Cambridge University Press
978-1-107-16239-6 — A Course in Finite Group Representation Theory
Peter Webb
Excerpt
More Information

1

Representations, Maschke's Theorem, and Semisimplicity

In this chapter, we present the basic definitions and examples to do with group representations. We then prove Maschke's theorem, which states that in many circumstances representations are completely reducible. We conclude by describing the properties of semisimple modules.

1.1 Definitions and Examples

Informally, a representation of a group is a collection of invertible linear transformations of a vector space (or, more generally, of a module for a ring) that multiply together in the same way as the group elements. The collection of linear transformations thus establishes a pattern of symmetry of the vector space, which copies the symmetry encoded by the group. Because symmetry is observed and understood so widely, and is even one of the fundamental notions of mathematics, there are applications of representation theory across the whole of mathematics as well as in other disciplines.

For many applications, especially those having to do with the natural world, it is appropriate to consider representations over fields of characteristic zero such as $\mathbb{C}$, $\mathbb{R}$, or $\mathbb{Q}$ (the fields of complex numbers, real numbers, or rational numbers). In other situations that might arise in topology or combinatorics or number theory, for instance, we find ourselves considering representations over fields of positive characteristic, such as the field with p elements $\mathbb{F}_p$, or over rings that are not fields, such as the ring of integers $\mathbb{Z}$. Many aspects of representation theory do change as the ring varies, but there are also parts of the theory that are similar regardless of the field characteristic or even if the ring is not a field. We develop the theory independently of the choice of ring where possible so as to be able to apply it in all situations and to establish a natural context for the results.

Let G denote a finite group, and let R be a commutative ring with a 1. If V is an R-module, we denote it 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 nonsingular $n \times n$ matrices over R, and we denote it by $GL(n, R)$ or $GL_n(R)$, or in case $R = \mathbb{F}_q$ is the finite field with q elements by $GL(n, q)$ or $GL_n(q)$. We point out also that unless otherwise stated, modules will be left modules and morphisms will be composed reading from right to left so that matrices in $GL(n, R)$ are thought of as acting from the left on column vectors.

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

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

In a situation where V is free as an R-module, on taking a basis for V, we may write each element of $GL(V)$ as a matrix with entries in R, and we obtain for each $g \in G$ a matrix $\rho(g)$. These matrices multiply together in the manner of the group, and we have a *matrix representation* of G. 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 also called the representation, but it is more properly called the *representation module* or *representation space* (if R is a field).

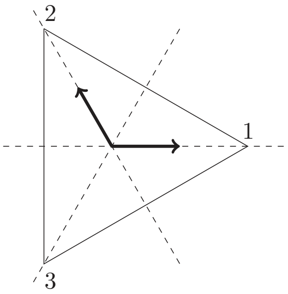
To illustrate some of the possibilities that may arise, we consider some examples.

Example 1.1.1. For any group G and commutative ring R, we can take $V = R$ and $\rho(g) = 1$ for all $g \in G$, where 1 denotes the identify map $R \to R$. This representation is called the *trivial representation*, and it is often denoted simply by its representation module R. Although this representation turns out to be extremely important in the theory, it does not at this point give much insight into the nature of a representation.

Example 1.1.2. A representation on a space $V = R$ of rank 1 is in general determined by specifying a homomorphism $G \to R^\times$. Here $R^\times$ is the group of units of R, and it is isomorphic to $GL(V)$. For example, if $G = \langle g \rangle$ is cyclic of order n and $k = \mathbb{C}$ is the field of complex numbers, there are n possible such homomorphisms, determined by $g \mapsto e^{\frac{2r\pi i}{n}}$ where $0 \leq r \leq n - 1$. Another important example of a degree 1 representation is the *sign representation* of the symmetric group S_n on n symbols, given by the group homomorphism that assigns to each permutation its sign, regarded as an element of the arbitrary ring R.

