ symmetric tensors, and} \\ V \otimes V &= I \oplus J. \end{aligned}$$

From this information we see on factoring out I and J that

$$\begin{aligned} S^2(V) &\cong \text{ symmetric tensors} \\ \Lambda^2(V) &\cong \text{ skew-symmetric tensors} \end{aligned}$$

and we have proved the following result.

(4.17) PROPOSITION. *Suppose V is a representation for G over a field k whose characteristic is not 2. Then*

$$V \otimes V \cong S^2(V) \oplus \Lambda^2(V),$$

as kG-modules, where G acts diagonally on $V \otimes V$ and by linear substitutions on $S^2(V)$ and $\Lambda^2(V)$.

Our application of this is that when constructing new representations from an existing representation V, the tensor square will always decompose in this fashion.

Suppose now that $k = \mathbb{C}$. If χ is the character of a representation V we write $S^2\chi$ and $\Lambda^2\chi$ for the characters of $S^2(V)$ and $\Lambda^2(V)$.

(4.18) PROPOSITION. *Let χ be the character of a representation V of G over $\mathbb{C}$. Then*

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

Proof. For each $g \in G$, $V \downarrow^G_{\langle g \rangle}$ is the direct sum of 1-dimensional representations of the cyclic group $\langle g \rangle$, and so we may choose a basis $u_1, \ldots, u_r$ for V such that $g \cdot u_i = \lambda_i u_i$ for scalars λ_i. The monomials u_i^2 with $1 \le i \le r$ and $u_i u_j$ with $1 \le i < j \le r$ form a basis for S^2V, and so the eigenvalues of g on this space are λ_i^2 with $1 \le i \le r$ and $\lambda_i\lambda_j$ with $1 \le i < j \le r$. Therefore

$$\begin{aligned} S^2\chi(g) &= \sum_{i=1}^{r} \lambda_i^2 + \sum_{1 \le i < j \le r} \lambda_i\lambda_j \\ &= \frac{1}{2}((\lambda_1 + \cdots + \lambda_r)^2 + (\lambda_1^2 + \cdots + \lambda_r^2)) \\ &= \frac{1}{2}(\chi(g)^2 + \chi(g^2)). \end{aligned}$$

Similarly $\Lambda^2 V$ has a basis $u_i \wedge u_j$ with $1 \le i < j \le r$, so the eigenvalues of g on $\Lambda^2 V$ are $\lambda_i\lambda_j$ with $1 \le i < j \le r$ and

$$\begin{aligned} \Lambda^2\chi(g) &= \sum_{1 \le i < j \le r} \lambda_i\lambda_j \\ &= \frac{1}{2}((\lambda_1 + \cdots + \lambda_r)^2 - (\lambda_1^2 + \cdots + \lambda_r^2)) \\ &= \frac{1}{2}(\chi(g)^2 - \chi(g^2)). \end{aligned}$$

□

The Construction of Character Tables

We may now summarize some major techniques used in constructing complex character tables. The first things to do are to determine

the conjugacy classes in G,
the abelianization G/G',
the 1-dimensional characters of G.

We construct characters of degree larger than 1 as

natural representations of G,
representations induced from subgroups,
tensor products of other representations,
symmetric and exterior powers of other representations,
contragredients of other representations.

As a special case of the induced representations, we have permutation representations. The representations obtained by these methods might not be simple, so we test them for simplicity and subtract off known character summands using the

orthogonality relations

which are assisted in the case of induced characters, by

Frobenius reciprocity.

The orthogonality relations provide a check on the accuracy of our calculations, and also enable us to complete the final row of the character table. The facts that the character degrees divide $|G|$ and that the sum of the squares of the degrees equals $|G|$ also help in this.

Exercises for Section 4.

1. Compute the character table of the dihedral group D_{2n} when n is even.
2. Let G be the non-abelian group of order 21:

$$G = \langle x, y \mid x^7 = y^3 = 1, yxy^{-1} = x^2 \rangle.$$

Show that G has 5 conjugacy classes, and find its character table.

3. Find the character table of the following group of order 36:

$$G = \langle a, b, c \mid a^3 = b^3 = c^4 = 1, ab = ba, cac^{-1} = b, cbc^{-1} = a^2 \rangle.$$

[It follows from these relations that $\langle a, b \rangle$ is a normal subgroup of G of order 9.]

4. Given any representation $\rho : G \to GL(V)$ where V is a vector space over any field k, evidently $\operatorname{Ker}\rho$ is a normal subgroup of G. Prove the following 'converse' to the last statement, namely: given a normal subgroup $N \triangleleft G$, there exists a representation ρ with $\operatorname{Ker}\rho = N$. If we assume further that $k = \mathbb{C}$, show how to identify $\operatorname{Ker}\rho$ knowing only the character of ρ.

5. Let k be any field, H a subgroup of G, and V a representation of H over k. Show that $V^* \uparrow_H^G \cong (V \uparrow_H^G)^*$. Deduce that $kG \cong (kG)^*$ and (more generally) that permutation modules are self-dual (i.e. isomorphic to their dual).

6. Let k be any field, and V any representation of G over k. Prove that $V \otimes kG$ is isomorphic to a direct sum of copies of kG.

7. Three-suffix tensors have components $\tau_{ijk} \in \mathbb{R}$ where $i, j, k \in \{1, 2, 3\}$, and form a vector space V of dimension 27 over $\mathbb{R}$. The symmetric group S_3 acts on V by permuting the suffixes. Decompose the space V as a direct sum of simple representations of S_3, giving the mutiplicities of each simple representation. [Observe that V is a permutation representation.]

Give also the decomposition of V as a direct sum of three subspaces consisting of tensors with different symmetry properties under S_3. What are the dimensions of these subspaces?

8. Let V be a representation of G over a field k of characteristic zero. Prove that the symmetric power $S^n(V)$ is isomorphic as a kG-module to the space of symmetric tensors in $V^{\otimes n}$.

9. Let U, V be kG-modules where k is a field, and suppose we are given a non-degenerate bilinear pairing

$$\langle \quad , \quad \rangle : U \times V \to k$$

which has the property $\langle u, v\rangle = \langle gu, gv\rangle$ for all $u \in U$, $v \in V$, $g \in G$. If U_1 is a subspace of U let $U_1^\perp = \{v \in V \mid \langle u, v\rangle = 0 \text{ for all } u \in U_1\}$ and if V_1 is a subspace of V let $V_1^\perp = \{u \in U \mid \langle u, v\rangle = 0 \text{ for all } v \in V_1\}$.

(a) Show that $V \cong U^*$ as kG-modules, and that there is an identification of V with U^* so that $\langle \quad , \quad \rangle$ identifies with the canonical pairing $U \times U^* \to k$.

(b) Show that if U_1 and V_1 are kG-submodules, then so are $U_1^\perp$ and $V_1^\perp$.

(c) Show that if $U_1 \subseteq U_2$ are kG-submodules of U then

$$U_1^\perp / U_2^\perp \cong (U_2/U_1)^*$$

as kG-modules.

(d) Show that the composition factors of U^* are the duals of the composition factors of U.

10. Let Ω be a G-set and $k\Omega$ the corresponding permutation module, where k is a field. Let $\langle \quad , \quad \rangle : k\Omega \times k\Omega \to k$ be the symmetric bilinear form specified on the elements of Ω as

$$\langle \omega_1, \omega_2\rangle = \begin{cases} 1 & \text{if } \omega_1 = \omega_2, \\ 0 & \text{otherwise.} \end{cases}$$

(a) Show that this bilinear form is G-invariant, i.e. $\langle \omega_1, \omega_2 \rangle = \langle g\omega_1, g\omega_2 \rangle$ for all $g \in G$.

(b) Show that $k\Omega$ is self-dual, i.e. $k\Omega \cong (k\Omega)^*$.

11. Let V be a kG-module where k is a field, and let $\langle \quad , \quad \rangle : V \times V^* \to k$ be the canonical pairing between V and its dual, so $\langle v, f \rangle = f(v)$.

(a) Show that the specification $\langle v_1 \otimes \cdots \otimes v_n, f_1 \otimes \cdots \otimes f_n \rangle = f_1(v_1) \cdots f_n(v_n)$ determines a non-degenerate bilinear pairing $\langle \quad , \quad \rangle : V^{\otimes n} \times (V^*)^{\otimes n} \to k$ which is invariant both for the diagonal action of G and the action of S_n given by permuting the positions of the tensors.

(b) Let I and J be the subspaces of $V^{\otimes n}$ which appear in the definitions of the symmetric and exterior powers, so $S^n(V) = V^{\otimes n}/I$ and $\Lambda^{\otimes n} = V^{\otimes n}/J$. Show that $I^\perp$ equals the space of symmetric tensors in $(V^*)^{\otimes n}$, and that $J^\perp$ equals the space of skew-symmetric tensors in $(V^*)^{\otimes n}$ (at least, when $\operatorname{char} k \neq 2$).

(c) Show that $(S^n(V))^* \cong \mathrm{ST}^n(V^*)$, and that $(\Lambda^n(V))^* \cong \mathrm{SST}^n(V^*)$, where ST^n denotes the symmetric tensors, and in general we define the skew-symmetric tensors $\mathrm{SST}^n(V^*)$ to be $J^\perp$.

12. Let $G = C_2 \times C_2$ be the Klein four group with generators a and b, and $k = \mathbb{F}_2$ the field of two elements. Let V be a 3-dimensional space on which a and b act via the matrices

$$\begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}.$$

Show that $S^2(V)$ is not isomorphic to either $ST^2(V)$ or $ST^2(V)^*$, where ST denotes the symmetric tensors. [Hint: Compute the dimensions of the spaces of fixed points of these representations.]

13. (Artin's Induction Theorem) Let $\mathbb{C}^{\mathrm{cc}(G)}$ denote the vector space of class functions on G and let $\mathcal{C}$ be a set of subgroups of G which contains a representative of each conjugacy class of cyclic subgroups of G. Consider the linear mappings

$$\mathrm{res}_{\mathcal{C}} : \mathbb{C}^{\mathrm{cc}(G)} \to \bigoplus_{H \in \mathcal{C}} \mathbb{C}^{\mathrm{cc}(H)}$$

and

$$\mathrm{ind}_{\mathcal{C}} : \bigoplus_{H \in \mathcal{C}} \mathbb{C}^{\mathrm{cc}(H)} \to \mathbb{C}^{\mathrm{cc}(G)}$$

whose component homomorphisms are the linear mappings given by restriction

$$\downarrow_H^G : \mathbb{C}^{\mathrm{cc}(G)} \to \mathbb{C}^{\mathrm{cc}(H)}$$

and induction

$$\uparrow_H^G : \mathbb{C}^{\mathrm{cc}(H)} \to \mathbb{C}^{\mathrm{cc}(G)}$$

(a) With respect to the usual inner product $\langle \quad , \quad \rangle_G$ on $\mathbb{C}^{\mathrm{cc}(G)}$ and the inner product on $\bigoplus_{H\in\mathcal{C}} \mathbb{C}^{\mathrm{cc}(H)}$ which is the orthogonal sum of the $\langle \quad , \quad \rangle_H$, show that $\mathrm{res}_{\mathcal{C}}$ and $\mathrm{ind}_{\mathcal{C}}$ are the transpose of each other.

(b) Show that $\mathrm{res}_{\mathcal{C}}$ is injective.

[Use the fact that $\mathbb{C}^{\mathrm{cc}(G)}$ has a basis consisting of characters, which take their information from cyclic subgroups.]

(c) Prove Artin's induction theorem: In $\mathbb{C}^{\mathrm{cc}(G)}$ every character χ can be written as a rational linear combination

$$\chi = \sum a_{H,\psi} \psi \uparrow_H^G$$

where the sum is taken over cyclic subgroups H of G, ψ ranges over characters of H and $a_{H,\psi} \in \mathbb{Q}$.

[Deduce this from surjectivity of $\mathrm{ind}_{\mathcal{C}}$ and the fact that it is given by a matrix with integer entries. A stronger statement of Artin's theorem is possible: there is a proof due to Brauer which gives an explicit formula for the coefficients $a_{H,\psi}$; from this we may deduce that when χ is the character of a $\mathbb{Q}G$-module the ψ which arise may all be taken to be the trivial character.]

(d) Show that if U is any $\mathbb{C}G$-module then there are $\mathbb{C}G$-modules P and Q, each a direct sum of modules of the form $V \uparrow_H^G$ where H is cyclic, for various V and H, so that $U^n \oplus P \cong Q$ for some n, where U^n is the direct sum of n copies of U.

14. (Molien's Theorem) (a) Let $\rho : G \to GL(V)$ be a complex representation of G, so that V is a $\mathbb{C}G$-module, and for each n let $\chi_{S^n(V)}$ be the character of the nth symmetric power of V. Show that for each $g \in G$ there is an equality of formal power series

$$\sum_{n=0}^{\infty} \chi_{S^n(V)}(g) t^n = \frac{1}{\det(1 - t\rho(g))}.$$

Here t is an indeterminate, and the determinant which appears in this expression is of a matrix with entries in the polynomial ring $\mathbb{C}[t]$, so that the determinant is a polynomial in t. On expanding the rational function on the right we obtain a formal power series which is asserted to be equal to the formal power series on the left.

[Choose a basis for V so that g acts diagonally, with eigenvalues $\xi_1, \ldots, \xi_d$. Show that on both sides of the equation the coefficient of t^n is equal to $\sum_{i_1+\cdots+i_d=n} \xi_1^{i_1} \cdots \xi_d^{i_d}$.]

(b) If W is a simple $\mathbb{C}G$-module we may write the multiplicity of W as a summand of $S^n(V)$ as $\langle \chi_{S^n(V)}, \chi_W \rangle$ and consider the formal power series

$$M_V(W) = \sum_{i=0}^{\infty} \langle \chi_{S^n(V)}, \chi_W \rangle t^n.$$

Show that

$$M_V(W) = \frac{1}{|G|} \sum_{g\in G} \frac{\chi_W(g^{-1})}{\det(1 - t\rho(g))}.$$

(c) When $G = S_3$ and V is the 2-dimensional simple $\mathbb{C}S_3$-module show that

$$M_V(\mathbb{C}) = \frac{1}{(1-t^2)(1-t^3)} = 1 + t^2 + t^3 + t^4 + t^5 + 2t^6 + t^7 + 2t^8 + 2t^9 + 2t^{10} + \cdots$$
$$M_V(\epsilon) = \frac{t^3}{(1-t^2)(1-t^3)} = t^3 + t^5 + t^6 + t^7 + t^8 + 2t^9 + t^{10} + \cdots$$
$$M_V(V) = \frac{t(1+t)}{(1-t^2)(1-t^3)} = t + t^2 + t^3 + 2t^4 + 2t^5 + 2t^6 + 3t^7 + 3t^8 + 3t^9 + 4t^{10} + \cdots$$

where $\mathbb{C}$ denotes the trivial module and ϵ the sign representation. Deduce, for example, that the eighth symmetric power $S^8(V) \cong \mathbb{C}^2 \oplus \epsilon \oplus V^3$.

5. More on Induction and Restriction: Theorems of Mackey and Clifford

We start with Mackey's decomposition formula, which is a further relationship between induction and restriction. For this we need to consider double cosets. Given subgroups H and K of G we define for each $g \in G$ the (H, K)-*double coset*

$$HgK = \{hgk \mid h \in H, k \in K\}.$$

If Ω is a left G-set we use the notation $G\backslash\Omega$ for the set of orbits of G on Ω, and denote a set of representatives for the orbits by $[G\backslash\Omega]$. Similarly if Ω is a right G-set we write Ω/G and $[\Omega/G]$. We will use all the time the fact that if Ω is a transitive G-set and $\omega \in \Omega$ then $\Omega \cong G/\operatorname{Stab}_G(\omega)$, the set of left cosets of the stabilizer of ω in G.

(5.1) PROPOSITION. *Let $H, K \leq G$.*

(1) Each (H, K)-double coset is a disjoint union of right cosets of H and a disjoint union of left cosets of K.

(2) Any two (H, K)-double cosets either coincide or are disjoint. The (H, K)-double cosets partition G.

(3) The set of (H, K)-double cosets is in bijection with the orbits $H\backslash(G/K)$, and with the orbits $(H\backslash G)/K$ under the mappings

$$HgK \mapsto H(gK) \in H\backslash(G/K)$$
$$HgK \mapsto (Hg)K \in (H\backslash G)/K.$$

Proof. (1) If $hgk \in HgK$ and $k_1 \in K$ then $hgk \cdot k_1 = hg(kk_1) \in HgK$ so that the entire left coset of K which contains hgk is contained in HgK. This shows that HgK is a union of left cosets of K, and similarly it is a union of right cosets of K.

(2) If $h_1g_1k_1 = h_2g_2k_2 \in Hg_1K \cap Hg_2K$ then $g_1 = h_1^{-1}h_2g_2k_2k_1^{-1} \in Hg_2K$ so that $Hg_1K \subseteq Hg_2K$, and similarly $Hg_2K \subseteq Hg_1K$. Thus if two double cosets are not disjoint, they coincide.

(3) In the statement of this result, G acts from the left on the left cosets G/K, hence so does H by restriction of the action. We denote the set of H-orbits on G/K by $H\backslash(G/K)$. The mapping

$$\{\text{double cosets}\} \to H\backslash(G/K)$$
$$HgK \mapsto H(gK)$$

is evidently well-defined and surjective. If $H(g_1K) = H(g_2K)$ then $g_2K = hg_1K$ for some $h \in H$, so $g_2 \in Hg_1K$ and $Hg_1K = Hg_2K$ by (2). Hence the mapping is injective.

The proof that double cosets biject with $(H\backslash G)/K$ is similar. □

In view of (3) we denote the set of (H, K)-double cosets in G by $H\backslash G/K$. We denote a set of representatives for these double cosets by $[H\backslash G/K]$.

(5.2) *Example.* Consider $S_2 = \{1, (12)\}$ as a subgroup of S_3. We have

$$S_2\backslash S_3/S_2 = \{\{1, (12)\}, \{(123), (132), (13), (23)\}\},$$

while, for example,

$$[S_2\backslash S_3/S_2] = \{1, (123)\}.$$

S_3 acts transitively on $\{1, 2, 3\}$ with $\mathrm{Stab}_{S_3}(3) = S_2$, so as S_3-sets we have

$$S_3/S_2 \cong \{1, 2, 3\}.$$

Thus the set of orbits on this set under the action of S_2 is

$$S_2\backslash(S_3/S_2) \leftrightarrow \{\{1, 2\}, \{3\}\}.$$

We observe that these orbits are indeed in bijection with the double cosets $S_2\backslash S_3/S_2$.

This example illustrates the point that when computing double cosets it may be advantageous to identify G/K as some naturally occuring G-set, rather than as the set of left cosets.

