

On Representations and Characters of Groups

Kadin Tucker

October 2022

Abstract

In this thesis we introduce the mathematical fields of representation theory and character theory, providing a broad outline of the main concepts of each from the background of a general knowledge of abstract algebra. We cover a broad introduction to the representations of groups viewed as group and algebra homomorphisms and as modules over the group algebra, then proceed to consider key results on the structure of representations. Character theory is then introduced, as well as the main components of the structure of characters through their formation of an orthonormal basis for the space of class functions.

Contents

1	Introduction	4
2	Modules	5
3	Algebras	11
4	Representations as Homomorphisms	14
5	Representations as Modules	18
6	Reducibility of Representations	21
7	Maschke's Theorem	24
8	Schur's Lemma	27
9	Dimensions of Composition Factors	31
10	Characters	35
11	Inner Products of Characters	41
12	Conclusion	49

1 Introduction

The abstract notion of a group came about following research by Évariste Galois on the relationships between polynomials over a field and groups of automorphisms in that field. Much of the theory of groups was developed by Arthur Cayley in the following decades under the notion that the abstract group can be defined solely by its multiplication table, also called, fittingly, a Cayley table. However, the mathematicians Richard Dedekind and Georg Frobenius, through a long correspondence, found great utility in studying groups not through solely their multiplication tables but viewed as groups of matrices. The correspondence between the two mathematicians gradually led to the outset of representation theory as well as character theory. [4]

Character theory in particular has a major role in research mathematics. Frobenius' theorem, a purely group-theoretical result, has no known proofs that do not use character theory. Burnside's $p^a q^b$ theorem is another purely group-theoretical result that was first proved using character theory; though, more recently, proofs have been discovered that do not require character theory. [6]

In the study of metrics, a mathematician might well ask: why do metrics necessarily have a codomain of the real numbers? Does it need to be the real numbers? To answer that, one finds quickly that metrics need to map to a totally ordered set to make sense, and that it needs to be to a set with well-defined addition. It becomes very helpful, also, that the set is a field, with multiplication and with numbers that can get arbitrarily small. This will lead us to \mathbb{Q} , and then to \mathbb{R} . However, what the mathematician finds is that every field with the desired properties has the same exact algebraic structure as \mathbb{R} . In its essence, representation theory is similar: there comes a point where the abstraction of groups is no longer useful and it becomes more useful to ground them to a more easily interpreted mathematical construct: the matrix. Part of the justification for this way of thinking is a corollary to the Artin-Wedderburn theorem:

Theorem 1.1. [1, Theorem 19.3.2] *Let G be a finite group. Then there exist positive integers n_1, \dots, n_k such that:*

$$\mathbb{C}[G] \cong \text{Mat}_{n_1}(\mathbb{C}) \times \cdots \times \text{Mat}_{n_k}(\mathbb{C}).$$

What this theorem says, in essence, is that the algebraic structure of a finite group can be understood as an algebraic structure of matrices over complex numbers. However, this formulation, is not at all constructive: the fact that there exists such a representation of the group G says nothing about what such a structure looks like; and, furthermore, how are the group G and the group algebra $\mathbb{C}[G]$ even connected? These are questions that a deeper study of representation theory can answer.

In this thesis we will explore how we can understand the connections between matrices and abstract groups in the context of the abstract algebraic generalities of modules, groups, and rings, and the advantages and disadvantages of such methods of understanding such connections.

The reader is expected to have some background in the fundamentals of the theory of rings, fields, and groups, as well as a solid understanding of linear algebra. The reader may also benefit from knowledge of module theory, though the fundamentals of module theory will be covered in this thesis.

2 Modules

In the following section we briefly review modules and vector spaces. The reader is expected to have some general background in modules

Definition 2.1. Let R be a ring with identity 1. Let M be a set equipped with two operations, called *addition*, $M \times M \rightarrow M$, and *scalar multiplication*, $R \times M \rightarrow M$, satisfying, for all $a, b \in R$, $m, n \in M$:

- (1) $(M, +)$ is an abelian group;
- (2) $a(m + n) = am + an$, and $(a + b)m = am + bm$;
- (3) $1m = m$.

The algebraic structure of M equipped with addition and scalar multiplication from the ring R on the left is called a *left R -module*.

Similarly, we can define a *right R -module* through defining the action of scalar multiplication on the right. Throughout this thesis we shall only consider left R -modules, and the broad term of R -module will mean a left R -module.

An R -module M is called a *vector space* if the ring R is a field.

An R -*submodule* of a module M is a subset N of M that is closed under addition and scalar multiplication from R .

From this definition it can be seen that every vector space is a module, but not every module is a vector space. From linear algebra there are many useful results about vector spaces, however these results do not in general extend to general modules.

We proceed to consider some noteworthy examples of modules.

Example 2.2.

- (1) Let R be a ring with unity. Then the set R is itself an R -module, with addition as in the ring and scalar multiplication being multiplication within the ring itself.

The submodules of R are those subsets of R which are closed under addition and under (left) multiplication from R itself; these are precisely the (left) ideals of R .

- (2) Let $\text{Mat}_n(F)$ be the set of $n \times n$ matrices over a field F . Then $\text{Mat}_n(F)$ is an F -module, and thus an F -vector space, with addition and scalar multiplication defined as usual for matrices.
- (3) Let F be a field. Write F^n to mean the n -fold cartesian product of F . Then F^n is an F -module, and F -vector space, through the coordinate-wise operations:

$$\begin{aligned}(a_1, \dots, a_n) + (b_1, \dots, b_n) &= (a_1 + b_1, \dots, a_n + b_n); \\ \lambda(a_1, \dots, a_n) &= (\lambda a_1, \dots, \lambda a_n).\end{aligned}$$

- (4) If S is a subring of a ring R , then R is also an S -module through typical multiplication from S in R . For example, the ring \mathbb{C} is an \mathbb{R} -vector space.
- (5) Let S again be a subring of a ring R , and let M be an R -module. Then M forms an S -module through restriction of the action of scalar multiplication from R to the set S .

Furthermore, the ring S need not be a subring of R but need only be isomorphic to a subring of R . If $\phi : S \rightarrow R$ is an injective homomorphism of rings, then M is an S -module through the action $sm := \phi(s)m$.

This fact will be used frequently throughout this thesis, where R is not a field but S is a field. The terms R -module, R -submodule and S -vector space, and S -subspace will be used to make clearer this distinction.

From this point forward, the letter R will always denote a ring, with unity, and the letter F will always denote a field.

Definition 2.3. Let M and N be R -modules. A mapping $\phi : M \rightarrow N$ is called an R -homomorphism if, for all $a \in R$ and $m_1, m_2 \in M$:

$$\begin{aligned}\phi(m_1 + m_2) &= \phi(m_1) + \phi(m_2); \\ \phi(am_1) &= a\phi(m_1).\end{aligned}$$

An R -homomorphism is called an R -isomorphism if it is bijective. If there exists an R -isomorphism $M \rightarrow N$, then the R -modules M and N are called *isomorphic*, and we write $M \cong N$. This is an equivalence relation.

An R -homomorphism is called an R -endomorphism if its domain and codomain are the same module. A bijective R -endomorphism is called an R -automorphism.

Example 2.4.