Cambridge University Press
978-1-107-16239-6 — A Course in Finite Group Representation Theory
Peter Webb
Excerpt
More Information

Example 1.1.3. Let $R = \mathbb{R}$, $V = \mathbb{R}^2$, and $G = S_3$. This group G is isomorphic to the group of symmetries of an equilateral triangle. The symmetries are the three reflections in the lines that bisect the equilateral triangle, together with three rotations:



Positioning the center of the triangle at the origin of V and labeling the three vertices of the triangle as 1, 2, and 3, we get a representation

$$() \mapsto \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

$$(1, 2) \mapsto \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

$$(1, 3) \mapsto \begin{bmatrix} -1 & 0 \\ -1 & 1 \end{bmatrix},$$

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

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

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

where we have taken basis vectors in the directions of vertices 1 and 2, 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 $\mathbb{R}$ the matrices have integer entries, and these may be interpreted in every ring. No matter what the ring is, the matrices always multiply together to give a copy of S_3.

At this point, we have constructed three representations of S_3: the trivial representation, the sign representation, and one of dimension 2.

Example 1.1.4. 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. We see that the assignment

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

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 any other characteristic it would not work, because the matrix shown would no longer have order p.

We can think of representations in various ways. One of them is that a representation is the specification of an action of a group on an R-module, as we now explain. 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 earlier, 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. What this means is that a typical element of RG is an expression $\sum_{g \in G} a_g g$ where $a_g \in R$, and the multiplication of these elements is given symbolically by

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

More concretely, we exemplify this definition by listing some elements of the group algebra $\mathbb{Q}S_3$. We write elements of S_3 in cycle notation, such as $(1, 2)$. This group element gives rise to a basis element of the group algebra which we write either as $1 \cdot (1, 2)$ or simply as $(1, 2)$ again. The group identity element $()$ also serves as the identity element of $\mathbb{Q}S_3$. 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:

$$\begin{aligned}(3(1, 2, 3) + (1, 2))(() - 2(2, 3)) &= 3(1, 2, 3) + (1, 2) - 6(1, 2) - 2(1, 2, 3)\\ &= (1, 2, 3) - 5(1, 2).\end{aligned}$$

An (associative) *R-algebra* is defined to be a (not necessarily commutative) 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.

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. Throughout this text, we may refer to group representations as modules (for the group algebra).

Proposition 1.1.5. *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 an 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. □

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 ${}_AA$ when we wish to emphasize the module structure, and this is the (left) regular representation of A. When $A = RG$, we may describe the 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 nonzero entry, and that nonzero 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 that 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 $\rho_W : G \to GL(W)$ that is the subrepresentation afforded by W.

Example 1.1.6. 1. Let $C_2 = \{1, -1\}$ be cyclic of order 2 and consider the representation

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

There are just four invariant subspaces, namely $\{0\}$, $\langle \binom{1}{0} \rangle$, $\langle \binom{0}{1} \rangle$, $\mathbb{R}^2$, and no others. The representation space $\mathbb{R}^2 = \langle \binom{1}{0} \rangle \oplus \langle \binom{0}{1} \rangle$ is the direct sum of two invariant subspaces.

Example 1.1.7. In Example 1.1.4, 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 nonzero invariant subspaces.

We make use of 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 that these notions entail is written out explicitly, and two representations that 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 just met this property in Example 1.1.6, which gives a representation that is a direct sum of two nonzero subspaces; by contrast, Example 1.1.7 provides an example of a subrepresentation that is not a direct summand.

1.2 Semisimple Representations

We come now to our first nontrivial result, one that is fundamental to the study of representations over fields of characteristic zero, or characteristic not dividing the group order. This surprising result says that in this situation representations always break apart as direct sums of smaller representations. We do now require the ring R to be a field, and in this situation, we will often use the symbols F or k instead of R.