In the next result we distinguish between conjugation on the left and on the right: ${}^g x = gxg^{-1}$ and $x^g = g^{-1}xg$. Later on we will write $c_g(x) = {}^g x$, so that $c_g : H \to {}^g H$ is the homomorphism which is left conjugation by g, and $c_{g^{-1}}(x) = x^g$.

(5.3) PROPOSITION. *Let H, K be subgroups of G and $g \in G$ an element. We have isomorphisms*

$$HgK/K \cong H/(H \cap {}^g K) \quad \text{as left } H\text{-sets}$$

and

$$H\backslash HgK \cong (H^g \cap K)\backslash K \quad \text{as right } K\text{-sets.}$$

Thus the double coset HgK is a union of $|H : H \cap {}^g K|$ left K-cosets and $|K : H^g \cap K|$ right H-cosets. We have

$$|G : K| = \sum_{g \in [H\backslash G/K]} |H : H \cap {}^g K|$$

and

$$|G : H| = \sum_{g \in [H\backslash G/K]} |K : H^g \cap K|.$$

Proof. HgK is the union of a single H-orbit of left K-cosets. The stablizer in H of one of these is

$$\begin{aligned}\mathrm{Stab}_H(gK) &= \{h \in H \mid hgK = gK\}\\ &= \{h \in H \mid h^g K = K\}\\ &= \{h \in H \mid h^g \in K\}\\ &= H \cap {}^gK.\end{aligned}$$

Thus $HgK/K \cong H/(H \cap {}^gK)$ as left H-sets and the number of left K-cosets in HgK equals $|H : H \cap {}^gK|$. By summing these numbers over all double cosets we obtain the total number of left K-cosets $|G : K|$.

The argument with right H-cosets is similar. □

We next introduce *conjugation* of representations, a concept we have in fact already met with induced representations. Suppose H is a subgroup of G, $g \in G$ and V is a representation of H. We define a representation ${}^gV$ of ${}^gH$ by specifying that ${}^gV = V$ as a set, and if ${}^gh \in {}^gH$ then ${}^gh \cdot v = hv$. Thus if $\rho : H \to GL(V)$ was the original representation, the conjugate representation is the composite homomorphism ${}^gH \xrightarrow{c_{g^{-1}}} H \xrightarrow{\rho} GL(V)$ where $c_{g^{-1}}({}^gh) = h$.

When studying the structure of induced representations $V \uparrow_H^G = \bigoplus_{g \in [G/H]} g \otimes V$, the subspace $g \otimes V$ is in fact a representation for ${}^gH$; for

$$ghg^{-1} \cdot (g \otimes v) = ghg^{-1}g \otimes v = gh \otimes v = g \otimes hv.$$

When $g \otimes V$ is identified with V via the linear isomorphism $g \otimes v \mapsto v$ the action of ${}^gH$ on V which arises coincides with the action we have just described on ${}^gV$.

(5.4) THEOREM (Mackey decomposition formula). *Let H, K be subgroups of G and V a representation for K over a commutative ring R. Then*

$$(V \uparrow_K^G) \downarrow_H^G \cong \bigoplus_{g \in [H \backslash G / K]} ({}^g(V \downarrow_{H^g \cap K}^K)) \uparrow_{H \cap {}^gK}^H$$

as RH-modules.

Proof. We have $V \uparrow_K^G = \bigoplus_{x \in [G/K]} x \otimes V$. Consider a particular double coset HgK. The terms

$$\bigoplus_{\substack{x \in [G/K] \\ x \in HgK}} x \otimes V$$

form an R-submodule invariant under the action of H, since it is the direct sum of an orbit of R-submodules permuted by H. Now

$$\begin{aligned}\mathrm{Stab}_H(g \otimes V) &= \{h \in H \mid hg \in gK\}\\ &= H \cap {}^gK.\end{aligned}$$

Therefore as a representation for H this subspace is $(g \otimes V) \uparrow_{H \cap {}^gK}^H$. As observed before the statement of this theorem we have $g \otimes V \cong {}^g(V \downarrow_{H^g \cap K}^K)$ as a representation of $H \cap {}^gK$. Putting these expressions together gives the result. □

As an application of Mackey's theorem we consider permutation modules arising from multiply transitive G-sets. We say that a G-set Ω is *n-transitive* if for every pair of n-tuples $(a_1, \ldots, a_n)$ and $(b_1, \ldots, b_n)$ in which the a_i are distinct elements of Ω and the b_i are distinct elements of Ω, there exists $g \in G$ with $ga_i = b_i$ for every i. For example, S_n acts n-transitively on $\{1, \ldots, n\}$, and one may show that A_n acts $(n-2)$-transitively on $\{1, \ldots, n\}$ provided $n \geq 3$. Notice that if G acts n-transitively on Ω then it also acts $(n-1)$-transitively.

(5.5) LEMMA. *Let Ω be a G-set. Then G acts n-transitively on Ω if and only if G acts transitively on Ω and for any $\omega \in \Omega$, $\mathrm{Stab}_G(\omega)$ acts $(n-1)$-transitively on $\Omega - \{\omega\}$.*

Proof. If G acts n-transitively then G also acts transitively, and if $a_2, \ldots, a_n$ and $b_2, \ldots, b_n$ are two sets of $n-1$ distinct points of Ω, none of them equal to ω, then there exists $g \in G$ so that $g(\omega) = (\omega)$ and $g(a_i) = b_i$ for all i. This shows that $\mathrm{Stab}_G(\omega)$ acts $(n-1)$-transitively on $\Omega - \{\omega\}$.

Conversely, suppose G acts transitively on Ω and $\mathrm{Stab}_G(\omega)$ always acts $(n-1)$-transitively on $\Omega - \{\omega\}$. Let $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$ be two sets of n distinct points of Ω. We may find $g_1 \in G$ so that $g_1 a_1 = b_1$. Now find $g_2 \in \mathrm{Stab}_G(b_1)$ so that $g_2 g_1 a_i 2 = b_i$ for $2 \leq i \leq n$ and put $g = g_2 g_1$. Then $g(a_i) = (b_i)$ for all i. □

(5.6) PROPOSITION. *Whenever Ω is a G-set the permutation module $\mathbb{C}\Omega$ may be written as a direct sum of $\mathbb{C}G$-modules*

$$\mathbb{C}\Omega = \mathbb{C} \oplus V$$

Suppose that $|\Omega| \geq 1$, so $V \neq 0$. The representation V is simple if and only if G acts 2-transitively on Ω. In that case, V is not the trivial representation.

Proof. Pick any orbit of G on Ω. It is isomorphic as a G-set to G/H for some subgroup $H \leq G$ and so $\mathbb{C}[G/H]$ is a direct summand of $\mathbb{C}\Omega$, with character $1 \uparrow_H^G$. Since

$$\langle 1, 1 \uparrow_H^G \rangle_G = \langle 1, 1 \rangle_H = 1$$

we deduce that $\mathbb{C}$ is a summand of $\mathbb{C}[G/H]$ and hence of $\mathbb{C}\Omega$.

In the equivalence of statements which forms the third sentence, neither side is true if G has more than one orbit on Ω, so we may assume $\Omega = G/H$. The character of $\mathbb{C}\Omega$ is

$1\uparrow_H^G$, and we compute

$$\begin{aligned}\langle 1\uparrow_H^G, 1\uparrow_H^G\rangle_G &= \langle (1\uparrow_H^G)\downarrow_H^G, 1\rangle_H \\ &= \langle \sum_{g\in[H\backslash G/H]} ({}^g1)\uparrow_{H\cap {}^gH}^H, 1\rangle_H \\ &= \sum_{g\in[H\backslash G/H]} \langle 1\uparrow_{H\cap {}^gH}^H, 1\rangle_H \\ &= \sum_{g\in[H\backslash G/H]} \langle 1,1\rangle_{H\cap {}^gH} \\ &= \sum_{g\in[H\backslash G/H]} 1 \\ &= |H\backslash G/H|,\end{aligned}$$

using Frobenius reciprocity twice and Mackey's formula. Now $|H\backslash G/H|$ is the number of orbits of H (the stabilizer of a point) on G/H. By Lemma 5.5 this number is 2 if G acts 2-transitively on Ω, and otherwise it is greater than 2 (since $|\Omega| \geq 1$). Writing $\mathbb{C}[G/H] = S_1 \oplus \cdots \oplus S_n$ as a direct sum of simple representations we have $\langle 1\uparrow_H^G, 1\uparrow_H^G\rangle_G \geq n$ and we get the value 2 for the inner product if and only if there are 2 simple representations in this expression, and they are non-isomorphic. One of S_1 and S_2 must be $\mathbb{C}$ and the other V, so V is not the trivial representation. □

(5.7) *Example.* Let $\Omega = \{1, \ldots, n\}$ acted upon by S_n and also A_n. Then $\mathbb{C}\Omega \cong \mathbb{C} \oplus V$ where V is a simple representation of S_n, which remains simple on restriction to A_n provided $n \geq 4$.

We now turn to Clifford's theorem, which we present in a weak and a strong form. The weak form is used as a step in proving the strong form a little later, and as a result in its own right it only has force in a situation where $|G|$ is not invertible in the ground ring.

(5.8) THEOREM (Weak form of Clifford's theorem). *Let k be any field, U a simple kG-module and N a normal subgroup of G. Then $U\downarrow_N^G$ is semisimple as a kN-module.*

Proof. Let V be any simple kN-submodule of U. For every $g \in G$, gV is also a kN-submodule since if $n \in N$ we have $n(gv) = g(g^{-1}ng)v \in gV$, using the fact that N is normal. Evidently gV is also simple, since if W were a kN-submodule of gV then $g^{-1}W$ would be a submodule of V. Now $\sum_{g\in G} gV$ is a non-zero G-invariant subspace of the simple kG-module U, and so $\sum_{g\in G} gV = U$. As a kN-module we see that $U\downarrow_N^G$ is the sum of simple submodules, and hence $U\downarrow_N^G$ is semisimple by the results of Section 1. □

The kN-submodules gV which appear in the proof of 5.8 are isomorphic to modules we have seen before. Since $N \lhd G$, the conjugate module ${}^gV$ is a representation for ${}^gN = N$. The mapping

$$\begin{aligned} {}^gV &\to gV \\ v &\mapsto gv \end{aligned}$$

is an isomorphism of kN-modules, since if $n \in N$ the action on ${}^gV$ is $n \cdot v = g^{-1}ngv$ and the action on gV is $n(gv) = g(g^{-1}ngv)$. Recall also that these modules appeared when we described induced modules. Part of Clifford's theorem states that the simple module U is in fact an induced module.

(5.9) THEOREM (Clifford's theorem). *Let k be any field, U a simple kG-module and N a normal subgroup of G. Write $U \downarrow_N^G = S_1^{a_1} \oplus \cdots \oplus S_r^{a_r}$ where the S_i are non-isomorphic simple kN-modules and the a_i are the multiplicities to which they occur. (We refer to the summands $S_i^{a_i}$ as the homogeneous components.) Then*
(1) G permutes the homogeneous components transitively,
(2) $a_1 = a_2 = \cdots = a_r$, and
(3) if $H = \mathrm{Stab}_G(S_1^{a_1})$ then $U \cong S_1^{a_1} \uparrow_H^G$.

Proof. We start by observing that the homogeneous component $S_i^{a_i}$ is characterized as the unique largest kN-submodule which is isomorphic to a direct sum of copies of S_i, as stated in Corollary 1.9. If $g \in G$ then $g(S_i^{a_i})$ is a direct sum of isomorphic simple modules gS_i, and so by this characterization must be contained in another homogeneous component: $g(S_i^{a_i}) \subseteq S_j^{a_j}$ for some j. Since $U = g(S_1^{a_1}) \oplus \cdots \oplus g(S_r^{a_r})$, by counting dimensions we have $g(S_i^{a_i}) = S_j^{a_j}$. Thus G permutes the homogeneous components. Since $\sum_{g \in G} g(S_1^{a_1})$ is a non-zero G-invariant submodule of the simple module U, it must equal U, and so the action on the homogeneous components is transitive. This establishes (1), and (2) follows since for any pair (i, j) we can find $g \in G$ with $g(S_i)^{a_i} = S_j^{a_j}$, so $a_i = a_j$. Finally, (3) is a direct consequence of Proposition 4.8. □

For now, we give just one application of Clifford's theorem; we will see more when we come to consider representations of p-groups in characteristic p. Although true as stated, the next corollary only has force when k is a field of characteristic zero, as we will see in the next section that the only simple representation for a p-group in characteristic p is the trivial representation.

(5.10) COROLLARY. *Let k be any algebraically closed field and G a p-group. Then every simple module for G has the form $U \uparrow_H^G$ where U is a 1-dimensional module for some subgroup H.*

Proof. We proceed by induction on $|G|$. Let $\rho : G \to GL(S)$ be a simple representation of G over k and put $N = \mathrm{Ker}\,\rho$. Then S is really a representation of G/N. If $N \neq 1$ then

G/N is a group of smaller order than G, so by induction S has the claimed structure as a representation of G/N, and hence also as a representation of G. Thus we may assume $N = 1$ and G embeds in $GL(S)$.

If G is abelian then all simple representations are 1-dimensional, so we are done. Assume now that G is not abelian. Then G has a normal abelian subgroup A which is not central. To construct this subgroup A, let $Z_2(G)$ denote the second centre of G, that is, the preimage in G of $Z(G/Z(G))$. If x is any element of $Z_2(G) - Z(G)$ then $A = \langle Z(G), x\rangle$ is a normal abelian subgroup not contained in $Z(G)$.

We apply Clifford's theorem:

$$S \downarrow_A^G = S_1^{a_1} \oplus \cdots \oplus S_r^{a_r}$$

and $S = V \uparrow_K^G$ where $V = S_1^{a_1}$ and $K = \mathrm{Stab}_G(S_1^{a_1})$. We argue that V must be a simple kK-module, since if it had a proper submodule W then $W \uparrow_K^G$ would be a proper submodule of S, which is simple. If $K \neq G$ then by induction $V = U \uparrow_H^K$ where U is 1-dimensional, and so $S = (U \uparrow_H^K) \uparrow_K^G = U \uparrow_H^G$ has the required form.

We show finally that the case $K = G$ cannot happen. For if it were to happen then $S \downarrow_A^G = S_1^{a_1}$ and since A is abelian $\dim S_1 = 1$. The elements of A must therefore act via scalar multiplication on S. Since such action would commute with the action of G, which is faithfully represented on S, we deduce that $A \subseteq Z(G)$, a contradiction. □

The conclusion of Corollary 5.10 also applies to supersoluble groups, which also have the property, if they are not abelian, that they have a non-central normal abelian subgroup.

Exercises for Section 5.

1. Let k be any field, and g any element of a finite group G.

(a) If $K \leq H \leq G$ are subgroups of G, V a kH-module, and W a kK-module, show that $({}^gV) \downarrow_{{}^gK}^{{}^gH} \cong {}^g(V \downarrow_K^H)$ and $({}^gW) \uparrow_{{}^gK}^{{}^gH} \cong {}^g(W \uparrow_K^H)$. [This allows one to interchange conjugation with induction, or with restriction, in Mackey's formula.]

(b) If U is any kG-module, show that ${}^gU \cong U$.

2. Consider the complex representations of S_n and A_n. Show that if S is any simple representation of S_n then $S\downarrow_{A_n}$ is the sum of at most 2 simple representations of A_n, and that if the degree of S is odd then $S\downarrow_{A_n}$ is simple.

In the situation where $S\downarrow_{A_n}$ is the sum of 2 simple representations of A_n, show that S is induced from a representation of A_n.

In the situation where $S\downarrow_{A_n}$ is simple, show that $S\downarrow_{A_n}\uparrow^{S_n} \cong S \oplus (\epsilon \otimes S)$ where ϵ is the sign representation, and that $S \ncong \epsilon \otimes S$.

6. Representations of p-groups in characteristic p

The study of representations of a group over a field whose characteristic divides the group order is more delicate than the case of ordinary representation theory (characteristic zero), since modules need not be semisimple, and we have to do more than count multiplicities of simple modules. The notion of a direct sum decomposition is still the first consideration in describing the structure of a representation, but now we may find ourselves in the situation where we have broken apart the modules as far as possible into direct summands, and still these summands are not simple. An example of this was given in 1.2.2. In view of this phenomenon we make the definition that a module U for an algebra A is *indecomposable* if it cannot be expressed as a direct sum of two modules except in a trivial way, that is if $U \cong V \oplus W$ then either $V = 0$ or $W = 0$.

We start with an explicit description of the representations of cyclic p-groups.

(6.1) PROPOSITION. *Let k be any field of characteristic p and let $G = \langle g \mid g^{p^n} = 1 \rangle$. Then there is a ring isomorphism $kG \cong k[X]/(X^{p^n})$, where $k[X]$ is the polynomial ring in an indeterminate X.*

Proof. We define a mapping

$$\begin{aligned} G &\to k[X]/(X^{p^n}) \\ g^s &\mapsto (X+1)^s. \end{aligned}$$

Since

$$(X+1)^{p^n} = X^{p^n} + p(\cdots) + 1 \equiv 1 \ (\mathrm{mod}(X^{p^n}))$$

this mapping is a group homomorphism, and hence it extends to a linear map

$$kG \to k[X]/(X^{p^n})$$

which is an algebra homomorphism. Since g^s is sent to X^s plus terms of lower degree, the images of $1, \ldots, g^{p^n-1}$ form a basis of $k[X]/(X^{p^n})$. The mapping therefore gives a bijection between a basis of kG and a basis of $k[X]/(X^{p^n})$, and so is an isomorphism. □

A module over a ring is said to be *cyclic* if it can be generated by one element. We now exploit the structure theorem for finitely-generated modules over a principal ideal domain, which says that such modules are direct sums of cyclic modules.

(6.2) THEOREM. *Let k be any field of characteristic p. Every finitely-generated $k[X]/(X^{p^n})$-module is a direct sum of cyclic modules $U_r = k[X]/(X^r)$ where $1 \le r \le p^n$. The only simple module is the 1-dimensional module U_1. Each module U_r has a unique composition series, and hence is indecomposable.*

Proof. The modules for $k[X]/(X^{p^n})$ may be identified with the modules for $k[X]$ on which X^{p^n} acts as zero. Every finitely-generated $k[X]$-module is a direct sum of modules $k[X]/I$ where I is an ideal. Hence every $k[X]/(X^{p^n})$-module is a direct sum of modules $k[X]/I$ on which X^{p^n} acts as zero, which is to say $(X^{p^n}) \subseteq I$. The ideals I which satisfy this last condition are the ideals (a) where $a \mid X^{p^n}$. This forces $I = (X^r)$ where $1 \le r \le p^n$, and $k[X]/I = U_r$.