- (1) Let M be an R -module, and let $m \in M$. Then the mapping $R \rightarrow M$ defined as $a \mapsto am$ is an R -homomorphism.
- (2) The mapping $f : m \mapsto m + n$, for fixed nonzero $n \in M$, is not necessarily an R -homomorphism. This is because of the following:

$$\begin{aligned}f(am) &= am + n, \\ af(m) &= a(m + n) = am + an.\end{aligned}$$

One can easily see that in \mathbb{Z} viewed as a module over itself, picking $a = 2$ and $m = n = 1$ yields $3 = f(am) \neq af(m) = 4$.

- (3) The mapping $f : \mathbb{R}^2 \rightarrow \mathbb{R}$ defined by $f(x, y) = x$ is an \mathbb{R} -homomorphism:

$$\begin{aligned}f(x_1 + x_2, y_1 + y_2) &= x_1 + x_2 = f(x_1, y_1) + f(x_2, y_2); \\ f(ax, ay) &= ax = af(x, y).\end{aligned}$$

- (4) Let S be a subring of R , and let M and N be R -modules. Then an R -homomorphism $f : M \rightarrow N$ is also an S -homomorphism.
- (5) The trivial mapping $\phi(x) = 0$ is always a homomorphism between any two modules.
- (6) Let R be a commutative ring, and let U and V be R -modules. By the notation $\text{Hom}_R(U, V)$ we mean the set of R -homomorphisms $U \rightarrow V$. This set itself has the structure of an R -module through the operations defined, for $\phi, \psi \in \text{Hom}_R(U, V)$ and $a \in R$:

$$\begin{aligned}(\phi + \psi)(x) &= \phi(x) + \psi(x); \\ (a\phi)(x) &= a\phi(x).\end{aligned}$$

Definition 2.5. Let M and N be R -modules, and let $\phi : M \rightarrow N$ be an R -homomorphism.

The *kernel* of the homomorphism ϕ is the set:

$$\ker \phi = \{m \in M \mid \phi(m) = 0\}.$$

The *image* of the homomorphism ϕ is the set:

$$\operatorname{im} \phi = \{\phi(m) \mid m \in M\}.$$

Example 2.6.

- (1) Consider \mathbb{Z} as a module over itself, and fix $n \in \mathbb{Z} \setminus \{0\}$. Then the endomorphisms $x \mapsto nx$ has the kernel $\{0\}$, since $nx = 0$ if and only if $x = 0$. This is precisely because \mathbb{Z} is an integral domain. This mapping has the image $n\mathbb{Z}$, an ideal in \mathbb{Z} . Note that $n\mathbb{Z} = \mathbb{Z}$ if and only if $n = 1$ or $n = -1$.
- (2) The mapping $f : \mathbb{R}^2 \rightarrow \mathbb{R}$ defined by $f(a, b) = a$ has the kernel $\mathbb{R}_2^2 := \{(0, b) \mid b \in \mathbb{R}\}$. The image of f is \mathbb{R} , since for each $a \in \mathbb{R}$ one may pick the element $(a, 0)$ as its preimage under f .
- (3) The trivial mapping $f : M \rightarrow N$ defined by $m \mapsto 0$ has the kernel M and the image $\{0\}$. It is the only mapping with this kernel and this image, since otherwise there exists at least one element of M that does not map to zero, and there exists at least one nonzero element of N to which f maps.

We will proceed to show some simple yet very useful properties of the kernel and image of a homomorphism.

Proposition 2.7. Let M and N be R -modules, and let $\phi : M \rightarrow N$ be an R -homomorphism. Then the following hold:

- (1) $\ker \phi$ is an R -submodule of M .
- (2) $\operatorname{im} \phi$ is an R -submodule of N .
- (3) ϕ is injective if and only if $\ker \phi = \{0\}$.
- (4) ϕ is surjective if and only if $\operatorname{im} \phi = N$.

Proof. Let $a, b \in R$, and let $m, n \in \ker \phi$. Then $\phi(am + bn) = a\phi(m) + b\phi(n)$ since ϕ is an R -homomorphism. Thus $\phi(am + bn) = 0 + 0 = 0$, so $am + bn \in \ker \phi$. This establishes (1).

Let $m, n \in \operatorname{im} \phi$. Then there exist $m', n' \in M$ such that $\phi(m') = m$ and $\phi(n') = n$. Then since ϕ is a homomorphism, we have that $am + bn = \phi(am' + bn')$. Thus $am + bn \in \operatorname{im} \phi$, because $am' + bn' \in M$. This establishes (2).

Suppose that ϕ is injective, and pick arbitrary $m, n \in M$. Then $\phi(m) = \phi(n)$ gives that $m = n$. Let $x \in \ker \phi$. Then $\phi(x) = 0 = \phi(0)$, which implies that $x = 0$. To show the converse, suppose now that $\ker \phi = \{0\}$, and suppose that $\phi(m) = \phi(n)$. Then $\phi(m - n) = 0$, so that $m - n \in \ker \phi$. Thus $m - n = 0$, and so $m = n$. It follows that ϕ is injective, and (3) is shown.

If ϕ is not surjective, then there exists some element $n \in N$ that does not have a preimage under ϕ in M , and hence $\operatorname{im} \phi \subsetneq N$. If ϕ is surjective, then every element N has some preimage in M under ϕ , and hence $N \subseteq \operatorname{im} \phi$. We have that $\operatorname{im} \phi \subseteq N$ by definition. This establishes (4). \square

We will now briefly review some concepts from linear algebra, though now in the language of modules.

Definition 2.8. Let V be an F -vector space, and let a_1, \dots, a_n be a finite collection of elements of V .

- (1) If, for all $v \in V$ there exist $\lambda_1, \dots, \lambda_n$ such that $v = \lambda_1 a_1 + \dots + \lambda_n a_n$, then the set a_1, \dots, a_n is said to *span* or *generate* the space V .
- (2) If $\lambda_1 v_1 + \dots + \lambda_n v_n = 0$ implies that $\lambda_1 = \dots = \lambda_n = 0$, then the set a_1, \dots, a_n is said to be *linearly independent*. Otherwise, the set is called *linearly dependent*.
- (3) The set a_1, \dots, a_n is called a *basis* for the vector space V if it is both linearly independent and spans the space V .

A key result from elementary linear algebra is that if an F -vector space V has a basis a_1, \dots, a_n , then any basis for V will also have n elements. This number n is called the *dimension* of V . If there exists no finite basis for V , then V is said to have infinite dimension.

The vector spaces considered in this thesis will always have a finite dimension n . In this case we always find an isomorphism to the F -vector space F^n . If the F -vector space V has the basis a_1, \dots, a_n , then the mapping $F^n \rightarrow V$ defined by $(\lambda_1, \dots, \lambda_n) \mapsto \lambda_1 a_1 + \dots + \lambda_n a_n$ is an F -isomorphism. Indeed the mapping is injective because a_1, \dots, a_n are linearly independent, and the mapping is surjective because a_1, \dots, a_n span the space V . From this, we may consider the structure of an n -dimensional F -vector space through the vector space F^n .

We proceed to study the concept of the direct sum of modules. Much of the study of representations and characters involves the study of their general structures, which, as will be seen, can be described through the language of modules and the direct sum.

Definition 2.9. Let P be an R -module and let M and N be R -submodules of P . The *sum* of the modules M and N is the R -module defined as:

$$M + N := \{m + n \mid m \in M, n \in N\}.$$

The modules M and N are said to be *in direct sum* if for all $x \in M + N$ there exist unique $m \in M$ and $n \in N$ such that $x = m + n$.

In other words, M and N are in direct sum if the mapping $M \times N \rightarrow M + N$ defined $(m, n) \mapsto m + n$ is injective.