Theorem 1.2.1 (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, that is, 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 $V = W \oplus \operatorname{Ker}(\pi)$ as vector spaces, but $\operatorname{Ker}(\pi)$ 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 furthermore $\pi'(v) \in W$ for all $v \in V$, π' is a projection onto W and so $V = W \oplus \operatorname{Ker}(\pi')$. We show finally that $\operatorname{Ker}(\pi')$ is an invariant subspace by verifying that π' is an FG-module homomorphism: if $h \in G$ and $v \in V$ then

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

because as g ranges over the elements of G, so does $h^{-1}g$. Now if $v \in \mathrm{Ker}(\pi')$ then $hv \in \mathrm{Ker}(\pi')$ also (since $\pi'(hv) = h\pi'(v) = 0$) and so $\mathrm{Ker}(\pi')$ is an invariant subspace. □

Because the next results apply more generally than to group representations, we let A be a ring with a 1 and consider its modules. A nonzero A-module V is said to be *simple* or *irreducible* if V has no A-submodules other than 0 and V.

Example 1.2.2. When A is an algebra over a field, every module of dimension 1 is simple. In Example 1.1.3, we have constructed three representations of $\mathbb{R}S_3$, and they are all simple. The trivial and sign representations are simple because they have dimension 1, and the 2-dimensional representation is simple because, visibly, no 1-dimensional subspace is invariant under the group action. We will see in Example 2.1.6 that this is a complete list of the simple representations of S_3 over $\mathbb{R}$.

We see immediately that a nonzero module is simple if and only if it is generated by each of its nonzero elements. Furthermore, the simple A-modules are exactly those of the form A/I for some maximal left ideal I of A: every such module is simple, and given a simple module S with a nonzero element $x \in S$ the A-module homomorphism $A \to S$ specified by $a \mapsto ax$ is surjective with kernel a maximal ideal I, so that $S \cong A/I$. Because all simple modules appear inside A in this way, we may deduce that if A is a finite-dimensional algebra over a field there are only finitely many isomorphism types of simple modules, these appearing among the composition factors of A when regarded as a module. As a consequence, the simple A-modules are all finite-dimensional.

A module that is the direct sum of simple submodules is said to be *semisimple* or *completely reducible*. We saw in Examples 1.1.6 and 1.1.7 two examples of modules, one of which was semisimple and the other of which was not. Every module of finite composition length is somehow built up out of its composition factors, which are simple modules, and we know from the Jordan–Hölder theorem that these composition factors are determined up to isomorphism, although there may be many composition series. The most rudimentary way these composition factors may be fitted together is as a direct sum, giving a semisimple module. In this case, the simple summands are the composition factors of the module, and their isomorphism types and multiplicities are uniquely determined. There may, however, be many ways to find simple submodules of a semisimple module so that the module is their direct sum.

We will now relate the property of semisimplicity to the property that appears in 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 that use Zorn's lemma. These finiteness conditions can be removed, and we leave the details to Exercise 14 at the end of this chapter.

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

Lemma 1.2.3. *Let A be a ring with a 1, and suppose that $U = S_1 + \cdots + S_n$ is an A-module that 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 of $\{1, \ldots, n\}$ 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 nonempty collection of subsets. 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, $W = U$. The consequences (1) and (2) are immediate. □

Proposition 1.2.4. *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) ⇒ (2) is immediate and the implications (2) ⇒ (1) and (2) ⇒ (3) follow from Lemma 1.2.3. To show that (3) ⇒ (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 at the end of this chapter). 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 then $U = V \oplus W$ for some submodule W that we have just observed satisfies condition (1), and hence so does U/V, because $U/V \cong W$. □

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

Corollary 1.2.5. *Let F be a field in which $|G|$ is invertible. Then every finite-dimensional FG-module is semisimple.*

Proof. This combines Theorem 1.2.1 with the equivalence of the statements of Proposition 1.2.4. □

This result 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 1.2.3 will be used on many occasions when we are considering modules that are not semisimple.

Corollary 1.2.6. *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, that 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