The submodules of U_r must have the form $J/(X^r)$ where J is some ideal containing (X^r), and they are precisely the submodules in the chain

$$0 \subset (X^{r-1})/(X^r) \subset (X^{r-2})/(X^r) \subset \cdots \subset (X)/(X^r) \subset U_r.$$

This is a composition series, since each successive quotient has dimension 1, and since it is a complete list of submodules, it is the only one. If we could write $U_r = V \oplus W$ as a non-trivial direct sum, then U_r would have at least 2 composition series, obtained by taking first a composition series for V, then one for W, or vice-versa. Hence each U_r is indecomposable and we have a complete list of the indecomposable modules. The only U_r which is simple is U_1, which is the trivial module. □

A module with a unique composition series is said to be *uniserial*. We see from the description of $k[X]/(X^{p^n})$-modules that U_r has a basis $1+(X^r), X+(X^r), \ldots, X^{r-1}+(X^r)$ so that X acts on U_r with matrix

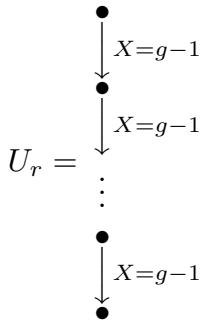
$$\begin{pmatrix} 0 & & & \\ 1 & 0 & & \\ & \ddots & \ddots & \\ & & 1 & 0 \end{pmatrix}.$$

Translating now to modules for kG where G is a cyclic p-group, the generator g acts on U_r as $X + 1$, which has matrix

$$\begin{pmatrix} 1 & & & \\ 1 & 1 & & \\ & \ddots & \ddots & \\ & & 1 & 1 \end{pmatrix}.$$

Thus we see that the indecomposable kG-modules are exactly given by specifying that the generator g acts via a matrix which is a single Jordan block, of size up to p^n. It is often

helpful to picture U_r as the diagram



One way to interpret this is that the vertices are in bijection with a basis of U_r, and the action of X or $g-1$ is given by the arrows. Where no arrow is shown starting from a particular vertex (as happens in this case only with the bottom one), the interpretation is that X and $g-1$ act as zero.

(6.3) PROPOSITION. *Let k be any field of characteristic p and G a p-group. The only simple kG-module is the trivial module.*

Proof. We offer two proofs of this.

Proof 1. We proceed by induction on $|G|$, the induction starting when G is the identity group, for which the result is true. Suppose $G \neq 1$ and the result is true for p-groups of smaller order. There exists a normal subgroup N of G of index p. If S is any simple kG-module then by Clifford's theorem $S\downarrow_N^G$ is semisimple. By induction, N acts trivially on S. Thus S is really a representation of G/N which is cyclic of order p. We have just proved that the only simple representation of this group is the trivial representation.

Proof 2. Let S be any simple kG-module and let $0 \neq x \in S$. The subgroup of S generated by the elements $\{gx \mid g \in G\}$ is invariant under the action of G, it is abelian and of exponent p, since it is a subgroup of a vector space in characteristic p. Thus it is a finite p group acted on by G. Consider the orbits of G on this finite group. Since G is a p-group the orbits have the form G/H where H is a subgroup, and so have size a power of p (or 1). The zero element is fixed by G, and we deduce that there must be another element fixed by G since otherwise the other orbits would all have size p^n with $n \geq 1$, and their union would not be a p-group. Thus there exists $y \in S$ fixed by G, and now $\langle y \rangle$ is a trivial submodule of S. By simplicity it must equal S. □

As an application of this we can give some information about the simple representations of arbitrary finite groups in characteristic p. For this we observe that in every finite group G there is a unique largest normal p-subgroup of G, denoted $O_p(G)$. For if H and K are normal p-subgroups of G then so is HK, and thus the subgroup generated by all normal p-subgroups of G is a again a normal p-subgroup, which evidently contains all the others.

(6.4) COROLLARY. *Let k be any field of characteristic p, G any finite group and S a simple kG-module. Then $O_p(G)$ acts trivially on S. Thus the simple kG-modules are precisely the simple $k[G/O_p(G)]$-modules, made into kG-modules via the homomorphism $G \to G/O_p(G)$.*

Proof. By Clifford's theorem, $S \downarrow^G_{O_p(G)}$ is semisimple. Therefore, by 6.3, $O_p(G)$ acts trivially on S. □

(6.5) *Example.* Let k be a field of characteristic 2, and consider the representations of A_4 over k. Since $O_2(A_4) = C_2 \times C_2$, the simple kA_4 modules are the simple $C_3 = A_4/O_2(A_4)$-representations, made into representations of A_4. Now kC_3 is semisimple, and if k contains a primitive cube root of unity ω (i.e. if $\mathbb{F}_4 \subseteq k$) there are three 1-dimensional simple representations, on which the generator of C_3 acts as $1, \omega$ or ω^2.

At this point we examine further the structure of representations which are not semisimple, and we work in the context of modules for a ring A. If U is an A-module we defined the socle of U to be the sum of all the simple submodules of U, and we showed (at least in the case that U is finite-dimensional) that it is the unique largest semisimple submodule of U. We now work with quotients and define a dual concept, the *radical* of U. We work with quotients instead of submodules, and use the fact that if M is a submodule of U, the quotient U/M is simple if and only if M is a maximal submodule of U. We put

$$\operatorname{Rad} U = \bigcap \{M \mid M \subset U \text{ is a maximal submodule}\}.$$

In our applications U will always be Noetherian, so this intersection will be non-empty.

(6.6) LEMMA. *Let U be a module for a ring A.*

(1) Suppose that $M_1, \dots, M_n$ are maximal submodules of U. Then there is a subset $I \subseteq \{1, \dots, n\}$ such that

$$U/(M_1 \cap \cdots \cap M_n) \cong \bigoplus_{i \in I} U/M_i$$

which, in particular, is a semisimple module.

(2) Suppose further that U has the descending chain condition on submodules. Then $U/\operatorname{Rad} U$ is a semisimple module, and $\operatorname{Rad} U$ is the unique smallest submodule of U with this property.

Proof. (1) Let I be a subset of $\{1, \dots, n\}$ maximal with the property that the quotient homomorphisms $U/(\bigcap_{i \in I} M_i) \to U/M_i$ induce an isomorphism $U/(\bigcap_{i \in I} M_i) \cong \bigoplus_{i \in I} U/M_i$. We show that $\bigcap_{i \in I} M_i = M_1 \cap \cdots \cap M_n$ and argue by contradiction. If it were not the case, there would exist M_j with $\bigcap_{i \in I} M_i \not\subseteq M_j$. Consider the homomorphism

$$f : U \to (\bigoplus_{i \in I} U/M_i) \oplus U/M_j$$

whose components are the quotient homomorphisms $U \to U/M_k$. This has kernel $M_j \cap \bigcap_{i\in I} M_i$, and it will suffice to show that f is surjective, because this will imply that the larger set $I \cup \{j\}$ has the same property as I, thereby contradicting the maximality of I.

To show that f is surjective let $g : U \to U/\bigcap_{i\in I} M_i \oplus U/M_j$ and observe that $(\bigcap_{i\in I} M_i) + M_j = U$ since the left-hand side is strictly larger than M_j, which is maximal in U. Thus if $x \in U$ we can write $x = y + z$ where $y \in \bigcap_{i\in I} M_i$ and $z \in M_j$. Now $g(y) = (0, x + M_j)$ and $g(z) = (x + \bigcap_{i\in I} M_i, 0)$ so that both summands $U/\bigcap_{i\in I} M_i$ and U/M_j are contained in the image of g and g is surjective. Since f is obtained by composing g with the isomorphism which identifies $U/\bigcap_{i\in I} M_i$ with $\bigoplus_{i\in I} U/M_i$, we deduce that f is surjective.

(2) By the assumption that U has the descending chain condition on submodules, $\operatorname{Rad} U$ must be the intersection of finitely many maximal submodules. Therefore $U/\operatorname{Rad} U$ is semisimple by part (1). If V is a submodule such that V is semisimple, say $U/V \cong S_1 \oplus \cdots \oplus S_n$ where the S_i are simple modules, let M_i be the kernel of $U \to U/V \xrightarrow{\text{projection}} S_i$. Then M_i is maximal and $V = M_1 \cap \cdots \cap M_n$. Thus $V \supseteq \operatorname{Rad} U$, and $\operatorname{Rad} U$ is contained in every submodule V for which U/V is semisimple. □

As a particular case, we define the radical of a ring A to be the radical of the regular representation $\operatorname{Rad}{}_A A$ and write simply $\operatorname{Rad} A$. Thus by 6.6, if A has the descending chain condition on left ideals (for example, if A is a finite-dimensional algebra over a field) then $\operatorname{Rad} A$ is the smallest left ideal of A such that $A/\operatorname{Rad} A$ is a semisimple module.

(6.7) PROPOSITION. *Let A be a ring. Then,*

(1) $\operatorname{Rad} A = \{a \in A \mid a \cdot S = 0$ *for every simple A-module $S\}$, and*

(2) $\operatorname{Rad} A$ *is a 2-sided ideal of A.*

(3) Suppose further that A is a finite-dimensional algebra over a field. Then

(a) $\operatorname{Rad} A$ *is the smallest left ideal of A such that $A/\operatorname{Rad} A$ is a semisimple A-module,*

(b) A is semisimple if and only if $\operatorname{Rad} A = 0$,

(c) $\operatorname{Rad} A$ *is nilpotent, and is the largest nilpotent ideal of A.*

Proof. (1) Given a simple module S and $0 \neq s \in S$, the module homomorphism ${}_A A \to S$ given by $a \mapsto as$ is surjective and its kernel is a maximal left ideal M_s. Now if $a \in \operatorname{Rad} A$ then $a \in M_s$ for every S and $s \in S$, so $as = 0$ and a annihilates every simple module. Conversely, if $a \cdot S = 0$ for every simple module S and M is a maximal left ideal then A/M is a simple module. Therefore $a \cdot (A/M) = 0$, which means $a \in M$. Hence $a \in \bigcap_{\text{maximal}M} M = \operatorname{Rad} A$.

(2) Being the intersection of left ideals, $\operatorname{Rad} A$ is also a left ideal of A. Suppose that $a \in \operatorname{Rad} A$ and $b \in A$, so $a \cdot S = 0$ for every simple S. Now $a \cdot bS \subseteq a \cdot S = 0$ so ab has the same property that a does.

(3) (a) and (b) are immediate from 6.6. We prove (c). Choose any composition series

$$0 = A_n \subset A_{n-1} \subset \cdots \subset A_1 \subset {}_A A$$

of the regular representation. Since each A_i/A_{i+1} is a simple A-module, $\operatorname{Rad} A \cdot A_i \subseteq A_{i+1}$ by part (1). Hence $(\operatorname{Rad} A)^r \cdot A \subseteq A_r$ and $(\operatorname{Rad} A)^n = 0$.

Suppose now that I is a nilpotent ideal of A, say $I^m = 0$, and let S be any simple A-module. Then

$$0 = I^m \cdot S \subseteq I^{m-1} \cdot S \subseteq \cdots \subseteq IS \subseteq S$$

is a chain of A-submodules of S, which are either 0 or S since S is simple. There must be some point where $0 = I^r S \neq I^{r-1} S = S$. Then $IS = I \cdot I^{r-1} S = I^r S = 0$, so in fact that point was the very first step. This shows that $I \subseteq \operatorname{Rad} A$ by part (1). Hence $\operatorname{Rad} A$ contains every nilpotent ideal of A, so is the unique largest such ideal. □

We may now determine the radical of kG when k is a field of characteristic p and G is a p-group. If R is any commutative ring, the ring homomorphism

$$\begin{aligned} \epsilon : RG &\to R \\ g &\mapsto 1 \quad \text{for all } g \in G \end{aligned}$$

is called the *augmentation map*. Regarded as a homomorphism of modules it expresses the trivial representation as a homomorphic image of the regular representation. The kernel of ϵ is called the *augmentation ideal*, and is denoted IG. Evidently IG consists of those elements $\sum_{g \in G} a_g g \in RG$ such that $\sum_{g \in G} a_g = 0$.

(6.8) PROPOSITION.

(1) Let R denote the trivial RG-module. Then $IG = \{x \in RG \mid x \cdot R = 0\}$.

(2) IG is free as an R-module with basis $\{g - 1 \mid 1 \neq g \in G\}$.

(3) If $R = k$ is a field of characteristic p and G is a p-group then $IG = \operatorname{Rad}(kG)$. It follows that IG is nilpotent in this case.

Proof. (1) The augmentation map ϵ is none other than the linear extension to RG of the homomorphism $\rho : G \to GL(1, R)$ which is the trivial representation. Thus each $x \in RG$ acts on R as multiplication by $\epsilon(x)$, and so will act as 0 precisely if $\epsilon(x) = 0$.

(2) The elements $g - 1$ where g ranges through the non-identity elements of G are linearly independent since the elements g are, and they lie in IG. We show that they span IG. Suppose $\sum_{g \in G} a_g g \in IG$, which means that $\sum_{g \in G} a_g = 0 \in R$. Then

$$\sum_{g \in G} a_g g = \sum_{g \in G} a_g g - \sum_{g \in G} a_g 1 = \sum_{1 \neq g \in G} a_g (g - 1)$$

is an expression as a linear combination of elements $g - 1$.

(3) When G is a p-group and $\operatorname{char}(k) = p$ we have seen in 6.3 that k is the only simple kG-module. The result follows by part (1) and 6.7. □

Working in the generality of a finite-dimensional algebra A again, the radical of A allows us to give a further description of the radical and socle of a module.

(6.9) PROPOSITION. *Let A be a finite-dimensional algebra over a field k, and U an A-module.*

(1) The following are all descriptions of $\operatorname{Rad} U$*:*
  (a) the intersection of the maximal submodules of U,
  (b) the smallest submodule of U with semisimple quotient,
  (c) $\operatorname{Rad} A \cdot U$.

(2) The following are all descriptions of $\operatorname{Soc} U$*:*
  (a) the sum of the simple submodules of U,
  (b) the largest semisimple submodule of U,
  (c) $\{u \in U \mid \operatorname{Rad} A \cdot u = 0\}$.

Proof. We have seen the equivalence of descriptions (a) and (b) in 1.10 and 6.6. Let us show that the submodule $\operatorname{Rad} A \cdot U$ in (1)(c) satisfies condition (1)(b). Firstly $U/(\operatorname{Rad} A \cdot U)$ is a module for $A/\operatorname{Rad} A$, which is a semisimple algebra. Hence $U/(\operatorname{Rad} A \cdot U)$ is a semisimple module and so $\operatorname{Rad} A \cdot U$ contains the submodule of (1)(b). On the other hand if $V \subseteq U$ is a submodule for which U/V is semisimple then $\operatorname{Rad} A \cdot (U/V) = 0$ by 6.7, so $V \supseteq \operatorname{Rad} A \cdot U$. In particular, the submodule of (1)(b) contains $\operatorname{Rad} A \cdot U$.

As for $\{u \in U \mid \operatorname{Rad} A \cdot u = 0\}$, this is the largest submodule of U annihilated by $\operatorname{Rad} A$. It is thus an $A/\operatorname{Rad} A$-module and hence is semisimple. Since every semisimple submodule of U is annihilated by $\operatorname{Rad} A$, it is the unique largest such submodule. □

(6.10) *Example.* Consider the situation of 6.1 and 6.2 in which G is a cyclic group of order p^n and k is a field of characteristic p. We see that $\operatorname{Rad} U_r \cong U_{r-1}$ and $\operatorname{Soc} U_r \cong U_1$ for $1 \leq r \leq p^n$, taking $U_0 = 0$.

We now iterate the notions of socle and radical and for each A-module U we define inductively

$$\operatorname{Rad}^n(U) = \operatorname{Rad}(\operatorname{Rad}^{n-1}(U))$$
$$\operatorname{Soc}^n(U)/\operatorname{Soc}^{n-1}(U) = \operatorname{Soc}(U/\operatorname{Soc}^{n-1} U).$$

It is immediate from 6.9 that

$$\operatorname{Rad}^n(U) = (\operatorname{Rad} A)^n \cdot U$$
$$\operatorname{Soc}^n(U) = \{u \in U \mid (\operatorname{Rad} A)^n \cdot u = 0\}$$

and these submodules of U form chains

$$\cdots \subseteq \operatorname{Rad}^2 U \subseteq \operatorname{Rad} U \subseteq U$$
$$0 \subseteq \operatorname{Soc} U \subseteq \operatorname{Soc}^2 U \subseteq \cdots$$

which are called, respectively, the *radical series* and *socle series* of U. They are also known as the lower Loewy series and upper Loewy series of U.

(6.11) PROPOSITION. *Let A be a finite-dimensional algebra over a field k, and U an A-module. The radical series of U is the fastest descending series of submodules of U with semisimple quotients, and the socle series of U is the fastest ascending series of U with semisimple quotients. The two series terminate, and if m and n are the least integers for which $\operatorname{Rad}^m U = 0$ and $\operatorname{Soc}^n U = U$ then $m = n$.*

Proof. Suppose that $\cdots \subseteq U_2 \subseteq U_1 \subseteq U_0 = U$ is a series of submodules of U with semisimple quotients. We show by induction on r that $\operatorname{Rad}^r(U) \subseteq U_r$. This is true when $r = 0$. Suppose that $r > 0$ and $\operatorname{Rad}^{r-1}(U) \subseteq U_{r-1}$. Then

$$\operatorname{Rad}^{r-1}(U)/(\operatorname{Rad}^{r-1}(U) \cap U_r) \cong (\operatorname{Rad}^{r-1} + U_r)/U_r \subseteq U_{r-1}/U_r$$

is semsimple, so $\operatorname{Rad}^{r-1}(U) \cap U_r \supseteq \operatorname{Rad}(\operatorname{Rad}^{r-1}(U)) = \operatorname{Rad}^r(U)$. Therefore $\operatorname{Rad}^r(U) \subseteq U_r$. This shows that the radical series descends faster than the series U_i. The argument that the socle series ascends faster is similar.

Since A is a finite-dimensional algebra we have $(\operatorname{Rad} A)^r = 0$ for some r. Then $\operatorname{Rad}^r U = 0$ and $\operatorname{Soc}^r U = U$ by 6.9. By what we have just proved, the radical series descends at least as fast as the socle series and so has equal or shorter length. By a similar argument (using the fact that the socle series is the fastest ascending series with semisimple quotients) the socle series ascends at least as fast as the radical series and so has equal or shorter length. We conclude that the two lengths are equal. □

The common length of the radical series and socle series of U is called the *Loewy length* of the module U.