If M and N are in direct sum, then their sum is called instead the *internal direct sum* of M and N , and denoted $M \oplus N$.

Example 2.10.

- (1) Let R be a nonzero ring. Then R does not exist in direct sum with itself as an R -module: $a + 0 = (a + a) + (-a)$, and hence the element a has two different representations in the sum $R + R$. In particular, we have that $R + R = R$.
- (2) Consider the R -module R^2 . Then the submodules $R_1^2 = \{(a, 0) \mid a \in R\}$ and $R_2^2 = \{(0, a) \mid a \in R\}$ are in direct sum: each element (a, b) can be expressed uniquely as $(a, 0) + (0, b)$. Note also that $R \cong R_1^2 \cong R_2^2$ as R -modules.

Definition 2.11. Let M and N be any two R -modules. Then the *external direct sum* of M and N is the module on $M \times N$ with operations defined, for $a \in R, m_1, m_2 \in M, n_1, n_2 \in N$, by:

$$\begin{aligned} a(m_1, n_1) &= (am_1, an_1); \\ (m_1, n_1) + (m_2, n_2) &= (m_1 + m_2, n_1 + n_2). \end{aligned}$$

The external direct sum of M and N is also written as $M \oplus N$.

It is quick to see that $M \oplus N$ is an R -module: $am \in M$ and $an \in N$, since M and N are R -modules, and $m_1 + m_2 \in M$ and $n_1 + n_2 \in N$, again since M and N are R -modules. The identity element of $M \oplus N$ is $(0, 0)$.

Example 2.12. The vector space F^n is precisely the external direct sum $F \oplus \cdots \oplus F$, with n copies of the F -vector space F .

We will now justify the use of the same notation for the internal and external direct sum. Let M and N be R -submodules of an R -module P . Let T be their external direct sum and let S be their internal direct sum. Then we show that the homomorphism $\phi : T \rightarrow S$ defined by $(m, n) \mapsto m + n$ is an isomorphism. The mapping ϕ is surjective, since every element of the internal direct sum takes the form $m + n$, and so one picks the preimage (m, n) . To see that ϕ is injective, we consider its kernel. Since S is an internal direct sum, the element 0 has a unique decomposition into $0 = m + n$. Then since $m = 0$ and $n = 0$ satisfies that $0 = 0 + 0$, it must be that $m = 0$ and $n = 0$. Particularly, we have that $m + n = 0$ if and only if $m = 0$ and $n = 0$. Thus, $\ker \phi = \{(0, 0)\}$. Then by Proposition 2.7, the mapping ϕ is injective.

From this point forward we shall use the broad term of direct sum usually without specifying whether the sum is internal or external. In general, we will speak of internal direct sums in the case that the modules in question are all submodules of some larger module, and we will speak of external direct sums otherwise.

A direct sum of modules extends in a natural, associative manner to longer strings of submodules. Let M, N , and L be R -submodules of some R -module P . Then:

$$(M \oplus N) \oplus L = \{(m + n) + \ell \mid m \in M, n \in N, \ell \in L\}.$$

However, since addition in modules is associative, we find that:

$$\begin{aligned} \{(m + n) + \ell \mid m \in M, n \in N, \ell \in L\} &= \{m + (n + \ell) \mid m \in M, n \in N, \ell \in L\} \\ &= M \oplus (N \oplus L). \end{aligned}$$

This may then be extended, through an induction argument, to arbitrarily long finite strings of direct sums of modules.

One may also further extend this notion to infinite strings of modules, though this is beyond the scope of this thesis in which we only consider finite direct sums.

Direct sums give us a notion of factorizing modules. Having the direct sum representation $P = M \oplus N$ allows us to consider M and N , each having simpler module structures, and through them understand the structure of the more complicated module P .

We now finish the discussion of direct sums through a useful proposition about the direct sums of two modules.

Proposition 2.13. *Let M and N be two R -submodules of an R -module P . Then M and N are in direct sum if and only if $M \cap N = \{0\}$.*

Proof. Suppose that M and N are in direct sum, and suppose that $x \in M \cap N$. Then x has the representations $x = x + 0 = 0 + x$. These representations must be the same, since M and N are in direct sum, hence $x = 0$.

Suppose that M and N are not in direct sum. Then there exists some x such that $x = a + b = a' + b'$, for distinct pairs $(a, b), (a', b')$. We have then also that $a - a' = b - b'$, with the left side

in M and the right side in N . Since the pairs (a, b) , (a', b') are distinct, at least one of $a - a'$ or $b - b'$ is nonzero, and so we have found a nonzero element of $M \cap N$. \square

We will now briefly define and discuss projections, which are closely connected to direct sums.

Definition 2.14. Let $M = M_1 \oplus \cdots \oplus M_n$ be an R -module. Then the mapping $M \rightarrow M_i$ defined by $m_1 + \cdots + m_i + \cdots + m_n \mapsto m_i$ is called the *projection* of M onto M_i .

This mapping is well defined precisely because the sum is direct: every element $m \in M$ has a unique decomposition into $m_1 + \cdots + m_n$, and hence there exists a unique coordinate m_i for each $m \in M$.

Proposition 2.15. [7, Proposition 2.29] Let $M = U \oplus V$, an R -module, and let ϕ be the projection of M onto U . Then:

- (1) ϕ is an R -homomorphism;
- (2) $\ker \phi = V$ and $\operatorname{im} \phi = U$.

Proof. Let $m = x_1 + y_1$ and $n = x_2 + y_2$ be elements of M , with $x_1, x_2 \in U$ and $y_1, y_2 \in V$. Let $a, b \in R$. Then:

$$\phi(am + bn) = \phi(ax_1 + bx_2 + ay_1 + by_2) = ax_1 + bx_2 = a\phi(x_1 + y_1) + b\phi(x_2 + y_2) = a\phi(m) + b\phi(n).$$

We have then shown (1). To show (2), we note that $\phi(m) = x_1$ equals zero only when $x_1 = 0$, in which case $m = y_1 \in V$; and $x \in U$ always has the preimage $x + 0$ under ϕ . \square

3 Algebras

Representation theory of groups involves treating elements of groups as matrices. As such, we will briefly study the algebraic properties of matrices.

By the notation $\text{Mat}_n(F)$ we mean the set of $n \times n$ matrices with entries taken from a field F . Through the usual operations of addition and multiplication this set forms a ring: multiplication of matrices is associative, has identity, and is distributive across addition; and the addition of matrices satisfies the axioms of addition. However, this ring is lacking many “nice” properties: rarely are its elements invertible, and only very rarely do they commute with other elements.

There is another property of this ring, however, that makes it much more useful. There exists an operation of scalar multiplication from the field F such that $\text{Mat}_n(F)$ is also an F -vector space. The combination of these properties of $\text{Mat}_n(F)$ leads us to define a new algebraic structure:

Definition 3.1. [6, Definition 1.1] Let F be a field, and let A be a ring with identity 1_A . Then the ring A is called an F -algebra if it is equipped with a (left) action from F that “agrees” with the algebraic structure of the ring A : that is, for $\lambda \in F$, $a, b \in A$:

- $\lambda(ab) = (\lambda a)b = a(\lambda b)$,
- $\lambda(a + b) = \lambda a + \lambda b$.

Example 3.2.

- (1) The set $\text{Mat}_n(F)$ of $n \times n$ matrices over a field F is an F -algebra through the addition, multiplication, and scalar multiplication of matrices.
- (2) Every field F is itself an F -algebra through its own multiplication.
- (3) The ring of polynomials $F[x]$ is an F -algebra: multiplication is defined between elements, and there exists a natural embedding of F in $F[x]$, which in turn provides a natural scalar multiplication from F .
- (4) Let A be an F -algebra. Then F is effectively a subring of A through identification of F with the set $\{\lambda \cdot 1_A \mid \lambda \in F\}$, where 1_A is the multiplicative identity element in A . In other words, every F -algebra has a subring isomorphic to F .

The ring $\text{Mat}_n(F)$ is the most typical example of an F -algebra and the central reason behind the study of algebras in this thesis.

Definition 3.3. Let A be an F -algebra. We define the *center* of A , written $Z(A)$, as the set of elements of A that commute with every other element of A under multiplication. That is:

$$Z(A) := \{z \in A \mid za = az \ \forall a \in A\}.$$

Example 3.4. Let A be an F -algebra. Then the ring A is commutative if and only if $Z(A) = A$: if $ab = ba$ for all $a, b \in A$ then also all such a and b are the elements of the center $Z(A)$; and if all elements of A are in the center $Z(A)$ then all elements of A commute with all other elements of A . As such, the F -algebras F and $F[x]$, being commutative rings, have themselves as their respective centers. However, the F -algebra $\text{Mat}_n(F)$ with $n \geq 2$, which is not commutative, has a center that is strictly contained within $\text{Mat}_n(F)$.

We now will give the following proposition about the center of the F -algebra $\text{Mat}_n(F)$.

Proposition 3.5. [3, Example 1.30(a)] Let $X \in \text{Mat}_n(F)$. Then $X \in Z(\text{Mat}_n(F))$ if and only if $X = \lambda I_n$ for some $\lambda \in F$.

Proof. The proof given is my own. We show that $Z(\text{Mat}_n(F)) = \{\lambda I_n \mid \lambda \in F\}$.

Pick $X \in Z(\text{Mat}_n(F))$. Then for all matrices $Y \in \text{Mat}_n(F)$, we have $XY = YX$. That is:

$$\sum_{k=1}^n X_{ik}Y_{kj} = \sum_{k=1}^n Y_{ik}X_{kj} \quad \forall 1 \leq i, j \leq n.$$

We show the result through particular choices for the matrix Y .

Fix arbitrary indices i, j . Let Y be the matrix for which $Y_{jj} = 1$, and all other entries are 0. If $i \neq j$, then the above equation becomes:

$$X_{ij} = 0.$$

By repeating the argument for all i, j , we find that X is a diagonal matrix.

We again fix i and j . Now let Y be the matrix for which $Y_{ii} = 1$, and all other entries are 0. Then the equation becomes:

$$X_{ii} = X_{jj}.$$

Hence, through repeating the argument for all indices i, j , all entries along the diagonal of X are the same.

We have now established that $Z(\text{Mat}_n(F)) \subseteq \{\lambda I_n \mid \lambda \in F\}$. To find the reverse inclusion, pick arbitrary $Y \in \text{Mat}_n(F)$. Then $(\lambda I_n Y)_{ij} = \lambda Y_{ij}$. Then since $\lambda \in F$, a commutative ring, we have that $\lambda Y_{ij} = Y_{ij} \lambda = (Y \lambda I_n)_{ij}$. \square

Remark 3.6. For any F -algebra A , the set $\{\lambda 1_A \mid \lambda \in F\}$ is central: for all $a \in A$, we have that $(\lambda 1_A)a = \lambda(a 1_A) = a(\lambda 1_A)$. This set is then the minimal possible center of an F -algebra: for A any F -algebra, we have that $\{\lambda 1_A \mid \lambda \in F\} \subseteq Z(A)$; and we have demonstrated, in Proposition 3.5, that there exists an F -algebra which has only this set as its center.

We will now define a particular algebra that will allow for a generalized understanding of the connection between general groups and groups of matrices.

Definition 3.7. [6, Definition 1.1(c)] Let G be a finite group¹ and F a field. Then the *group ring* or *group algebra* $F[G]$ is the F -vector space with the elements of G as a basis, and, additionally, with multiplication between elements of G defined naturally through the group operation. That is:

$$F[G] = \left\{ \sum_{g \in G} a_g g \mid a_g \in F \right\};$$

and:

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

Through this, the ring $F[G]$ has the structure of an F -algebra. Addition and scalar multiplication are in accord with the ring and F -algebra axioms through the definition of $F[G]$ as an F -vector space. The multiplication in $F[G]$ is associative because the multiplications in the group G and in the field F are associative. The multiplicative identity element is the element $1e$, with 1 being in the multiplicative identity of F , and with e being the identity element in G .

¹It is possible, and not especially difficult, to extend this definition to infinite groups, but this is beyond the scope of this thesis in which finite groups are of primary interest.

Remark 3.8.

- (1) The ring $F[G]$ is commutative if and only if G is abelian. Indeed, it is immediate from the definition of multiplication in $F[G]$ that the ring is commutative if G is abelian. If G is not abelian, then there exist $g, h \in G$ that do not commute, and hence the elements $1g$ and $1h$ do not commute in $F[G]$.
- (2) While every element of G is invertible as per the definition of a group, not every element of $F[G]$ is necessarily invertible. The element ag , for $a \in F \setminus \{0\}$ and $g \in G$, is invertible, with inverse $a^{-1}g^{-1}$, however the element $g + h$, for $g, h \in G$, is not necessarily invertible.

Example 3.9.

- (1) Let $G = \{e, x\}$ be a group of order 2. Then the group ring $\mathbb{R}[G]$ is the set:

$$\mathbb{R}[G] = \{a + bx \mid a, b \in \mathbb{R}, x^2 = 1\}.$$

This ring $\mathbb{R}[G]$ is commutative, since the group G is abelian. One can see furthermore, through that $x^2 - 1 = 0$, that $\mathbb{R}[G] \cong \mathbb{R}[x]/(x^2 - 1)$ as rings. The reader may choose to prove this fact through demonstrating the canonical ring isomorphism $a + bx \mapsto \overline{a + bx}$. In particular, since the polynomial $x^2 - 1$ is reducible in $\mathbb{R}[x]$, the quotient ring $\mathbb{R}[x]/(x^2 - 1)$ is not a field. Thus $\mathbb{R}[G]$ is also not a field.

- (2) The set $G := \langle i \rangle = \{1, -1, i, -i\}$, a subset of the complex numbers, forms a group under multiplication. However, the ring $\mathbb{R}[G]$ is not the same as \mathbb{C} . Indeed, the elements of 1_G and -1_G picked from G are linearly independent in $\mathbb{R}[G]$, according to the definition of the group ring, and so the sum $1_G + (-1_G)$ does not equal zero in $\mathbb{R}[G]$. As such, the element -1_G does not correspond to the additive inverse of 1 in $\mathbb{R}[G]$.
- (3) The group G itself can be viewed as a subgroup of the group $(F[G]^*, \cdot)$ the group of invertible elements of $F[G]$. However, the group G viewed in this way does not preserve any F -algebra structure and is not an F -subalgebra of $F[G]$.

Remark 3.10. Different fields F and different groups G give different properties for the group algebra. For example, as mentioned previously, the ring $F[G]$ is commutative if and only if G is abelian. The applications of $F[G]$ to the purposes of representations and characters also rely on the characteristic of the field F ; this will be demonstrated when we discuss Maschke's theorem further in the thesis.