We conclude this section by mentioning without proof the theorem of Jennings on the Loewy series of kG when G is a p-group and k is a field of characteristic p and summarize its implications. For proofs, see Benson's book [Ben]. Jennings constructs a decreasing series of subgroups

$$\kappa_r(G) = \{g \in G \mid g \equiv 1 \text{ modulo } \operatorname{Rad}^r(kG)\},$$

which is sometimes called the *Jennings series* of G. This series of subgroups has the properties

1) $[\kappa_r, \kappa_s] \subseteq \kappa_{r+s}$,
2) $g^p \in \kappa_{ip}$ for all $g \in \kappa_i$,
3) κ_r/κ_{2r} is elementary abelian.

Furthermore, we may generate κ_r as

$$\kappa_r = \langle [\kappa_{r-1}, G],\ \kappa^{(p)}_{\lceil r/p \rceil} \rangle,$$

where $\kappa_1 = G$, $\lceil r/p \rceil$ is the least integer greater than or equal to r/p, and $\kappa_r^{(p)}$ is the set of pth powers of elements of κ_r. Evidently the first term in this series is $\kappa_1(G) = G$ and we may see that the second term $\kappa_2(G)$ is the Frattini subgroup of G (the smallest normal

subgroup of G for which the quotient is elementary abelian). After that the terms need to be calculated on a case-by-case basis.

For each $i \geq 1$ let d_i be the dimension of κ_i/κ_{i+1} as a vector space over $\mathbb{F}_p$, and choose any elements $x_{i,s}$ of G such that the set $\{x_{i,s}\kappa_{i+1} \mid 1 \leq s \leq d_i\}$ forms a basis for κ_i/κ_{i+1}. Let $\bar{x}_{i,s} = x_{i,s} - 1 \in kG$. There are $|G|$ products of the form $\prod \bar{x}_{i,s}^{\alpha_{i,s}}$, where the factors are taken in some predetermined order, and $0 \leq \alpha_{i,s} \leq p-1$. The weight of such a product is defined to be $\sum i\alpha_{i,s}$. Jenning's theorem states that the set of products of weight w lie in $\mathrm{Rad}^w(kG)$, and forms a basis of $\mathrm{Rad}^w(kG)$ modulo $\mathrm{Rad}^{w+1}(kG)$. Thus the set of all these products is a basis for kG compatible with the powers of the radical.

For example, if we take an element x of order 4 and an element y of order 2 which generate the dihedral group of order 8, so $D_8 = \langle x, y \mid x^4 = y^2 = 1,\ yxy = x^{-1}\rangle$, we have $\kappa_1 = D_8$, $\kappa_2 = \langle x^2\rangle$, $\kappa_3 = 1$. We may choose $x_{1,1} = x$, $x_{1,2} = y$, $x_{2,1} = x^2$, and note that $\bar{x}^2 = \bar{x^2}$. Now the products $\bar{x}^{\alpha_{1,1}}\bar{x}^{2\alpha_{2,1}}\bar{y}^{\alpha_{1,2}} = \bar{x}^{\alpha_{1,1}+2\alpha_{2,1}}\bar{y}^{\alpha_{1,2}}$, where $0 \leq \alpha_{i,s} \leq 1$, form a basis of kD_8 which is compatible with the powers of the radical. In this special case, these elements may be simplified as $\bar{x}^i\bar{y}^j$ with $0 \leq i \leq 3$ and $0 \leq j \leq 1$.

When doing calculation with group rings of p-groups in characteristic p the basis given by Jennings is often to be preferred over the basis given by the group elements. This basis gives a description of the powers of the radical in group-theoretic terms, and it allows us to deduce a result about the socle series as well. Since each element $\bar{x}_{i,s}$ of weight i contributes factors of weights $0, i, 2i, 3i, \ldots, (p-1)i$ in Jennings' basis , the total number of products of weight w is the coefficient of t^w in

$$(1 + t + t^2 + \cdots + t^{p-1})^{d_1}(1 + t^2 + \cdots + t^{2(p-1)})^{d_2} \cdots = \prod_{i \geq 1} \left(\frac{(1-t^{ip})}{(1-t^i)} \right)^{d_i},$$

and this equals the polynomial $\sum_{w \geq 0} (\dim \mathrm{Rad}^w(kG)/\dim \mathrm{Rad}^{w+1}(kG))t^w$. We see from this that the dimensions of the factors in the radical series of kG are symmetric, in that they are the same if taken in reverse order. Jumping ahead of ourselves for a moment and using the fact that $kG \cong kG^*$ (see Section 8) and also using Exercise 6 to this section, we may see that when G is a p-group and k is a field of characteristic p the terms of the radical series and the socle series of kG coincide, although these terms appear in the two series in the opposite order.

Exercises for Section 6.

1. Let A be a ring. Prove that for each n, $\mathrm{Soc}^n {}_AA$ is a 2-sided ideal of A.

2. Let $\overline{G} = \sum_{g \in G} g$ as an element of kG, where k is a field. Show that the subspace $k\overline{G}$ of kG spanned by $\overline{G}$ is an ideal. Show that this ideal is nilpotent if and only if the characteristic of k divides $|G|$. Deduce that if kG is semisimple then $\mathrm{char}(k) \nmid |G|$.

3. Prove that if N is a normal subgroup of G and k is a field then $\mathrm{Rad}(kN) = kN \cap \mathrm{Rad}(kG)$.

4. Suppose that U is an indecomposable module with just two composition factors. Show that U is uniserial.

5. Show that the following conditions are equivalent for a module U which has a composition series.

(a) U is uniserial (i.e. U has a unique composition series).
(b) The set of all submodules of U is totally ordered by inclusion.
(c) $\operatorname{Rad}^r U/\operatorname{Rad}^{r+1} U$ is simple for all r.
(d) $\operatorname{Soc}^{r+1} U/\operatorname{Soc}^r U$ is simple for all r.

6. Let U be a kG-module and U^* its dual. Show that for each n

$$\operatorname{Soc}^n(U^*) = \{f \in U^* \mid f(\operatorname{Rad}^n(U) = 0\}$$

and

$$\operatorname{Rad}^n(U^*) = \{f \in U^* \mid f(\operatorname{Soc}^n(U) = 0\}.$$

Deduce that $\operatorname{Soc}^{n+1}(U^*)/\operatorname{Soc}^r(U^*) \cong (\operatorname{Rad}^n(U)/\operatorname{Rad}^{N+1}(U))^*$ as kG-modules. [Hint: recall Exercise 9 to Section 4.]

7. Let H be a subgroup of G.

(a) Let $\overline{H} = \sum_{h\in H} h$ be the sum of the elements of H, as an element of RG. Show that $RG \cdot \overline{H} \cong R\uparrow_H^G$ as RG-modules.

(b) Let IH be the augmentation ideal of RH, as a subset of RG. Show that $RG\cdot IH \cong IH\uparrow_H^G$ as RG-modules, and that $RG/(RG\cdot IH) \cong R\uparrow_H^G$ as RG-modules.

The next five exercises give a direct proof of the result stated in 6.8, that for a p-group in characteristic p the augmentation ideal is nilpotent.

8. Show that if elements $g_1, \ldots, g_n$ generate G as a group, then $(g_1 - 1), \ldots, (g_n - 1)$ generate the augmentation ideal IG as a left ideal of kG.
[Use the formula $(gh - 1) = g(h - 1) + (g - 1)$.]

9. Suppose that k is a field of characteristic p and G is a p-group. Prove that each element $(g - 1)$ is nilpotent. (More generally, every element of IG is nilpotent.)

10. Show that if N is a normal subgroup of G then the left ideal

$$RG \cdot IN = \{x \cdot y \mid x \in RG, y \in IN\}$$

of RG generated by IN is the kernel of the ring homomorphism $RG \to R[G/N]$ and is in fact a 2-sided ideal in RG.
[One approach to this uses the formula $g(n - 1) = ({}^g n - 1)g$.]
Show that $(RG \cdot IN)^r = RG \cdot (IN)^r$ for all r.

11. Show that if a particular element $(g - 1)$ appears n times in a product

$$(g_1 - 1)\cdots(g_r - 1)$$

then

$$(g_1 - 1)\cdots(g_r - 1) \equiv (g - 1)^n \cdot x \quad \text{modulo } kG \cdot (IG')$$

for some $x \in kG$, where G' denotes the commutator subgroup.
[Use the formula $(g-1)(h-1) = (h-1)(g-1) + (ghg^{-1}h^{-1}-1)hg$.]
Show that if G is a p-group and k a field of characteristic p then $IG^r \subseteq kG \cdot IG'$ for some power r.

12. Prove that if G is a p-group and k is a field of characteristic p then $(IG)^r = 0$ for some power r.

13. Calculate the Loewy length of kC_p^n, the group algebra of the direct product of n copies of a cycle of order p.

14. The dihedral group of order $2n$ has a presentation

$$D_{2n} = \langle x, y \mid x^2 = y^2 = (xy)^n = 1 \rangle.$$

Let k be a field of characteristic 2. Show that when n is a power of 2, each power $(ID_{2n})^r$ of the augmentation ideal is spanned modulo $(ID_{2n})^{r+1}$ by the two products $(x-1)(y-1)(x-1)(y-1)\cdots$ and $(y-1)(x-1)(y-1)(x-1)\cdots$ of length r. Hence calculate the Loewy length of kD_{2n} and show that $\operatorname{Rad}(kD_{2n})/\operatorname{Soc}(D_{2n})$ is the direct sum of two kD_{2n}-modules which are uniserial.

15. When $n \geq 3$, the generalized quaternion group of order 2^n has a presentation

$$Q_{2^n} = \langle x, y \mid x^{2^{n-1}} = 1,\ y^2 = x^{2^{n-2}},\ yxy^{-1} = x^{-1} \rangle.$$

Let k be a field of characteristic 2. Show that when $r \geq 1$ each power $(IQ_{2^n})^r$ of the augmentation ideal is spanned modulo $(IQ_{2^n})^{r+1}$ by $(x-1)^r$ and $(x-1)^{r-1}(y-1)$. Hence calculate the Loewy length of kQ_{2^n}.

16. Show that for each RG-module U, $U/(IG \cdot U)$ is the largest quotient of U on which G acts trivially. Prove that $U/(IG \cdot U) \cong R \otimes_{RG} U$.

17. (a) Let G be any group and $IG \subset \mathbb{Z}G$ the augmentation ideal over $\mathbb{Z}$. Prove that $IG/(IG)^2 \cong G/G'$ as abelian groups.
[Consider the homomorphism of abelian groups $IG \to G/G'$ given by $g-1 \mapsto gG'$. Use the formula $ab-1 = (a-1)+(b-1)+(a-1)(b-1)$ to show that $(IG)^2$ is contained in the kernel, and that the homomorphism $G/G' \to IG/(IG)^2$ given by $gG' \mapsto g-1+(IG)^2$ is well defined.]

(b) If now R is any commutative ring with 1 and $IG \subset RG$ is the augmentation ideal, show that $IG/(IG)^2 \cong R \otimes_{\mathbb{Z}} G/G'$ as R-modules.

18. Let Ω be a transitive G-set and k a field. Let $k\Omega$ be the corresponding permutation module. There is a homomorphism of kG-modules $\epsilon : k\Omega \to k$ defined as $\epsilon(\sum_{\omega\in\Omega} a_\omega \omega) = \sum_{\omega\in\Omega} a_\omega$. Let $\overline{\Omega} = \sum_{\omega\in\Omega} \omega \in k\Omega$.

(a) Show that every kG-module homomorphism $k\Omega \to k$ is a scalar multiple of ϵ.

(b) Show that the fixed points of G on $k\Omega$ are $k\Omega^G = k \cdot \overline{\Omega}$.

(c) Show that $\epsilon(\overline{\Omega}) = 0$ if and only if $\operatorname{char} k \mid |\Omega|$, and that if this happens then $\overline{\Omega} \in \operatorname{Rad} k\Omega$ and the trivial module k occurs as a composition factor of $k\Omega$ with multiplicity ≥ 2.

(d) Show that if $\epsilon(\overline{\Omega}) \neq 0$ then ϵ is a split epimorphism and $\overline{\Omega} \notin \operatorname{Rad} k\Omega$.

(e) Show that kG is semisimple if and only if the regular representation kG has the trivial module k as a direct summand (i.e. k is a projective module).

19. Let Ω be a transitive G-set for a possibly infinite group G and let $R\Omega$ be the corresponding permutation module. Show that Ω is infinite if and only if $(R\Omega)^G = 0$ and deduce that G is infinite if and only if $(RG)^G = 0$.

20. Let U_r be the indecomposable kC_p-module of dimension r, $1 \leq r \leq p$, where k is a field of characteristic p. Prove that $U_r = S^{r-1}(U_2)$, the $(r-1)$ symmetric power.
[One way to proceed is to show that if $C_p = \langle g \rangle$ then $(g-1)^{r-1}$ does not act as zero on $S^{r-1}(U_2)$ and use the classification of indecomposable kC_p-modules.]

21. Let $G = SL(2,p)$, the group of 2×2 matrices over $\mathbb{F}_p$ which have determinant 1, where p is a prime. The subgroups

$$P_1 = \{\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \mid \lambda \in \mathbb{F}_p\}, \quad P_2 = \{\begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix} \mid \lambda \in \mathbb{F}_p\}$$

have order p. Let U_2 be the natural 2-dimensional module on which G acts. When $0 \leq r \leq p-1$ prove that $S^r(U_2)$ is a uniserial $\mathbb{F}_pP_1$-module, and also a uniserial $\mathbb{F}_pP_2$-module, but that the only subspaces of $S^r(U_2)$ which are invariant under both P_1 and P_2 are 0 and $S^r(U_2)$. Deduce that $S^r(U_2)$ is a simple $\mathbb{F}_pG$-module.
[Background to the question which is not needed to solve it: $|G| = p(p^2-1)$; both P_1 and P_2 are Sylow p-subgroups of G. In fact, the simple modules constructed here form a complete list of the simple $\mathbb{F}_pSL(2,p)$-modules.]

22. Let g be an endomorphism of a finite-dimensional vector space V over a field k of characteristic p, and suppose that g has finite order p^d for some d. Show that as a $k\langle g \rangle$-module, V has an indecomposable direct summand of dimension at least $p^{d-1}+1$.
[You may assume the classification of indecomposable modules for cyclic p-groups in characteristic p.]

Deduce that if such an endomorphism g fixes a subspace of V of codimension 1 then g has order p or 1.
[An endomorphism (not necessarily of prime-power order) which fixes a subspace of codimension 1 is sometimes referred to as a *reflection* in a generalized sense.]

7. Projective modules for finite-dimensional algebras

In previous sections we have seen the start of techniques to describe modules which are not semisimple. The most basic decomposition of such a module is one that expresses it as a direct sum of modules which cannot be decomposed as a direct sum any further. These summands are called indecomposable modules. We have also examined the notions of radical series and socle series of a module, which are series of canonically defined submodules which may shed light on submodule structure. We combine these two notions in the study of projective modules for group rings, working at first in the generality of modules for finite dimensional algebras over a field. In this situation the indecomposable projective modules are the indecomposable summands of the regular representation. We will see that they are identified by the structure of their radical quotient. The projective modules are important because their structure is part of the structure of the regular representation. Since every module is a homomorphic image of a direct sum of copies of the regular representation, by knowing the structure of the projectives one knows, in some sense, all modules.

Recall that a module M over a ring A is said to be *free* if it has a basis, that is, a subset which spans M as an A-module, and is linearly independent over A. Whenever $\{x_i \mid i \in I\}$ is a basis it follows that $M = \bigoplus_{i\in I} Ax_i$ with $Ax_i \cong A$ for all i. Thus M is a finitely generated free module if and only if $M \cong A^n$ for some n, that is, M may be identified with the module of n-tuples of elements of A.

(7.1) PROPOSITION. *Let A be a ring and M an A-module. Then M is free on a subset $\{x_i \mid i \in I\}$ if and only if for every module N and mapping of sets $\phi : \{x_i \mid i \in I\} \to N$ there exists a unique morphism of modules $\psi : M \to N$ which extends ϕ.*

We omit the proof.

We define a module homomorphism $f : M \to N$ to be a *split epimorphism* if and only if there exists a homomorphism $g : N \to M$ so that $fg = 1_N$, the identity map on N. Note that a split epimorphism is necessarily an epimorphism since if $x \in N$ then $x = f(g(x))$ so that x lies in the image of f. We define similarly f to be a *split monomorphism* if there exists a homomorphism $g : N \to M$ so that $gf = 1_M$. Necessarily a split monomorphism is a monomorphism. We are about to show that if f is a split epimorphism then N is (isomorphic to) a direct summand of M. To combine both this and the corresponding result for split monomorphisms it is convenient to introduce short exact sequences. We say that a diagram of modules and module homomorphisms $L \xrightarrow{\alpha} M \xrightarrow{\beta} N$ is *exact* at M if $\operatorname{Im}\alpha = \operatorname{Ker}\beta$. A *short exact sequence* of modules is a diagram $0 \to L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0$ which is exact a each of L, M and N. Exactness at L and N means simply that α is a monomorphism and β is an epimorphism.

(7.2) PROPOSITION. *Let* $0 \to L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0$ *be a short exact sequence of modules over a ring. The following are equivalent:*

(1) α *is a split monomorphism,*

(2) β *is a split epimorphism, and*

(3) there is a commutative diagram

$$\begin{array}{ccccccccc} 0 & \to & L & \xrightarrow{\alpha} & M & \xrightarrow{\beta} & N & \to & 0 \\ & & \| & & \downarrow \gamma & & \| & & \\ 0 & \to & L & \xrightarrow{\iota_1} & L \oplus N & \xrightarrow{\pi_2} & N & \to & 0 \end{array}$$

where ι_1 *and* π_2 *are inclusion into the first summand and projection onto the second summand.*

In any diagram such as the one in (3) the morphism γ *is necessarily an isomorphism. Thus if any of the three conditions is satisfied it follows that* $M \cong L \oplus N$.

Proof. Condition (3) implies the first two, since the existence of such a commutative diagram implies that α is split by $\pi_1\gamma$ and β is split by $\gamma^{-1}\iota_2$.

Conversely if condition (1) is satisfied, so that $\delta\alpha = 1_L$ for some homomorphism $\delta : M \to L$, we obtain a commutative diagram as in (3) on taking the components of γ to be δ and β. If condition (2) is satisfied we obtain a commutative diagram similar to the one in (3) but with a homomorphism $\zeta : L \oplus N \to M$ in the wrong direction, whose components are α and a splitting of β. We obtain the diagram of (3) on showing that in any such diagram the middle vertical homomorphism must be invertible.