4 Representations as Homomorphisms

The concept of a group first emerged through Galois's study of field automorphisms. Let V be a finite-dimensional F -vector space. If we consider the group $\text{Aut}(V)$ of bijective linear transformations $V \rightarrow V$, forming a group under function composition, then from elementary linear algebra we know that each such linear transformation is equivalent to an $n \times n$ matrix, where $n = \dim V$. If $f : V \rightarrow V$ and $h : V \rightarrow V$ are linear transformations, and A and B , respectively, are their corresponding matrices in some basis, then we have the properties:

$$\begin{aligned} f(h(v)) &= ABv, \\ f^{-1}(v) &= A^{-1}v, \end{aligned}$$

where, in particular, the matrix A is invertible if and only if f is invertible. What we find is that this relationship between n -dimensional vector space automorphisms and invertible $n \times n$ matrices is an isomorphism of groups.

This correspondance between matrices and vector space automorphisms is, in part, the basis of representation theory: can something similar be done with other groups than just $\text{Aut}(V)$? We will proceed to generalize this notion, beginning with a brief definition of the general linear groups.

Definition 4.1. Let F be a field and let $n \in \mathbb{N}$. The *general linear group* of degree n over F , denoted $GL_n(F)$, is the group of invertible $n \times n$ matrices under multiplication.

We have noted now that for an F -vector space V of finite dimension n , the groups $\text{Aut}(V)$ and $GL_n(F)$ are isomorphic. Note, furthermore, that there are many possible isomorphisms between these two groups, depending on the basis chosen for V .

We will proceed to generalize this notion through defining a representation of a group.

Definition 4.2. [7, Definition 3.1] Let G be a group, and let F be a field. An F -*representation* of degree n of G is a homomorphism $\rho : G \rightarrow GL_n(F)$.

A representation is called *faithful* if it is injective.

Example 4.3.

- (1) Let V be an F -vector space of dimension n and let $G = \text{Aut}(V)$, the set of bijective linear transformations of V . Then from linear algebra we know that we have the family of representations:

$$\begin{aligned} \rho_{\mathcal{B}} : G &\rightarrow GL_n(F) \\ f &\mapsto [f]_{\mathcal{B}}, \end{aligned}$$

where $[f]_{\mathcal{B}}$ is the matrix of the linear transformation f in some basis \mathcal{B} .

- (2) The group (\mathbb{Q}^*, \cdot) has a trivial \mathbb{Q} -representation of degree 1, being $\rho : a \mapsto [a]$.

The first two examples we have considered here are representations of infinite groups; however from this point onward we will consider only finite groups.

- (3) The dihedral group D_8 , the set of symmetries of a square, has a typical representation of degree 2, which can be understood geometrically. Take $(1, 0)$, $(0, 1)$, $(-1, 0)$, and $(0, -1)$ in the plane \mathbb{R}^2 as the four vertices of a square. Then the rotations and reflections of these points onto themselves can be represented as matrices. Let T denote the matrix of

rotation counter-clockwise by an angle $\frac{\pi}{2}$, and let S be the matrix of reflection over the y -axis. That is:

$$T = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}; \quad S = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}.$$

We may continue by mapping each geometrically understood element of D_8 to the matrix which applies the symmetry to this square as defined. Let $\tau \in D_8$ denote the symmetry of rotation counter-clockwise by $\frac{\pi}{2}$, and let σ denote the symmetry over the y -axis. In particular, the elements τ and σ generate the group D_8 . We then find a representation ρ defined through:

$$\rho(\tau) = T; \quad \rho(\sigma) = S.$$

This then induces a group homomorphism $\rho : D_8 \rightarrow GL_2(\mathbb{R})$, since each element of D_8 can be expressed as a product of τ and σ and their inverses.

- (4) In general, the dihedral group D_{2n} has a faithful representation of degree 2, consisting of the symmetries of an n -gon portrayed in \mathbb{R}^2 represented as the matrices that apply the respective symmetries on a regular n -gon centered at the origin.
- (5) Not all representations are faithful. The trivial representation $\rho : g \mapsto I_n$ is only faithful for the trivial group $G = \{e\}$.
- (6) Consider the symmetric group \mathcal{S}_3 . Then this group has a natural faithful representation of degree 3.

Pick $\sigma \in \mathcal{S}_3$, viewed as a permutation of the set $\{1, 2, 3\}$. We will then construct a 3×3 matrix representation ρ of the permutation σ . For each index i , set the entry at row i and column $\sigma(i)$ to be 1, and set all other entries to 0. Then the matrix $\rho(\sigma)$ will permute the elements of a vector in the way that the permutation σ does. For example, if σ is the transposition (23) , then the corresponding matrix is as follows:

$$\rho((23)) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}.$$

We can observe that this corresponds to the permutation (23) through multiplication on the vector $(1, 2, 3)$:

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix} = \begin{bmatrix} 1 \\ 3 \\ 2 \end{bmatrix}.$$

In general, the symmetric group \mathcal{S}_n always has a natural faithful representation of degree n that can be constructed in this manner. Note this may be a representation over any field F , since it needs only the elements 0 and 1 as entries in its matrices. One may, for example, pick the field $\mathbb{Z}_2 = \{0, 1\}$.

- (7) Consider again the dihedral group D_{2n} . An alternative definition of this group is as the group of *rigid* permutations of n elements; that is, permutations in which elements retain their adjacencies after being permuted; [2, Section 1.2]. This can be seen through a labelling of the vertices of an n -gon and understanding the shape through an ordering of its vertices. Then D_{2n} has a representation of degree n , understood as the natural representation of D_{2n} viewed as a subgroup of \mathcal{S}_n . This is called the *restriction* of the representation to the subgroup D_{2n} , which is simply the restriction of the representation to a subgroup of its domain.

- (8) Let G be a finite group. Cayley's theorem states that G is isomorphic to a subgroup of \mathcal{S}_n , where $n = |G|$; [1, Theorem 5.1]. As \mathcal{S}_n has a natural faithful representation, it follows that G always has a faithful representation of degree n .

However, a group can have a representation of smaller degree. Notably, every dihedral group D_{2n} has a representation of degree 2, even though its canonical representation, viewed as a subgroup of \mathcal{S}_n , has degree n .

- (9) Let F be an infinite field. Then F -representations of finite groups are never isomorphisms. This is because $GL_n(F)$ is an infinite group, and it is hence impossible to find a surjection $G \rightarrow GL_n(F)$ when G is finite.

In effect, a representation is quite well described by its name: it provides a representation of each element of a group G in the form of a matrix such that the matrix multiplication agrees with the internal operation in the group.

Definition 4.4. The representation ρ of degree n of \mathcal{S}_n defined by:

$$(\rho(\sigma))_{ij} = \begin{cases} 1 & \sigma(i) = j; \\ 0 & \text{otherwise} \end{cases},$$

is called the *canonical representation* of \mathcal{S}_n .

The representation given in Example 4.3(6) is the canonical representation of \mathcal{S}_3 .

We can also speak of the canonical representation of the group D_{2n} viewed as a subgroup \mathcal{S}_n : it is precisely the restriction of the canonical representation of \mathcal{S}_n to its subgroup D_{2n} .

The representation of D_{2n} of degree 2 defined by the rotation and reflection matrices of points about the origin in the plane will be called the *geometric representation* of D_{2n} .

The representation given in Example 4.3(3) is the geometric representation of D_8 .

Faithful representations are of particular interest due to the following. Let G be a finite group, let F be a field, and let $\rho : G \rightarrow GL_n(F)$ be a faithful F -representation of degree n . Then by the first isomorphism theorem, since ρ is faithful, we find that:

$$G \cong \rho(G) \leq GL_n(F).$$

Hence, given a faithful representation of a group, we find that the group is isomorphic to some group of matrices.

Given Cayley's theorem, presented in Example 4.3(8), every finite group G has a faithful representation. This is the basis of a proof for Sylow's first theorem: we can determine that it suffices to prove that the groups $GL_n(\mathbb{Z}_2)$ possess a Sylow-2 subgroup, since then $G \cong \rho(G)$, where $\rho : G \rightarrow GL_n(\mathbb{Z}_2)$ is the canonical representation of G viewed as a subgroup of \mathcal{S}_n . [3, Groupes, Théorème 2.14]

Matrices in general can be given more algebraic structure than just the group structure of $GL_n(F)$: there also exist operations of addition and scalar multiplication not accounted for. What we will find is that there is a natural extension of representations to the group algebra.

Let $G = \{g_1, \dots, g_n\}$ be a finite group, and let $\lambda \in F$. Recall that ρ is a representation of G if it is a homomorphism $\rho : G \rightarrow GL_n(F)$. This then extends quite naturally to a homomorphism of F -algebras, $\mathcal{R} : F[G] \rightarrow \text{Mat}_n(F)$, defined through:

$$\mathcal{R}(\lambda g_i) = \lambda \rho(g_i).$$

Since G is a set of generators for $F[G]$ over the set of scalars F , it suffices to define the homomorphism in this way.

We demonstrate that \mathcal{R} forms a homomorphism of F -algebras. Pick $x = \sum_{i=1}^n a_i g_i$ and $y = \sum_{i=1}^n b_i g_i$ as arbitrary elements of $F[G]$, and let $\lambda, \mu \in F$. Then:

$$\lambda x + \mu y = \sum_{i=1}^n (\lambda a_i + \mu b_i) g_i,$$

gives:

$$\mathcal{R}(\lambda x + \mu y) = \sum_{i=1}^n (\lambda a_i + \mu b_i) \rho(g_i) = \lambda \sum_{i=1}^n a_i \rho(g_i) + \mu \sum_{i=1}^n b_i \rho(g_i) = \lambda \mathcal{R}(x) + \mu \mathcal{R}(y).$$

It remains to show that \mathcal{R} is a homomorphism with respect to multiplication. We consider the product xy , and use that ρ is a homomorphism of groups. For:

$$xy = \sum_{1 \leq i, j \leq n} a_i b_j g_i g_j$$

we have:

$$\mathcal{R}(xy) = \sum_{1 \leq i, j \leq n} a_i b_j \rho(g_i g_j) = \sum_{1 \leq i, j \leq n} a_i b_j \rho(g_i) \rho(g_j) = \mathcal{R}(x) \mathcal{R}(y).$$

This concludes that \mathcal{R} is a homomorphism of F -algebras.

Futhermore, the restriction of the function \mathcal{R} to the set G viewed as a subset of $F[G]$ forms a group homomorphism. This is clear, since $\mathcal{R}(g) = \rho(g)$ for all $g \in G$, and ρ is a homomorphism of groups.

It follows that given a representation $\rho : G \rightarrow GL_n(F)$ there exists an extension $\mathcal{R} : F[G] \rightarrow \text{Mat}_n(F)$, a homomorphism of F -algebras. Furthermore, given a homomorphism $\mathcal{R} : F[G] \rightarrow \text{Mat}_n(F)$ of F -algebras, there exists a restriction $\rho : G \rightarrow GL_n(F)$ that is a homomorphism of groups. We will call both such homomorphisms F -representations of the group G . [6, pg. 13]

We conclude this section by defining equivalence of representations.

Definition 4.5. [7, Definition 3.3] Let ρ, τ be two F -representations of a group G of degree n . Then ρ and τ are called *equivalent* if there exists an invertible $n \times n$ matrix T such that $\rho(g) = T\tau(g)T^{-1}$ for all $g \in G$.

In particular, two representations are equivalent if they produce the same linear transformations but possibly in different bases.

This is indeed an equivalence relation. For reflexivity, pick $T = I_n$. For symmetry, observe that $\rho(g) = T\tau(g)T^{-1}$ gives $\tau(g) = T^{-1}\rho(g)(T^{-1})^{-1}$. For transitivity, if $\rho(g) = T\tau(g)T^{-1}$ and $\tau(g) = S\sigma(g)S^{-1}$, then $\rho(g) = TS\sigma(g)(TS)^{-1}$.

5 Representations as Modules

Representations are most intuitively understood as homomorphisms. However, some of the key properties of representations are more easily understood through a different formulation: as modules over the group algebra.

The goal is to insert a representation into the structure of a module, building on the vector space in which matrices from $GL_n(F)$ act as transformations. To do so, we recall the notion of a group action:

Definition 5.1. Let T be a set, and let G be a group. A *left group action* from G on T is a mapping $G \times T \rightarrow T$, written $(g, t) \mapsto g \cdot t$, satisfying, for all $g, h \in G$ and $t \in T$:

- $e \cdot t = t$;
- $g \cdot (h \cdot t) = (gh) \cdot t$.

Example 5.2.

- (1) Let $T = \mathbb{R}^2$, and let $G = (\mathbb{R}^*, \cdot)$. Then the operation $g \cdot (a, b) = (ga, gb)$ is a group action:

$$1 \cdot (a, b) = (a, b);$$

$$g \cdot (h \cdot (a, b)) = g \cdot (ha, hb) = (gha, ghb) = (gh) \cdot (a, b).$$

Later we will look at how a group can be treated as a set of scalars through the language of modules.

- (2) Let G be any group, and let $T = G$, so that G acts on itself. The action defined:

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

is called *conjugation*.

Similarly, one can define right group actions, but only left group actions are of interest in this thesis. We will refer to left group actions just as group actions.

Definition 5.3. Let G be a group and let V be an F -vector space. A group action from G on V is called *linear* if for all $g \in G$, $u, v \in V$, $a \in F$:

- $g \cdot (u + v) = g \cdot u + g \cdot v$,
- $g \cdot (au) = a(g \cdot u)$.

The action from $GL_n(F)$ on F^n defined as $A \cdot v = Av$, as usual matrix multiplication for v an $n \times 1$ column matrix, is a linear group action. As such, one can immediately see that given an F -representation ρ of G of degree n there exists a natural linear group action from G on F^n given by:

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

Conversely, given a linear group action we can find a representation that agrees with this action. Let a group G act linearly on an F -vector space V . Let $\mu_g : V \rightarrow V$ be the endomorphism $v \mapsto g \cdot v$. This is an endomorphism precisely because the action of G on V is linear. Then, let $\rho_{\mathcal{B}}$ be the function that maps $g \in G$ to the matrix of the endomorphism $v \mapsto g \cdot v$ in some basis \mathcal{B} : this function $\rho_{\mathcal{B}}$ is then a representation of G . We observe that $\rho_{\mathcal{B}}$ is a homomorphism of groups through the following reasoning: the endomorphism $v \mapsto g \cdot h \cdot v$ is equivalent to $\mu_g \circ \mu_h$, which has the matrix $[g][h]$, where $[g]$ is the matrix of μ_g and $[h]$ is the matrix of μ_h .

This result is formalized in the following proposition:

Proposition 5.4. [7, Theorem 4.12] Let V be an F -vector space of dimension n , and let G be a group. Then:

- If $\rho : G \rightarrow GL_n(F)$ is a representation of G , then $g \cdot v := \rho(g)v$ is a linear group action of G on V .
- If $g \cdot v$ is a linear group action of G on V , then the mapping $g \mapsto [g]$, where $[g]$ is the matrix in some basis of the endomorphism $v \mapsto g \cdot v$, is a representation of G .