The fact that the middle homomorphism in the diagram must be invertible is a consequence of both the 'five lemma' and the 'snake lemma' in homological algebra. We leave it here as an exercise. □

In the event that α and β are split, we say that the short exact sequence in Proposition 7.2 is *split*. Notice that whenever $\beta : M \to N$ is an epimorphism it is part of the short exact sequence $0 \to \operatorname{Ker}\beta \hookrightarrow M \xrightarrow{\beta} N \to 0$ and so we deduce that if β is a split epimorphism then N is a direct summand of M. A similar comment evidently applies to split monomorphisms.

(7.3) PROPOSITION. *The following are equivalent for an* A*-module* U.

(1) U *is a direct summand of a free module.*

(2) Every epimorphism $V \to U$ *is split.*

(3) For every pair of morphisms

$$\begin{array}{ccc} & & U \\ & & \downarrow \alpha \\ V & \xrightarrow{\beta} & W \end{array}$$

where β is an epimorphism, there exists a morphism $\gamma : U \to V$ with $\beta\gamma = \alpha$.

(4) For every short exact sequence of A-modules $0 \to V \to W \to X \to 0$ the corresponding sequence

$$0 \to \mathrm{Hom}_A(U, V) \to \mathrm{Hom}_A(U, W) \to \mathrm{Hom}_A(U, X) \to 0$$

is exact.

Proof. This result is standard and we do not prove it here. In condition (4) the sequence of homomorphism groups is always exact at the left-hand terms $\mathrm{Hom}_A(U, V)$ and $\mathrm{Hom}_A(U, W)$ without requiring any special property of U (we say that $\mathrm{Hom}_A(U, \quad)$ is *left exact*). The force of condition (4) is that the sequence should be exact at the right-hand term. □

We say that a module U satisfying any of the four conditions of 7.3 is *projective*. Notice that direct sums and also direct summands of projective modules are projective. An indecomposable module which is projective is an indecomposable projective module, and these modules will be very important in our study. In other texts the indecomposable projective modules are also known as PIMs, or Principal Indecomposable Modules, but we will not use this terminology here.

One way to obtain projective A-modules is from idempotents of the ring A. If $e^2 = e \in A$ then ${}_AA = Ae \oplus A(1-e)$ as A-modules, and so the submodules Ae and $A(1-e)$ are projective. We formalize this with the next result, which should be compared with 3.22 in which we were dealing with ring summands of A and central idempotents.

(7.4) PROPOSITION. *Let A be a ring. The decompositions of the regular representation as a direct sum of submodules*

$${}_AA = A_1 \oplus \cdots \oplus A_r$$

biject with expressions $1 = e_1 + \cdots + e_r$ for the identity of A as a sum of orthogonal idempotents, in such a way that $A_i = Ae_i$. The summand A_i is indecomposable if and only if the idempotent e_i is primitive.

Proof. Suppose that $1 = e_1 + \cdots + e_r$ is an expression of the identity as a sum of orthogonal idempotents. Then

$${}_AA = Ae_1 \oplus \cdots \oplus Ae_r,$$

for the Ae_i are evidently submodules of A, and their sum is A since if $x \in A$ then $x = xe_1 + \cdots + xe_r$. The sum is direct since if $x \in Ae_i \cap \sum_{j \neq i} Ae_j$ then $x = xe_i$ and also $x = \sum_{j \neq i} a_j e_j$ so $x = xe_i = \sum_{j \neq i} a_j e_j e_i = 0$.

Conversely, suppose that ${}_AA = A_1 \oplus \cdots \oplus A_r$ is a direct sum of submodules. We may write $1 = e_1 + \cdots + e_r$ where $e_i \in A_i$ is a uniquely determined element. Now

$e_i = e_i 1 = e_i e_1 + \cdots + e_i e_r$ is an expression in which $e_i e_j \in A_j$, and since the only such expression is e_i itself we deduce that

$$e_i e_j = \begin{cases} e_i & \text{if } i = j, \\ 0 & \text{otherwise.} \end{cases}$$

The two constructions just described, in which we associate an expression for 1 as a sum of idempotents to a module direct sum decomposition and vice-versa, are mutually inverse, giving a bijection as claimed.

If a summand A_i decomposes as the direct sum of two other summands, this gives rise to an expression for e_i as a sum of two orthogonal idempotents, and conversely. Thus A_i is indecomposable if and only if e_i is primitive. □

In 3.22 there was a statement about the uniqueness of summands in a decomposition of A as a direct sum of indecomposable rings, and we should point out that the corresponding uniqueness statement need not hold with module decompositions of ${}_A A$. For an example of this we might take $A = M_2(R)$, the ring of 2×2-matrices over a ring R, in which

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

The submodules here are all different. We will see later that if A is a finite-dimensional algebra over a field then in any two decompositions of ${}_A A$ as a direct sum of indecomposable submodules, the submodules are isomorphic in pairs.

We will also see that when A is a finite-dimensional algebra over a field, every indecomposable projective A-module may be realized as Ae for some primitive idempotent e. For other rings this need not be true, and an example is $\mathbb{Z}G$, for which it is the case that the only idempotents are 0 and 1 (see the exercises to Section 8). For certain finite groups (an example is the cyclic group of order 23, but this takes us beyond the scope of this book) there exist indecomposable projective $\mathbb{Z}G$-modules which are not free, so such modules will never have the form $\mathbb{Z}Ge$.

(7.5) *Example.* We present an example of a decomposition of the regular representation in a situation which is not semisimple. Many of the observations we will make are consequences of theory to be presented in later sections, but it seems worthwhile to show that the calculations can be done by direct arguments.

Consider the group ring $\mathbb{F}_4 S_3$ where $\mathbb{F}_4$ is the field of 4 elements. By Proposition 4.5 the 1-dimensional representations of S_3 are the simple representations of $S_3/S_3' \cong C_2$, lifted to S_3. But $\mathbb{F}_4 C_2$ has only one simple module, namely the trivial module, by Proposition 6.3, so this is the only 1-dimensional $\mathbb{F}_4 S_3$-module. The 2-dimensional representation of S_3 constructed in Section 1 over any coefficient ring is now seen to be simple here, since otherwise it would have a trivial submodule; but the eigenvalues of the element $(1,2,3)$ on this module are ω and ω^2, where $\omega \in \mathbb{F}_4$ is a primitive cube root of 1, so there is no trivial submodule.

Let $K = \langle (1,2,3) \rangle$ be the subgroup of S_3 of order 3. Now $\mathbb{F}_4 K$ is semisimple with three 1-dimensional representations on which $(1,2,3)$ acts as 1, ω and ω^2, respectively. In fact

$$\mathbb{F}_4 K = \mathbb{F}_4 K e_1 \oplus \mathbb{F}_4 K e_2 \oplus \mathbb{F}_4 K e_3$$

where

$$\begin{aligned} e_1 &= () + (1,2,3) + (1,3,2) \\ e_2 &= () + \omega(1,2,3) + \omega^2(1,3,2) \\ e_3 &= () + \omega^2(1,2,3) + \omega(1,3,2) \end{aligned}$$

are orthogonal idempotents in $\mathbb{F}_4 K$. We may see that these are orthogonal idempotents by direct calculation, but it can also be seen by observing that the corresponding elements of $\mathbb{C}K$ with ω replaced by $e^{\frac{2\pi i}{3}}$ are orthogonal and square to 3 times themselves (Theorem 3.23), and lie in $\mathbb{Z}[e^{\frac{2\pi i}{3}}]K$. Reduction modulo 2 gives a ring homomorphism $\mathbb{Z}[e^{\frac{2\pi i}{3}}] \to \mathbb{F}_4$ which maps these elements to e_1, e_2 and e_3, while retaining their properties. Thus

$$\mathbb{F}_4 S_3 = \mathbb{F}_4 S_3 e_1 \oplus \mathbb{F}_4 S_3 e_2 \oplus \mathbb{F}_4 S_3 e_3$$

and we have constructed modules $\mathbb{F}_4 S_3 e_i$ which are projective. We have not yet shown that they are indecomposable.

We easily compute that

$$(1,2,3)e_1 = e_1, \quad (1,2,3)e_2 = \omega^2 e_2, \quad (1,2,3)e_3 = \omega e_3$$

and from this we see that $K \cdot \mathbb{F}_4 e_i = \mathbb{F}_4 e_i$ for all i. Since $S_3 = K \cup (1,2)K$ we have $\mathbb{F}_4 S_3 e_i = \mathbb{F}_4 e_i \oplus \mathbb{F}_4 (1,2) e_i$, which has dimension 2 for all i. We have already seen that when $i = 2$ or 3, e_i is an eigenvector for $(1,2,3)$ with eigenvalue ω or ω^2, and a similar calculation shows that the same is true for $(1,2)e_i$. Thus when $i = 2$ or 3, $\mathbb{F}_4 S_3 e_i$ has no trivial submodule and hence is simple by the observations made at the start of this example. We have an isomorphism of $\mathbb{F}_4 S_3$-modules

$$\begin{aligned} \mathbb{F}_4 S_3 e_2 &\to \mathbb{F}_4 S_3 e_3 \\ e_2 &\mapsto (1,2) e_3 \\ (1,2) e_2 &\mapsto e_3. \end{aligned}$$

On the other hand $\mathbb{F}_4 S_3 e_1$ has fixed points $\mathbb{F}_4 \sum_{g \in S_3} g$ of dimension 1 and so has two composition factors, which are trivial. On restriction to $\mathbb{F}_4 \langle (1,2) \rangle$ it is the regular representation, and it is a uniserial module.

We see from all this that $\mathbb{F}_4 S_3 = \begin{smallmatrix} 1 \\ 1 \end{smallmatrix} \oplus 2 \oplus 2$, in a diagrammatic notation. Thus the 2-dimensional simple $\mathbb{F}_4 S_3$-module is projective, and the trivial module appears as the unique simple quotient of a projective module of dimension 2 whose socle is also the trivial module. These summands of $\mathbb{F}_4 S_3$ are indecomposable, and so e_1, e_2 and e_3 are primitive idempotents in $\mathbb{F}_4 S_3$. We see also that the radical of $\mathbb{F}_4 S_3$ is the span of $\sum_{g \in S_3} g$. □

We now develop the theory of projective covers. We first make the definition that an *essential epimorphism* is an epimorphism of modules $f : U \to V$ with the property that no proper submodule of U is mapped surjectively onto V by f. An equivalent formulation is that whenever $g : W \to U$ is a map such that fg is an epimorphism, then g is an epimorphism. One immediately asks for examples of essential epimorphisms, but it is probably more instructive to consider epimorphisms which are not essential. If $U \to V$ is any epimorphism and X is a non-zero module then the epimorphism $U \oplus X \to V$ which is zero on X can never be essential because U is a submodule of $U \oplus X$ mapped surjectively onto V. Thus if $U \to V$ is essential then U can have no direct summands which are mapped to zero. One may think of an essential epimorphism as being minimal, in that no unnecessary parts of U are present. The greatest source of essential epimorphisms is Nakayama's lemma.

(7.6) THEOREM (Nakayama's Lemma). *If U is any Noetherian module, the homomorphism $U \to U/\operatorname{Rad} U$ is essential.*

Proof. Suppose V is a submodule of U. If $V \neq U$ then $V \subseteq M \subset U$ where M is a maximal submodule of U. Now $V + \operatorname{Rad} U \subseteq M$ and so the composite $V \to U \to U/\operatorname{Rad} U$ has image contained in $M/\operatorname{Rad} U$, which is not equal to $U/\operatorname{Rad} U$ since $(U/\operatorname{Rad} U)/(M/\operatorname{Rad} U) \cong U/M \neq 0$. □

Evidently an equivalent way to state Nakayama's lemma is that if V is a submodule of U with the property that $V + \operatorname{Rad} U = U$, then $V = U$.

As an example of an essential epimorphism we could consider the indecomposable kG-module U_r of dimension r, where k is a field of characteristic p and G is cyclic of order p^n. Since U_r has a unique maximal submodule, of codimension 1, the epimorphism $U_r \to U_1$ is essential, by Nakayama's lemma.

The next result is not at all difficult and could usefully be proved as an exercise.

(7.7) PROPOSITION.

(a) *Suppose that $f : U \to V$ and $g : V \to W$ are two module homomorphsms. If two of f, g and gf are essential epimorphisms then so is the third.*

(b) *Let $f : U \to V$ be a homomorphism of modules for a finite-dimensional algebra over a field. Then f is an essential epimorphism if and only if the homomorphism of radical quotients $U/\operatorname{Rad} U \to V/\operatorname{Rad} V$ is an isomorphism.*

(c) *Let $f_i : U_i \to V_i$ be homomorphisms of modules for a finite-dimensional algebra over a field, where $i = 1, \ldots, n$. The f_i are all essential epimorphisms if and only if*

$$\oplus f_i : \bigoplus_i U_i \to \bigoplus_i V_i$$

is an essential epimorphism.

Proof. (a) Suppose f and g are essential epimorphisms. Then gf is an epimorphism also, and it is essential because if U_0 is a proper submodule of U then $f(U_0)$ is a proper submodule of V since f is essential, and hence $g(f(U_0))$ is a proper submodule of S since g is essential.

Next suppose f and gf are essential epimorphisms. Since $W = \mathrm{Im}(gf) \subseteq \mathrm{Im}(g)$ it follows that g is an epimorphism. If V_0 is a proper submodule of V then $f^{-1}(V_0)$ is a proper submodule of U since f is an epimorphism, and now $g(V_0) = gf(f^{-1}(V_0))$ is a proper submodule of S since gf is essential.

Suppose that g and gf are essential epimorphisms. If f were not an epimorphism then $f(U)$ would be a proper submodule of V, so $gf(U)$ would be a proper submodule of W since gf is essential. Since $gf(U) = W$ we conclude that f is an epimorphism. If U_0 is a proper submodule of U then $gf(U_0)$ is a proper submodule of W, since gf is essential, so $f(U_0)$ is a proper submodule of V since g is an epimorphism. Hence f is essential.

(b) Consider the commutative square

$$\begin{array}{ccc} U & \longrightarrow & V \\ \downarrow & & \downarrow \\ U/\operatorname{Rad} U & \longrightarrow & V/\operatorname{Rad} V \end{array}$$

where the vertical homomorphisms are essential epimorphisms by Nakayama's lemma. Now if either of the horizontal arrows is an essential epimorphism then so is the other, using part (a). The bottom arrow is an essential epimorphism if and only if it is an isomorphism; for $U/\operatorname{Rad} U$ is a semisimple module and so the kernel of the map to $V/\operatorname{Rad} V$ has a direct complement in $U/\operatorname{Rad} U$, which maps onto $V/\operatorname{Rad} V$. Thus if $U/\operatorname{Rad} U \to V/\operatorname{Rad} V$ is an essential epimorphism its kernel must be zero and hence it must be an isomorphism.

(c) The map

$$(\oplus_i U_i)/\operatorname{Rad}(\oplus_i U_i) \to (\oplus_i V_i)/\operatorname{Rad}(\oplus_i V_i)$$

induced by $\oplus f_i$ may be identified as a map

$$\bigoplus_i (U_i/\operatorname{Rad} U_i) \to \bigoplus_i (V_i/\operatorname{Rad} V_i),$$

and it is an isomorphism if and only if each map $U_i/\operatorname{Rad} U_i \to V_i/\operatorname{Rad} V_i$ is an isomorphism. These conditions hold if and only if $\oplus f_i$ is an essential epimorphism, if and only if each f_i is an essential epimorphism by part (b). □

We define a *projective cover* of a module U to be an essential epimorphism $P \to U$, where P is a projective module. Strictly speaking the projective cover is the homomorphism, but we may also refer to the module P as the projective cover of U. We are justified in calling it *the* projective cover by the second part of the following result, which says that projective covers (if they exist) are unique.

(7.8) PROPOSITION.

(1) Suppose that $f : P \to U$ is a projective cover of a module U and $g : Q \to U$ is an epimorphism where Q is a projective module. Then we may write $Q = Q_1 \oplus Q_2$ so that g has components $g = (g_1, 0)$ with respect to this direct sum decomposition and $g_1 : Q_1 \to U$ appears in a commutative triangle

$$\begin{array}{ccc} & & Q_1 \\ & \overset{\gamma}{\swarrow} & \big\downarrow g_1 \\ P & \xrightarrow{f} & U \end{array}$$

where γ is an isomorphism.

(2) If any exist, the projective covers of a module U are all isomorphic, by isomorphisms which commute with the essential epimorphisms.

Proof. (1) In the diagram

$$\begin{array}{ccc} & & Q \\ & & \big\downarrow g \\ P & \xrightarrow{f} & U \end{array}$$

we may lift in both directions to obtain maps $\alpha : P \to Q$ and $\beta : Q \to P$ so that the two triangles commute. Now $f\beta\alpha = g\alpha = f$ is an epimorphism, so $\beta\alpha$ is also an epimorphism since f is essential. Thus β is an epimorphism. Since P is projective β splits and $Q = Q_1 \oplus Q_2$ where $Q_2 = \operatorname{Ker}\beta$, and β maps Q_1 isomorphically to P. Thus $g = (f\beta|_{Q_1}, 0)$ is as claimed with $\gamma = \beta|_{Q_1}$.

(2) Supposing that $f : P \to U$ and $g : Q \to U$ are both projective covers, since Q_1 is a submodule of Q which maps onto U and f is essential we deduce that $Q = Q_1$. Now $\gamma : Q \to P$ is the required isomorphism. □

(7.9) COROLLARY. *If P and Q are Noetherian projective modules over a ring then $P \cong Q$ if and only if $P/\operatorname{Rad} P \cong Q/\operatorname{Rad} Q$.*

Proof. By Nakayama's lemma P and Q are the projective covers of $P/\operatorname{Rad} P$ and $Q/\operatorname{Rad} Q$. It is clear that if P and Q are isomorphic then so are $P/\operatorname{Rad} P$ and $Q/\operatorname{Rad} Q$, and conversely if these quotients are isomorphic then so are their projective covers, by uniqueness of projective covers. □

If now P and Q are projective modules for a finite-dimensional algebra A over a field the radical quotients $P/\operatorname{Rad} P$ and $Q/\operatorname{Rad} Q$ are semisimple, and to classify the indecomposable projectives it will suffice to classify these semisimple quotients, by Corollary 7.9. We will see in this case that if P is an indecomposable projective A-module then it is isomorphic to a module Af for some primitive idempotent $f \in A$, and the quotient $P/\operatorname{Rad} P$ is isomorphic to $(A/\operatorname{Rad} A)e$ for some primitive idempotent e of $A/\operatorname{Rad} A$ where $e = f + \operatorname{Rad} A$.

In general if I is an ideal of a ring A and f is an idempotent of A then clearly $f + I$ is also an idempotent of A/I. On the other hand, given an idempotent e of A/I, if we can always find an idempotent $f \in A$ such that $e = f + I$ we say we can *lift idempotents* from A/I to A.

We state the next results about lifting idempotents in the context of a ring with a nilpotent ideal I, but readers familiar with completions will recognize that these results extend to a situation where A is complete with respect to the I-adic topology on A.

(7.10) THEOREM. *Let I be a nilpotent ideal of a ring A and e an idempotent in A/I. Then there exists an idempotent $f \in A$ with $e = f + I$. If e is primitive, so is f.*

Proof. We define idempotents $e_i \in A/I^i$ inductively such that $e_i + I^{i-1}/I^i = e_{i-1}$ for all i, starting with $e_1 = e$. Suppose that e_{i-1} is an idempotent of A/I^{i-1}. Pick any element $a \in A/I^i$ mapping onto e_{i-1}, so that $a^2 - a \in I^{i-1}/I^i$. Since $(I^{i-1})^2 \subseteq I^i$ we have $(a^2 - a)^2 = 0 \in A/I^i$. Put $e_i = 3a^2 - 2a^3$. This does map to $e_{i-1} \in A/I^{i-1}$ and we have

$$\begin{aligned} e_i^2 - e_i &= (3a^2 - 2a^3)(3a^2 - 2a^3 - 1) \\ &= -(3 - 2a)(1 + 2a)(a^2 - a)^2 \\ &= 0. \end{aligned}$$

This completes the inductive definition, and if $I^r = 0$ we put $f = e_r$.

Suppose that e is primitive and that f can be written $f = f_1 + f_2$ where f_1 and f_2 are orthogonal idempotents. Then $e = e_1 + e_2$, where $e_i = f_i + I$, is also a sum of orthogonal idempotents. Therefore one of these is zero, say, $e_1 = 0 \in A/I$. This means that $f_1^2 = f_1 \in I$. But I is nilpotent, and so contains no non-zero idempotent. □

We will very soon see in the situation of 7.10 that it is also true that if f is primitive, so is e.

(7.11) COROLLARY. *Let I be a nilpotent ideal of a ring A and let $1 = e_1 + \cdots + e_n$ be a sum of orthogonal idempotents in A/I. Then we can write $1 = f_1 + \cdots + f_n$ in A, where the f_i are orthogonal idempotents such that $f_i + I = e_i$ for all i. If the e_i are primitive then so are the f_i.*

Proof. We proceed by induction on n, the induction starting when $n = 1$. Suppose that $n > 1$ and the result holds for smaller values of n. We will write $1 = e_1 + E$ in A/I where

$E = e_2 + \cdots + e_n$ is an idempotent orthogonal to e_1, and by Theorem 7.10 we may lift e_1 to an idempotent $f_1 \in A$. Write $F = 1 - f_1$, so that F is an idempotent which lifts E. Now F is the identity element of the ring FAF which has a nilpotent ideal FIF. The composite homomorphism $FAF \hookrightarrow A \to A/I$ has kernel $FAF \cap I$ and this equals FIF, since clearly $FAF \cap I \supseteq FIF$, and if $x \in FAF \cap I$ then $x = FxF \in FIF$, so $FAF \cap I \subseteq FIF$. Inclusion of FAF in A thus induces a monomorphism $FAF/FIF \to A/I$, and its image is $E(A/I)E$. In $E(A/I)E$ the identity element E is the sum of $n-1$ orthogonal idempotents, and this expression is the image of a similar expression for $F + FIF$ in FAF/FIF. By induction, there is a sum of orthogonal idempotents $F = f_2 + \cdots + f_n$ in FAF which lifts the expression in FAF/FIF and hence also lifts the expression for E in A/I, so we have idempotents $f_i \in A$, $i = 1, \ldots, n$ with $f_i + I = e_i$. These f_i are orthogonal; for $f_2, \ldots, f_n$ are orthogonal in FAF by induction, and if $i > 1$ then $Ff_i = f_i$ so we have $f_1 f_i = f_1 F f_i = 0$.

The final assertion about primitivity is the last statement of 7.10. □

(7.12) COROLLARY. *Let f be an idempotent in a ring A which has a nilpotent ideal I. Then f is primitive if and only if $f + I$ is primitive.*

Proof. We have seen in 7.10 that if $f + I$ is primitive, then so is f. Conversely, if $f + I$ can be written $f + I = e_1 + e_2$ where the e_i are orthogonal idempotents of A/I, then by applying 7.11 to the ring fAf (of which f is the identity) we may write $f = g_1 + g_2$ where the g_i are orthogonal idempotents of A which lift the e_i. □

We now classify the indecomposable projective modules over a finite-dimensional algebra as the projective covers of the simple modules. We first describe how these projective covers arise, and then show that they exhaust the possibilities for indecomposable projective modules. We postpone explicit examples until the next section, in which we consider group algebras.

(7.13) THEOREM. *Let A be a finite-dimensional algebra over a field. For each simple module S there is an indecomposable projective module P_S with $P_S/\operatorname{Rad} P_S \cong S$. It follows that P_S is the projective cover of S, and is uniquely determined up to isomorphism by this property. The projective module P_S has the form $P_S = Af$ where f is a primitive idempotent with the property that $fS \neq 0$, and if T is any simple module not isomorphic to S then $fT = 0$.*

Proof. Let $e \in A/\operatorname{Rad} A$ be any primitive idempotent such that $eS \neq 0$, and let f be any lift of e to A. Then $fS \neq 0$ and f is primitive. We define $P_S = Af$, an indecomposable projective module. Now

$$P_S/\operatorname{Rad} P_S = Af/\operatorname{Rad} A \cdot Af \cong (A/\operatorname{Rad} A) \cdot (f + \operatorname{Rad} A) = S$$

the isomorphism arising because the map $Af \to (A/\operatorname{Rad} A)\cdot(f+\operatorname{Rad} A)$ defined by $af \mapsto (af+\operatorname{Rad} A)$ has kernel $(\operatorname{Rad} A)\cdot f$. We have $fS = eS \neq 0$ and $fT = eT = 0$ if $T \ncong S$ since a primitive idempotent e in the semisimple ring $A/\operatorname{Rad} A$ is non-zero on a unique isomorphism class of simple modules. □

(7.14) THEOREM. *Let A be a finite-dimensional algebra over a field k. Up to isomorphism, the indecomposable projective A-modules are exactly the modules P_S which are the projective covers of the simple modules, and $P_S \cong P_T$ if and only if $S \cong T$. Each projective P_S appears as a direct summand of the regular representation, with multiplicity equal to the multiplicity of S as a summand of $kG/\operatorname{Rad}(kG)$. If k is algebraically closed we have*

$$A \cong \bigoplus_{\text{simple } S} (P_S)^{\dim S}.$$

Proof. Let P be an indecomposable projective module and write

$$P/\operatorname{Rad} P \cong S_1 \oplus \cdots \oplus S_n.$$

Then $P \to S_1 \oplus \cdots \oplus S_n$ is a projective cover. Now

$$P_{S_1} \oplus \cdots \oplus P_{S_n} \to S_1 \oplus \cdots \oplus S_n$$

is also a projective cover, and by uniqueness of projective covers we have

$$P \cong P_{S_1} \oplus \cdots \oplus P_{S_n}.$$

Since P is indecomposable we have $n = 1$ and $P \cong P_{S_1}$.

Suppose that each simple A module S occurs with multiplicity n_S as a summand of the semisimple ring $A/\operatorname{Rad} A$. Both A and $\bigoplus_{\text{simple } S} P_S^{n_S}$ are the projective cover of $A/\operatorname{Rad} A$, and so they are isomorphic. It is always the case that $n_S \neq 0$, and when k is algebraically closed $n_S = \dim S$. □

(7.15) THEOREM. *Let A be a finite-dimensional algebra over a field k, and U a finitely-generated A-module. Then U has a projective cover.*

Proof. Since $U/\operatorname{Rad} U$ is semisimple we may write $U/\operatorname{Rad} U = S_1 \oplus \cdots \oplus S_n$, where the S_i are simple modules. Let P_{S_i} be the projective cover of S_i and $h : P_{S_1} \oplus \cdots \oplus P_{S_n} \to U/\operatorname{Rad} U$ the projective cover of $U/\operatorname{Rad} U$. By projectivity there exists a homomorphism f such that the following diagram commutes:

$$\begin{array}{ccc} & & P_{S_1} \oplus \cdots \oplus P_{S_n} \\ & \overset{f}{\swarrow} & \big\downarrow h \\ U & \xrightarrow{g} & U/\operatorname{Rad} U \end{array}.$$

Since both g and h are essential epimorphisms, so is f by 7.7. Therefore f is a projective cover. □

We should really learn more from 7.15 than simply that U has a projective cover: the projective cover of U is the same as the projective cover of $U/\operatorname{Rad} U$.

(7.16) *Example.* The arguments which show the existence of projective covers have a sense of inevitability about them and we may get the impression that projective covers always exist in arbitrary situations. In fact they fail to exist in general for integral group rings. If $G = \{e, g\}$ is a cyclic group of order 2, consider the submodule $3\mathbb{Z} \cdot e + \mathbb{Z} \cdot (e + g)$ of $\mathbb{Z}G$ generated as an abelian group by $3e$ and $e + g$. We rapidly check that this subgroup is invariant under the action of G, and is a $\mathbb{Z}G$-submodule, and it is not the whole of $\mathbb{Z}G$ since it does not contain e. Applying the augmentation map $\epsilon : \mathbb{Z}G \to \mathbb{Z}$ we have $\epsilon(3e) = 3$ and $\epsilon(e + g) = 2$ so $\epsilon(3\mathbb{Z} \cdot e + \mathbb{Z} \cdot (e + g)) = 3\mathbb{Z} + 2\mathbb{Z} = \mathbb{Z}$, and thus ϵ is an epimorphism which is not essential. If $\mathbb{Z}$ were to have a projective cover it would be a proper summand of $\mathbb{Z}G$ by 7.8. On reducing modulo 2 we would deduce that $\mathbb{F}_2G$ decomposes, which we know not to be the case. □

Now that we have classified the projective modules for a finite-dimensional algebra we turn to one of their important uses, which is to determine the multiplicity of a simple module S as a composition factor of an arbitrary module U (with a composition series). If

$$0 = U_0 \subset U_1 \subset \cdots \subset U_n = U$$

is any composition series of U, the number of quotients U_i/U_{i-1} isomorphic to S is determined independently of the choice of composition series, by the Jordan-Hölder theorem. We call this number the *(composition factor) multiplicity* of S in U.

(7.17) PROPOSITION. *Let S be a simple module for a finite-dimensional algebra A with projective cover P_S, and let U be a finite-dimensional A-module.*
(1) If T is a simple A-module then

$$\dim \operatorname{Hom}_A(P_S, T) = \begin{cases} \dim \operatorname{End}_A(S) & \text{if } S \cong T, \\ 0 & \text{otherwise.} \end{cases}$$

(2) The multiplicity of S as a composition factor of U is

$$\dim \operatorname{Hom}_A(P_S, U)/\dim \operatorname{End}_A(S).$$

(3) If $e \in A$ is an idempotent then $\dim \operatorname{Hom}_A(Ae, U) = \dim eU$.

Proof. (1) If $P_S \to T$ is any non-zero homomorphism, the kernel must contain $\operatorname{Rad} P_S$, being a maximal submodule of S. Since $P_S/\operatorname{Rad} P_S \cong S$ is simple, the kernel must be $\operatorname{Rad} P_S$ and $S \cong T$. Every homomorphism $P_S \to S$ is the composite $P_S \to P_S/\operatorname{Rad} P_S \to S$ of the quotient map and either an isomorphism of $P_S/\operatorname{Rad} P_S$ with S or the zero map. This gives an isomorphism $\operatorname{Hom}_A(P_S, S) \cong \operatorname{End}_A(S)$.

(2) Let

$$0 = U_0 \subset U_1 \subset \cdots \subset U_n = U$$

be a composition series of U. We prove the result by induction on the composition length n, the case $n = 1$ having just been established. Suppose $n > 1$ and that the multiplicity of S in U_{n-1} is $\dim \mathrm{Hom}_A(P_S, U_{n-1})/\dim \mathrm{End}_A(S)$. The exact sequence

$$0 \to U_{n-1} \to U \to U/U_{n-1} \to 0$$

gives rise to an exact sequence

$$0 \to \mathrm{Hom}_A(P_S, U_{n-1}) \to \mathrm{Hom}_A(P_S, U) \to \mathrm{Hom}_A(P_S, U/U_{n-1}) \to 0$$

by 7.3, so that

$$\dim \mathrm{Hom}_A(P_S, U) = \dim \mathrm{Hom}_A(P_S, U_{n-1}) + \dim \mathrm{Hom}_A(P_S, U/U_{n-1}).$$

Dividing these dimensions by $\dim \mathrm{End}_A(S)$ gives the result, by part (1).

(3) There is an isomorphism of vector spaces $\mathrm{Hom}_A(Ae, U) \cong eU$ specified by $\phi \mapsto \phi(e)$. Note here that since $\phi(e) = \phi(ee) = e\phi(e)$ we must have $\phi(e) \in eU$. This mapping is injective since each A-module homomorphism $\phi : Ae \to U$ is determined by its value on e as $\phi(ae) = a\phi(e)$. It is surjective since the equation just written down does define a module homomorphism for each choice of $\phi(e) \in eU$. □

Notice in 7.17 that if the field over which A is defined is algebraically closed then $\dim \mathrm{End}_A(S) = 1$, by Schur's lemma, so that the multiplicity of S in U is just $\dim \mathrm{Hom}_A(P_S, U)$.

Again in the context of a finite-dimensional algebra A, we define for each pair of simple A-modules S and T the integer

$$c_{ST} = \text{the composition factor multiplicity of } S \text{ in } P_T.$$

These are called the *Cartan invariants* of A, and they form a matrix $C = (c_{ST})$ with rows and columns indexed by the isomorphism types of simple A-modules, called the *Cartan matrix* of A.

(7.18) COROLLARY. *Let A be a finite-dimensional algebra over a field, let S and T be simple A-modules and let e_S, e_T be idempotents so that $P_S = Ae_S$ and $P_T = Ae_T$ are projective covers of S and T. Then*

$$c_{ST} = \dim \mathrm{Hom}_A(P_S, P_T)/\dim \mathrm{End}_A(S) = \dim e_S A e_T/\dim \mathrm{End}_A(S).$$

While it is rather weak information just to know the composition factors of the projective modules, this is at least a start in describing these modules, and the information may be conveniently displayed as a matrix. We will see later on in the case of group algebras that there is an extremely effective way of computing the Cartan matrix using the decomposition matrix.

Exercises for Section 7.

1. Let A be a finite-dimensional algebra over a field. Show that A is semisimple if and only if all finite-dimensional A-modules are projective.

2. Suppose that we have module homomorphisms $U \xrightarrow{f} V \xrightarrow{g} W$. Show that part of Proposition 7.6(a) can be strengthened to say the following: if gf is an essential epimorphism and f is an epimorphism then both f and g are essential epimorphisms.

3. In this question U, V and W are modules for a finite-dimensional algebra over a field.
(a) Show that $U \to W$ is an essential epimorphism if and only if U is a homomorphic image of P_W in such a way that the composite $P_W \to U \to W$ is the projective cover of W.
(b) Prove the following 'extension and converse' to Nakayama's lemma: let V be any submodule of U. Then $U \to U/V$ is an essential epimorphism $\Leftrightarrow V \subseteq \operatorname{Rad} U$.

4. Let P_S be an indecomposable projective module for a finite-dimensional algebra over a field. Show that every homomorphic image of P_S
(a) has a unique maximal submodule, and
(b) is indecomposable.

5. Let A be a finite-dimensional algebra over a field, and suppose that f, f' are primitive idempotents of A. Show that the indecomposable projective modules Af and Af' are isomorphic if and only if $fS = f'S$ for every simple module S.

6. Let A be a finite-dimensional algebra over a field, and suppose that Q is a projective A-module. Show that in any expression

$$Q = P_{S_1}^{n_1} \oplus \cdots \oplus P_{S_r}^{n_r}$$

where $S_1, \ldots, S_r$ are non-isomorphic simple modules, we have

$$n_i = \dim \operatorname{Hom}_A(Q, S_i) / \dim \operatorname{End}_A(S_i).$$

7. Let A be a finite-dimensional algebra over a field. Suppose that V is an A-module, and that a certain simple A-module S occurs as a composition factor of V with multiplicity 1. Suppose that there exist non-zero homomorphisms $S \to V$ and $V \to S$. Prove that S is a direct summand of V.

8. Let $G = S_n$, let k be a field of characteristic 2 and let $\Omega = \{1, 2, \ldots, n\}$ permuted transitively by G.

(a) When $n = 3$, show that the permutation module $k\Omega$ is semisimple, being the direct sum of the one-dimensional trivial module and the 2-dimensional simple module.

(b) When $n = 4$ there is a normal subgroup $V \lhd S_4$ with $S_4/V \cong S_3$, where $V = \langle (1,2)(3,4), (1,3)(2,4) \rangle$. The simple kS_4-modules are precisely the two simple kS_3-modules, made into kS_4-modules via the quotient homomorphism to S_3. Show that $k\Omega$ is uniserial with three composition factors which are the trivial module, the 2-dimensional simple module and the trivial module.
[Use Exercise 18 from Section 6.]

8. Projective modules for group algebras

This section is a mix of general facts about group algebras and specific examples to do with certain types of group. We start with a summary of the situation for p-groups over a field of characteristic p, much of which we have already seen.

(8.1) THEOREM. *Let k be a field of characteristic p and G a p-group. The regular representation is an indecomposable projective module, which is the projective cover of the trivial representation. Every finitely generated projective module is free. The only idempotents in kG are 0 and 1.*

Proof. We have seen in 6.8 that $\mathrm{Rad}(kG) = IG$ and $kG/\mathrm{Rad}(kG) \cong k$. It follows immediately that kG is indecomposable, either directly by arguing that $kG = U \oplus V$ would imply $k = U/\mathrm{Rad}\, U \oplus V/\mathrm{Rad}\, V$, or using the theory of Section 7. By Nakayama's lemma kG is the projective cover of k. By 7.13 and 6.3 every indecomposable projective is isomorphic to kG. Every finitely generated projective is a direct sum of indecomposable projectives, and so is free. Finally, every idempotent $e \in kG$ gives a module decomposition $kG = kGe \oplus kG(1-e)$. If $e \neq 0$ then we must have $kG = kGe$, so $kG(1-e) = 0$ and $e = 1$. □

We can deduce from this some information about projective modules for arbitrary groups, using the following lemma, which is valid over an arbitrary commutative ring R.

(8.2) LEMMA. *Let H be a subgroup of G.*
(1) If P is a projective RG-module then $P\downarrow_H^G$ is a projective RH-module.
(2) If Q is a projective RH-module then $Q\uparrow_H^G$ is a projective RG-module.