Remark 5.5. It is to be noted from this formulation that a linear group action does not induce a unique representation, depending, as it does, on the basis in which the representation is defined. However, any two representations induced by the same linear group action are equivalent. This is because to change a matrix to a new basis means conjugating by the change of basis matrix T , which matches the definition (Definition 4.5) of equivalent representations.

The reader may have noted the similarity between the definitions of scalar multiplication on a module and a linear group action. In fact it is possible to generalize this and blend the linear group action into the typical scalar multiplication of a module: this is done using the ring $F[G]$.

Proposition 5.6. [7, adapted from Proposition 4.5] Let G be a finite group acting on an F -module V . Then we can define an $F[G]$ -module structure on V through the scalar multiplication:

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

Proof. We go through each of the three module axioms for scalar multiplication.

- *Distributive over module elements:* we can demonstrate this through the linearity of the group action:

$$\begin{aligned} \left(\sum_{g \in G} a_g g \right) \cdot (u + v) &= \sum_{g \in G} a_g (g \cdot (u + v)) \\ &= \sum_{g \in G} a_g (g \cdot u + g \cdot v) = \sum_{g \in G} a_g (g \cdot u) + \sum_{g \in G} a_g (g \cdot v). \end{aligned}$$

- *Distributive over scalar elements:*

$$\begin{aligned} \left(\sum_{g \in G} a_g g + \sum_{g \in G} b_g g \right) \cdot v &= \left(\sum_{g \in G} (a_g + b_g) g \right) \cdot v \\ &= \sum_{g \in G} (a_g + b_g) (g \cdot v) = \sum_{g \in G} a_g (g \cdot v) + \sum_{g \in G} b_g (g \cdot v). \end{aligned}$$

- *Identity element:* the identity of $F[G]$ is $1e$, and by the properties of a group action, $e \cdot v = v$. \square

Similarly, the structure of an $F[G]$ -module induces a linear group action through the restriction of the scalar multiplication to the set of elements from g , and is also an F -vector space through a restriction of the scalars to those from F .

In this way, we can equally consider a representation as an $F[G]$ -module. This formulation is useful because it allows one to study representations through the language of modules. Understanding the structure of representations as homomorphisms is more difficult; this will be briefly explored later.

Important to note is that the set V viewed as an F -vector space and the set V viewed as an $F[G]$ -module are very different: the latter has, as part of its algebraic structure, an action from the group G , while the former does not. The structure of a set V as an $F[G]$ -module is also not at all unique; there can be many such structures depending on the underlying representation.

For example, consider the group \mathcal{S}_2 and the \mathbb{C} -vector space \mathbb{C}^2 . Let us consider the canonical representation of degree 2 of the group \mathcal{S}_2 , that is:

$$\rho((1\ 2)) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}; \quad \rho(e) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

where e is the identity element in \mathcal{S}_2 . As we will see in Example 6.2(7), the structure of the $\mathbb{C}[\mathcal{S}_2]$ -module \mathbb{C}^2 is very different from that of the \mathbb{C} -vector space \mathbb{C}^2 : there additionally exists a scalar element that permutes the coordinates of a vector.

In effect, adding an action from G expands the set of scalars in the module. The way that these new scalars may behave means that we cannot treat this module structure in the same way as an F -vector space.

We will proceed to look at how the properties of representations as homomorphisms translate into the language of modules.

Proposition 5.7. *[7, Theorem 4.12(2)] Let ρ be a representation of a group G , and let M be the $F[G]$ -module of this representation*

- (1) *If ρ is a representation of degree n , then M is an n -dimensional F -vector space.*
- (2) *Suppose ρ is equivalent to a representation τ having the module P . Then $M \cong P$.*

Proof. If ρ is a representation of degree n , then its action applies necessarily to an F -vector space of dimension n . Hence the degree of an $F[G]$ -module M is precisely the F -dimension of M ; that is, the dimension of M seen as an F -vector space; this establishes (1).

Suppose $\rho(g) = T\tau(g)T^{-1}$, and let M and P be the module characterizations of ρ and τ , respectively. Define the mapping $\phi : M \rightarrow P$ by $x \mapsto T^{-1}x$. Then we show that this is an $F[G]$ -isomorphism. It suffices to show that ϕ is an F -homomorphism and also satisfies $\phi(gx) = g\phi(x)$ for all $g \in G$.

That ϕ is an F -homomorphism is clear. Pick $g \in G$. We then show that $\phi(gx) = g\phi(x)$:

$$\phi(gx) = \phi(\rho(g)x) = \phi(T\tau(g)T^{-1}x) = \tau(g)T^{-1}x = \tau(g)\phi(x) = g\phi(x).$$

The last equality follows from that the scalar multiplication of g in P is, by definition, equivalent to matrix multiplication by $\tau(g)$.

It remains to show that ϕ is bijective, which is easily seen through the explicit inverse function $x \mapsto Tx$. We have then established (2). \square

Remark 5.8. Let A be an F -algebra. Let M be an A -module, and let N be an A -submodule of M . Then N is an F -vector subspace of M .

It has already been established that every A -module is canonically an F -vector space as well. If N is an A -submodule of M , then it is a subset of M that is closed under addition and scalar multiplication from F , and is hence an F -subspace of M .

We will use this fact to extend the properties of vector spaces known from linear algebra to $F[G]$ -modules.

6 Reducibility of Representations

We will now move on to discuss the concept of reducibility of modules. While this is a generality of modules, it is a central topic in the discussion of representations and the concept is demonstrated most clearly in the context of representations themselves.

Definition 6.1. [7, Definition 5.3] Let M be an R -module. Then M is called *irreducible* if it has exactly two distinct submodules, being M itself and $\{0\}$.

Note that this means $\{0\}$ is not an irreducible module, as it has only one submodule, itself.

Example 6.2.

- (1) Recall that a division ring is one whose nonzero elements all have multiplicative inverses; particularly, a field is a commutative division ring. The R -module R is irreducible if and only if R is a division ring. The submodules of a ring are precisely the ideals of the ring, and a ring has solely the ideals R and $\{0\}$ if and only if it is a division ring. This is one way in which vector spaces are easier to work with than general modules, to be shown in more detail in the following examples.
- (2) Consider the module R^n . Then this has submodules R_1^n, \dots, R_n^n , where R_i^n is defined as the module with elements of R^n with all coordinates 0 except for the i 'th. Each R_i^n is isomorphic to R as an R -module, however these are then irreducible if and only if R is a division ring, as otherwise they have nontrivial ideals.
- (3) Consider the ring \mathbb{Z} viewed as a \mathbb{Z} -module. Then will we show that \mathbb{Z} has no irreducible submodules. The ring \mathbb{Z} is a principal ideal domain, and as such its ideals and hence submodules each take the form (a) , for $a \in \mathbb{Z}$. If (a) is not the zero module (remember that the zero module is not considered irreducible), then we get the strict inclusion relation $(2a) \subsetneq (a)$. We find this relationship because 2 is not invertible in \mathbb{Z} . Hence, every nonzero submodule of \mathbb{Z} has a nontrivial submodule.
- (4) Let F be a field, and consider the F -vector space F^n , for some $n \in \mathbb{N}$. The F -vector space F is irreducible, as, being a field, it has solely the ideals $\{0\}$ and F itself. Each subspace of F^n is isomorphic to F^r , for $1 \leq r \leq n$, and each F^r has a subspace isomorphic to F . Hence F^r is irreducible if and only if $r = 1$, and so the irreducible submodules of F^n are precisely those isomorphic to F .
- (5) Let V be an F -vector space with finite dimension n . Then $V \cong F^n$, and each subspace of V is isomorphic to F^r , for $r \leq n$. We conclude, then, by the above point, that an F -vector subspace U of V is irreducible if and only if $U \cong F$.
- (6) Let G be a finite group, and let M be a representation—that is, an $F[G]$ -module—of degree 1. Then M is irreducible: if M has a strict subspace N , it is necessarily of smaller F -dimension than M . That M is a representation of degree 1 means precisely that the F -dimension of M is 1, and hence any strict F -subspace of M must be of dimension 0 and hence is the module $\{0\}$. Since every $F[G]$ -submodule is an F -subspace, it follows that every representation of degree 1 is irreducible.
- (7) An F -representation of a finite group G , understood as an $F[G]$ -module, does not follow the same rules of reducibility as do vector spaces: we show that the converse to the above does not hold in general.