Proof. (1) As a RH-module,

$$RG\downarrow_H \cong \bigoplus_{g\in[H\backslash G]} RHg \cong (RH)^{|G:H|}$$

which is a free module. Hence a direct summand of RG^n on restriction to H is a direct summand of $RH^{|G:H|n}$, which is again projective.

(2) We have

$$(RH)\uparrow_H^G \cong (R\uparrow_1^H)\uparrow_H^G \cong R\uparrow_1^G \cong RG$$

so that direct summands of RH^n induce to direct summands of RG^n. □

(8.3) COROLLARY. *Let k be a field of characteristic p and let p^a be the exact power of p which divides $|G|$. If P is a projective kG-module then $p^a \mid \dim P$.*

Proof. Let H be a Sylow p-subgroup of G and P a projective kG-module. Then $P\downarrow_H^G$ is projective by 8.2, hence free as a kH-module by 8.1, and of dimension a multiple of $|H|$. □

We now examine in detail the projective modules for several specific kinds of groups. The following result will be used in constructing these modules. It is valid over an arbitrary commutative ring R.

(8.4) PROPOSITION. *Suppose that V is any RG-module which is free as an R-module and P is a projective RG-module. Then $V \otimes_R P$ is projective.*

Proof. If $P \oplus P' \cong RG^n$ then $V \otimes RG^n \cong V \otimes P \oplus V \otimes P'$ and it suffices to show that $V \otimes RG^n$ is free. We offer two proofs of the fact that $V \otimes RG \cong RG^{\operatorname{rank} V}$. The first is that $V \otimes RG \cong V \otimes (R \uparrow_1^G) \cong (V \otimes R) \uparrow_1^G \cong V \uparrow_1^G$. As a module for the identity group, V is just a free R-module and so $V \uparrow_1^G \cong (R \uparrow_1^G)^{\operatorname{rank} V} \cong RG^{\operatorname{rank} V}$.

The second proof is really the same as the first, but we make the isomorphism explicit. Let V^{triv} be the same R-module as V, but with the trivial G-action, so $V^{\mathrm{triv}} \cong R^{\operatorname{rank} V}$ as RG-modules. We define a linear map

$$\begin{array}{c} V \otimes RG \to V^{\mathrm{triv}} \otimes RG \\ v \otimes g \mapsto g^{-1}v \otimes g \end{array},$$

which has inverse $gw \otimes g \leftarrow w \otimes g$. One checks that these mutually inverse linear maps are RG-module homomorphisms. Finally $V^{\mathrm{triv}} \otimes RG \cong RG^{\operatorname{rank} V}$. □

In the calculations which follow we will need to use the fact that for representations over a field, taking the Kronecker product with a fixed representation preserves exactness.

(8.5) LEMMA. *Let $0 \to U \to V \to W \to 0$ be a short exact sequence of kG-modules and X another kG-module, where k is a field. Then the sequence*

$$0 \to U \otimes_k X \to V \otimes_k X \to W \otimes_k X \to 0$$

is exact. Thus if U is a submodule of V then $(V/U) \otimes_k X \cong (V \otimes_k X)/(U \otimes_k X)$.

Proof. The exactness is a question of linear algebra which is independent of the group action. For the reader who knows a little homological algebra, the result is equivalent to the statement that higher Tor groups vanish over a field. We may also give a more direct approach by taking bases for the modules concerned. We may suppose that U is a submodule of V. Let $v_1, \ldots, v_n$ be a basis for V such that $v_1, \ldots, v_d$ is a basis for U and let $x_1, \ldots, x_m$ be a basis for X. Now the $v_i \otimes_k x_j$ with $1 \le i \le n$ and $1 \le j \le m$ form a basis for $V \otimes_k X$, and the same elements with $1 \le i \le d$ and $1 \le j \le m$ form a basis for $U \otimes_k X$. This shows that $U \otimes_k X$ is a submodule of $V \otimes_k X$, and the quotient has as a basis the images of the $v_i \otimes_k x_j$ with $d+1 \le i \le n$ and $1 \le j \le m$, which is in bijection with a basis of $W \otimes_k X$. □

(8.6) *Example.* We describe the projective kG-modules where k is a field of characteristic p and $G = H \times K$ where H is a p-group and K has order prime to p. Following this example we will consider projective modules for the semidirect products $H \rtimes K$ and $K \rtimes H$ and the observations we will make when we do this also apply to the direct product. However, it seems profitable to consider the simpler example first.

We make use of the following general isomorphism (not dependent on the particular hypotheses we have here):

$$k[H \times K] \cong kH \otimes kK \quad \text{as } k\text{-algebras},$$

which arises because kG has as a basis the elements (h, k) where $h \in H$, $k \in K$, and $kH \otimes kK$ has as a basis the corresponding elements $h \otimes k$. These two bases multiply together in the same fashion, and so we have an algebra isomorphism. In this calculation the only tensor product which will appear is tensor product over the field k. We next observe that

$$\operatorname{Rad} kG = \operatorname{Rad} kH \otimes kK.$$

This is because the quotient

$$(kH \otimes kK)/(\operatorname{Rad} kH \otimes kK) \cong (kH/\operatorname{Rad} kH) \otimes kK \cong k \otimes kK$$

is semisimple, since kK is semisimple, so that

$$\operatorname{Rad}(kH \otimes kK) \subseteq \operatorname{Rad} kH \otimes kK.$$

On the other hand $\operatorname{Rad} kH \otimes kK$ is a nilpotent ideal of $kH \otimes kK$, so is contained in the radical, and we have equality.

Let us write $kK = S_1^{n_1} \oplus \cdots \oplus S_r^{n_r}$, where $S_1, \ldots, S_r$ are the non-isomorphic simple kK-modules. Since $H = O_p(G)$, these are also the non-isomorphic simple kG-modules. We have

$$kG = kH \otimes kK = (kH \otimes S_1)^{n_1} \oplus \cdots \oplus (kH \otimes S_r)^{n_r}$$

and so the $kH \otimes S_i$ are projective kG-modules. Each occurs with multiplicity equal to the multiplicity of S_i as a summand of $kG/\operatorname{Rad}(kG)$, and so must be indecomposable, using 7.13. We have therefore constructed all the indecomposable projective kG-modules, and they are the modules $P_{S_i} = kH \otimes S_i$.

Suppose that $0 \subset P_1 \subset \cdots \subset P_n = kH$ is a composition series of the regular representation of H. Since H is a p-group, all the composition factors are the trivial representation, k. Because $\_\_ \otimes_k S_i$ preserves exact sequences, the series $0 \subset P_1 \otimes S_i \subset \cdots \subset P_n \otimes S_i = P_{S_i}$ has quotients $k \otimes S_i = S_i$, which are simple, and so this is a composition series of P_{S_i}.

As an example, suppose that H is cyclic of order p^s. Then $kH = U_{p^s}$ has a composition series in which $P_j = \operatorname{Rad}(kH)^j \cdot kH \cong U_j$ and from the description of the radical of kG we see that the terms in the composition series of P_{S_i} are $P_j \otimes S_i = \operatorname{Rad}(kG)^j \cdot P_{S_i}$. Because

the radical series is in fact a composition series, it follows (as in Exercise 5 to Section 6) that this is the unique composition series of P_{S_i}, and that there are no more submodules of P_{S_i} other than the ones listed.

We move on now to describe the projective kG-modules where k is a field of characteristic p and $G = H \rtimes K$ where H is a p-group and $|K|$ is prime to p. The last example is a special case of this situation, and so the results about to be obtained also apply in that case. However, our results will be less specific than in 8.6. Here, again, $H = O_p(G)$, and so the simple kG-modules are precisely the simple kK-modules. Since G acts on these via the ring surjection $kG \to kK$, the kernel of this map acts as zero on all simple modules and so is contained in the radical. But also kK is a semisimple ring, so the kernel is the radical, and in particular it is a nilpotent ideal. (The kernel is in fact the ideal $kG \cdot IH$ considered in Exercise 10 of Section 6, but we do not need this here.) The idempotent $e_1 = \frac{1}{|K|} \sum_{g \in K} g$ is the primitive idempotent of kK which projects onto the unique 1-dimensional simple summand of kK. It is already an idempotent in kG, so it is its own lift to kG, and hence it is primitive in kG by 7.9. We conclude that $P_k = kGe_1$, by 7.12. This identifies P_k as a reasonably explicit subset of kG, but we now do better than this.

(8.7) PROPOSITION. *Let k be a field of characteristic p and let $G = H \rtimes K$ where H is a p-group and K has order prime to p. Then $P_k \cong kH$ where H acts on kH by left multiplication and K acts by conjugation.*

Proof. It comes as a surprise that there should be an action of G on kH in the manner specified. Explicitly, if $\sum_{g \in H} a_g g$, $x \in H$ and $y \in K$ then $x \sum_{g \in H} a_g g = \sum_{g \in H} a_g xg$ and $y \sum_{g \in H} a_g g = \sum_{g \in H} a_g ygy^{-1}$. We could verify that this does give an action of G on kH, but instead we show that G acts on P_k via these formulae. We have $kG = kH \cdot kK$ and $kKe_1 = ke_1$, so $P_k \cong kGe_1 = kHe_1$. We claim that $kHe_1 \cong kH$ as k-vector spaces via an isomorphism in which he_1 corresponds to h. Indeed the elements he_1 are independent as h ranges through H, so we have just specified a bijection between two bases. Now H and K act on kHe_1 as $x \cdot he_1 = xhe_1$ for $x \in H$ and $y \cdot he_1 = yhy^{-1}ye_1 = yhy^{-1}e_1$ for $y \in K$. Identifying kHe_1 with kH, these actions are as specified in the statement of the result. □

We should point out that whenever we have a semidirect product $G = H \rtimes K$ there is an action of G on kH in the way we have just described, but in general if H is not a Sylow p-subgroup of G this module will not be P_k.

(8.8) PROPOSITION. *Let k be a field of characteristic p and let $G = H \rtimes K$ where H is a p-group and K has order prime to p. If S is any simple kG-module then $P_S \cong P_k \otimes S$. There is an isomorphism of kG-modules $P_k \otimes kK \cong kG$.*

Proof. By 8.4 $P_k \otimes S$ is projective. Tensoring the epimorphism $P_k \to k$ with S gives an epimorphism $P_k \otimes S \to S$. Now

$$\mathrm{Rad}(P_k \otimes S) = \mathrm{Rad}(kG) \cdot (P_k \otimes S) \supseteq \mathrm{Rad}(kH) \cdot (P_k \otimes S) = (\mathrm{Rad}(kH) \cdot P_k) \otimes S$$

since H is a normal p-subgroup and so acts trivially on S. Since $(\mathrm{Rad}(kH) \cdot P_k) \otimes S$ has codimension in $P_k \otimes S$ equal to $\dim S$ we have that $S \cong (P_k \otimes S)/\mathrm{Rad}(P_k \otimes S)$. This shows that $P_k \otimes S$ is the projective cover of S. Finally, since kK is identified as the radical quotient of kG, $P_k \otimes kK$ is the direct sum of projective modules P_S, each appearing as often as S appears as a summand of kK. This description identifies $P_k \otimes kK$ as kG. □

Observe that since H is normal in G, IH is invariant under the conjugation action of K, and so

$$P_k = kH \supset IH \supset IH^2 \supset \cdots$$

is a chain of kG-submodules of P_k. Our next aim is to describe the kG-module structure of the quotients IH^s/IH^{s+1}, and for this we specialize to the case $H = \langle x \rangle \cong C_{p^n}$ and $K = \langle y \rangle \cong C_q$ are cyclic groups with $p \nmid q$. Suppose that ${}^y x = x^r$, so that

$$G = \langle x, y \mid x^{p^n} = 1 = y^q, {}^y x = x^r \rangle.$$

In this case the powers IH^s are a complete list of the submodules of P_k, and so it is a composition series of P_k as a kG-module. The action of y on IH is given by

$$\begin{aligned} y(x-1) &= {}^y x - 1 \\ &= x^r - 1 \\ &= (x-1)(x^{r-1} + \cdots + x + 1 - r) + r(x-1) \\ &\equiv r(x-1) \pmod{IH^2}. \end{aligned}$$

More generally for some $\alpha \in IH^2$,

$$\begin{aligned} y(x-1)^s &= (x^r - 1)^s \\ &= (r(x-1) + \alpha)^s \\ &= r^s(x-1)^s + sr(x-1)^{s-1}\alpha + \cdots \\ &\equiv r^s(x-1)^s \pmod{IH^{s+1}}. \end{aligned}$$

Thus y acts on the quotient IH^s/IH^{s+1} as multiplication by r^s. One way to describe this is that if $W = IH/IH^s$ then $IH^s/IH^{s+1} = W^{\otimes s}$, the s-fold tensor power. We now summarize these assertions.

(8.9) PROPOSITION. *Let k be a field of characteristic p and let $G = \langle x\rangle \rtimes \langle y\rangle$ where $\langle x\rangle = C_{p^n}$ and $\langle y\rangle = C_q$ has order prime to p. Suppose that ${}^y x = x^r$ and let W be the 1-dimensional kG-module on which y acts as multiplication by r. If S is any simple kG-module then P_S has a unique composition series, equal to the radical series, in which the quotients* $\operatorname{Rad}^i P_S/\operatorname{Rad}^{i+1} P_S$ *are* $S, S\otimes W, S\otimes W^{\otimes 2}, \dots, S\otimes W^{\otimes p^n-1} = S$.

The assertion about the uniqueness of the composition series follows from Exercise 5 of Section 6, since the factors in the radical series are all simple.

To continue this example we observe that the isomorphism types of the composition factors of P_S occur in a cycle which repeats itself. Since $x \mapsto x^r$ is an automorphism of C_{p^n} there is a least positive integer f such that $r^f \equiv 1 \pmod{p^n}$. Put $p^n - 1 = ef$. Then the modules $k, W, W^{\otimes 2}, W^{\otimes 3}, \dots$ give rise to f different representations. They repeat e times in P_k, except for k which appears $e+1$ times, and a similar repetition occurs with the composition factors $S\otimes W^{\otimes i}$ of P_S.

We now consider the projective modules for groups which are a semidirect product of a p-group and a group of order prime to p, but with the roles of these groups the opposite of what they were in the last example. We say that a group G has a *normal p-complement* if and only if it has a normal subgroup $K \lhd G$ of order prime to p with $|G:K|$ a power of p. Necessarily in this situation, if H is a Sylow p-subgroup of G then $G = K \rtimes H$ by the Schur-Zassenhaus theorem.

(8.10) THEOREM. *Let G be a finite group and k a field of characteristic p. The following are equivalent.*

(1) G has a normal p-complement.

(2) For every simple kG-module S, the composition factors of the projective cover P_S are all isomorphic to S.

(3) The composition factors of P_k are all isomorphic to k.

Proof. (1) $\Rightarrow$ (2): Let $G = K \rtimes H$ where $p \nmid |K|$ and H is a Sylow p-subgroup of G. We show that kH, regarded as a kG-module via the homomorphism $G \to H$, is a projective module. In fact, since kK is semisimple we may write $kK = k \oplus U$ for some kK-module U, and now $kG = kK \uparrow_K^G = k \uparrow_K^G \oplus U \uparrow_K^G$. Here $k \uparrow_K^G \cong kH$ as kG-modules (they are permutation modules with stabilizer K) and so kH is projective, being a summand of kG.

Now if S is any simple kG-module then $S \otimes_k kH$ is also projective by 8.4, and all its composition factors are copies of $S = S \otimes_k k$ since the composition factors of kH are all k (using 6.3 and 8.5). The indecomposable summands of $S \otimes_k kH$ are all copies of P_S, and their composition factors are all copies of S.

(2) $\Rightarrow$ (3) is immediate.

(3) $\Rightarrow$ (1): Suppose that the composition factors of P_k are all trivial. If $g \in G$ is any element of order prime to p (we say such an element is *p-regular*) then $P_k \downarrow_{\langle g\rangle}^G \cong k^t$ for

some t, since $k\langle g\rangle$ is semisimple. Thus g lies in the kernel of the action on P_k and if we put

$$K = \langle g \in G \;\big|\; g \text{ is } p\text{-regular}\rangle$$

then K is a normal subgroup of G, G/K is a p-group and K acts trivially on P_k. We show that K contains no element of order p: if $g \in K$ were such an element, then as $P_k \downarrow^G_{\langle g\rangle}$ is a projective $k\langle g\rangle$-module, it is isomorphic to a direct sum of copies of $k\langle g\rangle$ by 8.1, and so g does not act trivially on P_k. It follows that $p \not| \, |K|$, thus completing the proof. □

We have already studied an example of the situation described in 8.10, namely kS_3 where k is the field with four elements. In this example we may take $H = \langle (1,2)\rangle$. Observe that if V is the 2-dimensional simple kS_3-module then $V \otimes kH \cong V \oplus V$ since V is projective, so that the module $S \otimes kH$ which appeared in the proof of 8.10 need not be indecomposable.

Working over a field k, we next examine the behaviour of projective modules under the operation of dualization. We recall the definition $U^* = \mathrm{Hom}_k(U,k)$ and record the following properties:

(8.11) PROPOSITION. *Let k be a field. Then*
(1) $U^{**} \cong U$ as kG-modules,
(2) U is semisimple if and only if U^* is semisimple,
(3) U is indecomposable if and only if U^* is indecomposable, and
(4) a morphism $f : U \to V$ is a monomorphism (epimorphism) if and only if $f^* : V^* \to U^*$ is an epimorphism (monomorphism).

(8.12) PROPOSITION. *Let k be a field. Then*
(1) $kG^* \cong kG$ as kG-modules, and
(2) P is a projective kG-module if and only if P^* is a projective kG-module.

Proof. (1) We denote the elements of kG^* dual to the basis elements $\{g \;\big|\; g \in G\}$ by $\hat{g}$, so that $\hat{g}(h) = \delta_{g,h} \in k$, the Kronecker δ. We define an isomorphism of vector spaces

$$\begin{aligned} kG &\to kG^* \\ \sum_{g\in G} a_g g &\mapsto \sum_{g\in G} a_g \hat{g}\,. \end{aligned}$$

To see that this is a kG-module homomorphism we observe that if $x \in G$ then

$$(x\hat{g})(h) = \hat{g}(x^{-1}h) = \delta_{g,x^{-1}h} = \delta_{xg,h} = \widehat{xg}(h)$$

for $g, h \in G$, so that $x\hat{g} = \widehat{xg}$.

(2) Since $P^{**} \cong P$ it suffices to prove one implication. If P is a summand of kG^n then P^* is a summand of $(kG^n)^* \cong kG^n$, and so is also projective. □

When we previously introduced projective modules we could at the same time have defined injective modules, which enjoy properties similar to those of projective modules, but in a dual form. We say that a module I is *injective* if and only if whenever there are morphisms

$$\begin{array}{ccc} & & I \\ & & \uparrow \alpha \\ V & \xleftarrow{\beta} & W \end{array}$$

with β a monomorphism, then there exists a morphism $\gamma : V \to I$ so that $\gamma\beta = \alpha$. Dually to Proposition 7.3, it is equivalent to require that every monomorphism $I \to V$ is split; and also that $\mathrm{Hom}_A(\_\_, I)$ sends exact sequences to exact sequences. We leave this equivalence as an exercise. It is not true (in general) that injective modules are direct summands of free modules, but what we now show is that for group algebras over a field this special property does in fact hold.

(8.13) COROLLARY. *Let k be a field.*
(1) Projective kG-modules are the same as injective kG-modules.
(2) Each indecomposable projective kG-module has a simple socle.

Proof. (1) Suppose P is projective and that there are morphisms

$$\begin{array}{ccc} & & P \\ & & \uparrow \alpha \\ V & \xleftarrow{\beta} & W \end{array}$$

with β injective. Then in the diagram

$$\begin{array}{ccc} & & P^* \\ & & \downarrow \alpha^* \\ V^* & \xrightarrow{\beta^*} & W^* \end{array}$$

β^* is surjective, and so by projectivity of P^* there exists $f : P^* \to V^*$ such that $\beta^* f = \alpha^*$. Since $f^*\beta = \alpha$ we see that P is injective.

To see that all injectives are projective, a similar argument shows that their duals are projective, hence injective, whence the original modules are projective, being the duals of injectives.

(2) One way to proceed is to quote Exercise 6 of Section 6 which implies that $\mathrm{Soc}(P) \cong (P^*/\operatorname{Rad} P^*)^*$. If P is an indecomposable projective module then so is P^* and $P^*/\operatorname{Rad} P^*$ is simple. Thus so is $\mathrm{Soc}(P)$.

Alternatively, since homomorphisms $S \to P$ are in bijection (via duality) with homomorphisms $P^* \to S^*$, if P is indecomposable projective and S is simple then P^* is also indecomposable projective and

$$\begin{aligned}\dim \mathrm{Hom}_{kG}(S,P) &= \dim \mathrm{Hom}_{kG}(P^*,S^*) \\ &= \begin{cases} \dim \mathrm{End}(S^*) & \text{if } P^* \text{ is the projective cover of } S^*, \\ 0 & \text{otherwise.} \end{cases}\end{aligned}$$

Since $\dim \mathrm{End}(S^*) = \dim \mathrm{End}(S)$ this implies that P has a unique simple submodule and $\mathrm{Soc}(P)$ is simple. □

An algebra for which injective modules and projective modules coincide is called *self-injective* or *quasi-Frobenius*, so we have just shown that group rings of finite groups over a field are self-injective. For such an algebra, whenever a projective module occurs as a quotient of a submodule of another module, it is a direct summand.

(8.14) COROLLARY. *Suppose U is a kG-module, where k is a field, for which there are submodules $U_0 \subseteq U_1 \subseteq U$ with $U_1/U_0 = P$ a projective module. Then $U \cong P \oplus U'$ for some submodule U' of U.*

Proof. The exact sequence $0 \to U_0 \to U_1 \to P \to 0$ splits, and so $U_1 \cong P \oplus U_0$. Thus P is isomorphic to a submodule of U, and since P is injective the monomorphism $P \to U$ must split. □

We will now sharpen part (2) of 8.13 by showing that $\mathrm{Soc}\, P_S \cong S$, and we will also show that the Cartan matrix for group algebras is symmetric. These are properties which hold for a class of algebras called symmetric algebras, of which group algebras are examples. We say that a finite dimensional algebra A over a field k is a *symmetric algebra* if there is a non-degenerate bilinear form $(\ ,\ ) : A \times A \to k$ such that

(1) (symmetry) $(a,b) = (b,a)$ for all $a, b \in A$,

(2) (associativity) $(ab,c) = (a,bc)$ for all $a, b, c \in A$.

The group algebra kG is a symmetric algebra with the bilinear form defined on the basis elements by

$$(g,h) = \begin{cases} 1 & \text{if gh=1} \\ 0 & \text{otherwise} \end{cases}$$

as is readily verified. Notice that this bilinear form may be described on general elements $a, b \in kG$ by $(a,b) =$ coefficient of 1 in ab.

For the record, a finite-dimensional algebra over a field on which there is a non-degenerate associative bilinear form is called a *Frobenius algebra*. It is the case that every Frobenius algebra is a quasi-Frobenius algebra, and it would have been possible to present a development leading to the results of Corollary 8.13 by proving this implication.

We will use the bilinear form on kG in the proof of the next result, whose statement also holds for symmetric algebras in general.

(8.15) THEOREM. *Let P be an indecomposable projective module for a group algebra kG. Then $P/\operatorname{Rad} P \cong \operatorname{Soc} P$.*

Proof. We may choose a primitive idempotent $e \in kG$ so that $P \cong kGe$ as kG-modules. We claim that $\operatorname{Soc}(kGe) = \operatorname{Soc}(kG) \cdot e$, since $\operatorname{Soc}(kG) \cdot e \subseteq \operatorname{Soc}(kG)$ and $\operatorname{Soc}(kG) \cdot e \subseteq kGe$ so $\operatorname{Soc}(kG) \cdot e \subseteq kGe \cap \operatorname{Soc}(kG) = \operatorname{Soc}(kGe)$, since the last intersection is the largest semisimple submodule of Ae. On the other hand $\operatorname{Soc}(kGe) \subseteq \operatorname{Soc}(kG)$ since $\operatorname{Soc}(kGe)$ is semisimple so $\operatorname{Soc}(kGe) = \operatorname{Soc}(kGe) \cdot e \subseteq \operatorname{Soc}(kG) \cdot e$.

Next, $\operatorname{Hom}(kGe, \operatorname{Soc}(kG)e) \cong e \operatorname{Soc}(kG)e$ by 7.16, and since $\operatorname{Soc}(kG)e$ is simple, by 8.13, this is non-zero if and only if $\operatorname{Soc}(kG)e \cong kGe/\operatorname{Rad}(kGe)$. We show that $e \operatorname{Soc}(kG)e \neq 0$.

If $e \operatorname{Soc}(kG)e = 0$ then

$$\begin{aligned} 0 &= (1, e \operatorname{Soc}(kG)e) \\ &= (e, \operatorname{Soc}(kG)e) \\ &= (\operatorname{Soc}(kG)e, e) \\ &= (kG \cdot \operatorname{Soc}(kG)e, e) \\ &= (kG, \operatorname{Soc}(kG)e \cdot e) \\ &= (kG, \operatorname{Soc}(kGe)). \end{aligned}$$

Since the bilinear form is non-degenerate this implies that $\operatorname{Soc}(kGe) = 0$, a contradiction. □

(8.16) COROLLARY. *Let k be a field.*

(1) If P is any projective kG-module and S is a simple kG-module, the multiplicity of S in $P/\operatorname{Rad} P$ equals the multiplicity of S in $\operatorname{Soc} P$. In particular

$$\dim P^G = \dim P_G = \dim(P^*)^G = \dim(P^*)_G,$$

where P^G is the fixed points of G on P and P_G denotes the largest trivial quotient of P.

(2) For every simple kG-module S, $(P_S)^* \cong P_{S^*}$.

Proof. (1) This is true for every indecomposable projective module, hence also for every projective module. For the middle equality we may use an argument similar to the one which appeared in the proof of 8.13 (2).

(2) We have seen in the proof of 8.13 that $(P_S)^*$ is the projective cover of $(\operatorname{Soc} P_S)^*$, and because of 8.15 we may identify the latter module as S^*. □

From this last observation we are able to deduce that, over a large enough field, the Cartan matrix of kG is symmetric. We recall that the Cartan invariants are the numbers

$$c_{ST} = \text{multiplicity of } S \text{ as a composition factor of } P_T$$

where S and T are simple. The precise condition we require on the size of the field is that it should be a splitting field, and this is something which is discussed in the next section.

(8.17) THEOREM. *Let k be a field and let S, T be simple kG-modules. The Cartan invariants satisfy*

$$c_{ST} \cdot \dim \mathrm{End}_{kG}(T) = c_{TS} \cdot \dim \mathrm{End}_{kG}(S).$$

If $\dim \mathrm{End}_{kG}(S) = 1$ for all simple modules S (for example, if k is algebraically closed) then the Cartan matrix $C = (c_{ST})$ is symmetric.

Proof. We recall from 7.17 that

$$c_{ST} = \dim \mathrm{Hom}_{kG}(P_S, P_T) / \dim \mathrm{End}_{kG}(S)$$

and in view of this we must show that $\dim \mathrm{Hom}_{kG}(P_S, P_T) = \dim \mathrm{Hom}_{kG}(P_T, P_S)$. Now

$$\mathrm{Hom}_{kG}(P_S, P_T) = \mathrm{Hom}_k(P_S, P_T)^G \cong (P_S^* \otimes_k P_T)^G$$

by 3.3 and 3.4. Since $P_S^* \otimes_k P_T$ is projective by 8.4, this is the same as

$$(P_S^* \otimes_k P_T)^{*G} \cong (P_S \otimes_k P_T^*)^G \cong \mathrm{Hom}_{kG}(P_T, P_S),$$

using 8.16. □

We conclude this section by summarizing some further aspects of injective modules. We define an *essential monomorphism* to be a monomorphism of modules $f : V \to U$ with the property that whenever $g : U \to W$ is a map such that gf is a monomorphism then g is a monomorphism. An *injective hull* (or *injective envelope*) of U is an essential monomorphism $U \to I$ where I is an injective module. By direct arguments, or by taking the corresponding results for essential epimorphisms and projective covers and applying the duality $U \mapsto U^*$ we may prove for finitely-generated kG-modules the following statements.

- The inclusion $\mathrm{Soc}\, U \to U$ is an essential monomorphism.
- Given homomorphisms $W \xrightarrow{g} V \xrightarrow{f} U$, if two of f, g and fg are essential monomorphisms then so is the third.
- A homomorphism $f : V \to U$ is an essential monomorphism if and only if $f|_{\mathrm{Soc}\, V} : \mathrm{Soc}\, V \to \mathrm{Soc}\, U$ is an isomorphism.
- $U \to I$ is an injective hull if and only if $I^* \to U^*$ is a projective cover. Injective hulls always exist and are unique. From Theorem 8.15 we see that $S \to P_S$ is the injective hull of the simple module S.

- The multiplicity of a simple module S as a composition factor of a module U equals $\dim \mathrm{Hom}(U, P_S)/\dim \mathrm{End}(S)$.

Exercises for Section 8.

1. Prove that if G is any finite group then the only idempotents in the integral group ring $\mathbb{Z}G$ are 0 and 1.
[If e is idempotent consider the rank of the free abelian group $\mathbb{Z}Ge$ and also its image under the homomorphism $\mathbb{Z}G \to \mathbb{F}_pG$ for each prime p dividing $|G|$, which is a projective $\mathbb{F}_pG$-module. Show that $\mathrm{rank}_{\mathbb{Z}}\, \mathbb{Z}Ge$ is divisible by $|G|$. Deduce from this that if $e \neq 0$ then $e = 1$.]

2. (a) Let $H = C_2 \times C_2$ and let k be a field of characteristic 2. Show that $(IH)^2$ is a one-dimensional space spanned by $\sum_{h\in H} h$.
(b) Let $G = A_4 = (C_2 \times C_2) \rtimes C_3$ and let $\mathbb{F}_4$ be the field with four elements. Compute the radical series of each of the three indecomposable projectives for $\mathbb{F}_4A_4$ and identify each of the quotients

$$\mathrm{Rad}^n P_S/\mathrm{Rad}^{n+1} P_S.$$

Now do the same for the socle series. Hence determine the Cartan matrix of $\mathbb{F}_4A_4$.
[Start by observing that $\mathbb{F}_4A_4$ has 3 simple modules, all of dimension 1, which one might denote by 1, ω and ω^2. This exercise may be done by applying the kind of calculation which led to Proposition 8.9.]
(c) Now consider $\mathbb{F}_2A_4$ where $\mathbb{F}_2$ is the field with two elements. Prove that the 2-dimensional $\mathbb{F}_2$-vector space on which a generator of C_3 acts via $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ is a simple $\mathbb{F}_2C_3$-module. Calculate the radical and socle series for each of the two indecomposable projective modules for $\mathbb{F}_2A_4$ and hence determine the Cartan matrix of $\mathbb{F}_2A_4$.

3. Let $G = H \rtimes K$ where H is a p-group, K is a p'-group, and let k be a field of characteristic p. Regard kH as a kG-module via its isomorphism with P_k, so H acts as usual and K acts by conjugation.
(a) Show that for each n, $(IH)^n$ is a kG-submodule of kH, and that $(IH)^n/(IH)^{n+1}$ is a kG-module on which H acts trivially.
(b) Show that

$$P_k = kH \supseteq IH \supseteq (IH)^2 \supseteq (IH)^3 \cdots$$

is the radical series of P_k as a kG-module.
(c) Show that there is a map

$$IH/(IH)^2 \otimes_k (IH)^n/(IH)^{n+1} \to (IH)^{n+1}/(IH)^{n+2}$$
$$x + (IH)^2 \otimes y + (IH)^{n+1} \mapsto xy + (IH)^{n+2}$$

which is a map of kG-modules. Deduce that $(IH)^n/(IH)^{n+1}$ is a homomorphic image of $(IH/(IH)^2)^{\otimes n}$.
(d) Show that the abelianization H/H' becomes a $\mathbb{Z}G$-module under the action $g \cdot xH' =$

$gxg^{-1}H'$. Show that the isomorphism $IH/(IH)^2 \to k \otimes_{\mathbb{Z}} H/H'$ specified by $(x-1)+(IH)^2 \mapsto 1 \otimes xH'$ of Section 6 Exercise 17 is an isomorphism of kG-modules.

4. The group $SL(2,3)$ is isomorphic to the semidirect product $Q_8 \rtimes C_3$ where the cyclic group C_3 acts on $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ by cycling the three generators i, j and k. Assuming this structure, compute the radical series of each of the three indecomposable projectives for $\mathbb{F}_4 SL(2,3)$ and identify each of the quotients

$$\operatorname{Rad}^n P_S / \operatorname{Rad}^{n+1} P_S.$$

[Use Section 6 Exercise 15.]

5. Let $G = P \rtimes S_3$ be a group which is the semidirect product of a 2-group P and the symmetric group of degree 3. (Examples of such groups are $S_4 = V \rtimes S_3$ where $V = \langle (1,2)(3,4), (1,3)(2,4) \rangle$, and $GL(2,3) \cong Q_8 \rtimes S_3$ where Q_8 is the quaternion group of order 8.)

(a) Let k be a field of characteristic 2. Show that kG has two non-isomorphic simple modules.

(b) Let $e_1, e_2, e_3 \in \mathbb{F}_4 S_3$ be the orthogonal idempotents which appeared in Example 7.5. Show that each e_i is primitive in $\mathbb{F}_4 G$ and that $\dim \mathbb{F}_4 G e_i = 2|P|$ for all i.
[Use the fact that the $\mathbb{F}_4 G e_i$ are projective modules.]

(c) Show that if $e_1 = () + (1,2,3) + (1,3,2)$ then $\mathbb{F}_4 S_4 e_1$ is the projective cover of the trivial module and that $\mathbb{F}_4 S_4 e_2$ and $\mathbb{F}_4 S_4 e_3$ are isomorphic, being copies of the projective cover of a 2-dimensional module.

(d) Show that $\mathbb{F}_4 G e_i \cong \mathbb{F}_4 \langle (1,2,3) \rangle e_i \uparrow^G_{\langle (1,2,3) \rangle}$ for each i.

6. Let A be a finite-dimensional algebra over a field k, and let A_A be the right regular representation of A. The vector space dual $(A_A)^* = \operatorname{Hom}_k(A_A, k)$ becomes a left A-module via the action $(af)(b) = f(ba)$ where $a \in A$, $b \in A_A$ and $f \in (A_A)^*$. Prove that the following two statements are equivalent:
(a) $(A_A)^* \cong {}_A A$ as left A-modules.
(b) There is a non-degenerate associative bilinear pairing $A \times A \to k$.
An algebra satisfying these conditions is called a *Frobenius algebra*. Prove that, for a Frobenius algebra, projective and injective modules are the same thing.

7. Let A be a finite-dimensional algebra over a field k and suppose that the left regular representation ${}_A A$ is injective. Show that every projective module is injective and that every injective module is projective.

8. Let S and T be simple kG-modules, with projective covers P_S and P_T, where k is an algebraically closed field.
(a) For each n prove that

$$\begin{aligned} \operatorname{Hom}_{kG}(P_T, \operatorname{Soc}^n P_S) &= \operatorname{Hom}_{kG}(P_T / \operatorname{Rad}^n P_T, \operatorname{Soc}^n P_S) \\ &= \operatorname{Hom}_{kG}(P_T / \operatorname{Rad}^n P_T, P_S). \end{aligned}$$

(b) Deduce Landrock's theorem: the multiplicity of T in the nth socle layer of P_S equals the multiplicity of S in the nth radical layer of P_T.
(c) Use Exercise 6 of Section 6 to show that these multiplicities equal the multiplicity of T^* in the nth radical layer of P_{S^*}, and also the multiplicity of S^* in the nth socle layer of P_{T^*}.

9. Let U be an indecomposable kG-module, where k is a field of characteristic p, and let P_k be the projective cover of the trivial module. Prove that

$$\dim((\sum_{g\in G} g)\cdot U) = \begin{cases} 1 & \text{if } U \cong P_k, \\ 0 & \text{otherwise.} \end{cases}$$

For an arbitrary finite dimensional module V, show that $\dim((\sum_{g\in G} g)\cdot V)$ is the multiplicity with which P_k occurs as a direct summand of V.
[Observe that $kG^G = P_k^G = k\cdot\sum_{g\in G} g$. Remember that P_k is injective and has socle isomorphic to k.]

10. Let U be a kG-module, where k is a field, and let P_S be an indecomposable projective kG-module with simple quotient S. Show that in any decomposition of U as a direct sum of indecomposable modules, the multiplicity with which P_S occurs is equal to

$$\frac{\dim \mathrm{Hom}_{kG}(P_S, U) - \dim \mathrm{Hom}_{kG}(P_S/\operatorname{Soc} P_S, U)}{\dim \mathrm{End}_{kG}(S)}$$

and also to

$$\frac{\dim \mathrm{Hom}_{kG}(U, P_S) - \dim \mathrm{Hom}_{kG}(U, \operatorname{Rad} P_S)}{\dim \mathrm{End}_{kG}(S)}.$$