Let ρ be the canonical \mathbb{C} -representation of \mathcal{S}_2 ; that is:

$$\rho((1\ 2)) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}; \quad \rho(e) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Understanding this representation as a module would be through an $\mathbb{C}[G]$ -module structure on the set \mathbb{C}^2 . However, this is not at all the same as the \mathbb{C} -vector space \mathbb{C}^2 .

The \mathbb{C} -vector space \mathbb{C}^2 has the irreducible \mathbb{C} -subspaces \mathbb{C}_1^2 and \mathbb{C}_2^2 . However, we will show that these are not $\mathbb{C}[G]$ -modules. Pick the column vector $\begin{bmatrix} x \\ 0 \end{bmatrix}$ from \mathbb{C}_1^2 . Then:

$$\rho(\sigma) \begin{bmatrix} x \\ 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} x \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ x \end{bmatrix} \notin \mathbb{C}_1^2.$$

Hence \mathbb{C}_1^2 is not closed under scalar multiplication as an $\mathbb{C}[G]$ -module. The same fact is true for \mathbb{C}_2^2 and can be seen in the same way.

We can go further and note that if \mathbb{C}^2 has any $\mathbb{C}[G]$ -submodules then they must also be \mathbb{C} -subspaces. In general, an $F[G]$ -module has fewer $F[G]$ -submodules than F -subspaces in the sense that the set of $F[G]$ -submodules of an $F[G]$ -module M is a subset of the set of F -subspaces of M .

- (8) The set \mathbb{C}^2 , viewed as an $\mathbb{C}[\mathcal{S}_2]$ -module, is not irreducible. The \mathbb{C} -subspace $\{(a, a) \mid a \in \mathbb{C}\}$, which is isomorphic to \mathbb{C} , is closed under the action from \mathcal{S}_2 since permuting the coordinates has no effect on them.

The property of reducibility and irreducibility is the primary justification for understanding representations as modules. Understanding what a reducible module looks like is relatively straightforward, but what does it mean to be reducible for a representation seen as a homomorphism?

Suppose that $M = U \oplus V$, where M , U , and V are $F[G]$ -modules. Write ρ for the homomorphism of the representation M . In particular, the submodules U and V are finite-dimensional F -vector spaces that are closed under multiplication from $\text{im } \rho$. The module M is also a finite dimensional F -vector space, and hence $M \cong F^n$ for some natural number n . Without loss of generality, take V to be the set of vectors with coordinates all zeros from positions 1 until some $r < n$, and U the set of vectors with coordinates all zero from all positions $r + 1$ until n . Consider just the $F[G]$ -module U . Suppose $A \in \text{im } \rho$, and pick $u \in U$. Then:

$$\begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{r1} & \cdots & a_{rn} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix} \begin{bmatrix} u_1 \\ \vdots \\ u_r \\ \vdots \\ 0 \end{bmatrix} = \begin{bmatrix} a_{11}u_1 + \cdots + a_{1r}u_r \\ \vdots \\ a_{r1}u_1 + \cdots + a_{rr}u_r \\ \vdots \\ a_{n1}u_1 + \cdots + a_{nr}u_r \end{bmatrix}.$$

For this to satisfy the property of closure, the coordinates $r + 1$ through n on the right-hand side of the above equation must all be zero. This can only be guaranteed when the lower left block of the matrix A , consisting of rows $r + 1$ through n and columns 1 through r , is zero.

If we then repeat this same process with the submodule V , we find similarly that the upper right block equals zero. We find hence that the representation ρ takes the block diagonal form:

$$\rho(g) = \left[\begin{array}{c|c} A_1 & 0 \\ \hline 0 & A_2 \end{array} \right].$$

In particular, there exist representations ρ_1 and ρ_2 of G on U and V respectively such that:

$$\rho(g) = \left[\begin{array}{c|c} \rho_1(g) & 0 \\ \hline 0 & \rho_2(g) \end{array} \right].$$

Conversely, supposing we have a representation in this block-diagonal form, we can find that its resulting representation as a module can be decomposed into a direct sum of modules. We have $M = U \oplus V$, where M is the module induced by ρ , the submodule U is the module induced by ρ_1 , and the submodule V is the module induced by ρ_2 .

7 Maschke's Theorem

This section is dedicated to a fundamental result about the decomposition of representations. We begin by defining completely reducible modules:

Definition 7.1. [7, Definition 8.6] An R -module M is called *completely reducible* if there exist irreducible submodules M_1, \dots, M_n of M for some $n \in \mathbb{N}$ such that:

$$M = M_1 \oplus M_2 \oplus \dots \oplus M_n.^2$$

Note that this is an internal direct sum, as M_1, \dots, M_n are all submodules of M .

Example 7.2.

- (1) Let F be a field. Then the F -vector space F^n is completely reducible:

$$F^n = F_1^n \oplus \dots \oplus F_n^n.$$

- (2) Let R be a ring. Then the R -module R^n is not completely reducible into $R_1^n \oplus \dots \oplus R_n^n$ unless R is a division ring. If R is not a division ring, each component R_i^n can be further subdivided into its nontrivial ideals.
- (3) The ring \mathbb{Z} viewed as a module over itself is not completely reducible, given that it has no irreducible submodules.

Before proceeding with Maschke's theorem, we briefly define the characteristic of a field.

Definition 7.3. [3, Corps, théorie de Galois, Définition 1.1] Let F be a field, and let $n \in \mathbb{N}$. Write $n \cdot 1$ to mean the sum of n copies of the multiplicative identity element 1 in the field F .

- If there exists n such that $n \cdot 1 = 0$, then the field F is said to have *characteristic* p , where p is the smallest positive integer for which $p \cdot 1 = 0$.
- Otherwise, if there exists no positive integer n such that $n \cdot 1 = 0$, then the field F is said to have characteristic 0.

In particular, a field F with characteristic zero can be viewed as containing the natural numbers through identification with the subset $\{n \cdot 1 \mid n \in \mathbb{N}\}$ of F .

We now proceed to Maschke's theorem.

Theorem 7.4. [7, Theorem 8.1] (*Maschke's Theorem*) Let G be a finite group and let F be a field of characteristic 0.³ Let M be an $F[G]$ -module of finite F -dimension n . Then if U is an $F[G]$ -submodule of M , there exists a submodule W of M such that:

$$M = U \oplus W.$$

Proof. This proof is slightly modified from the one given in [7] and includes some notes on where the characteristic of F being 0 is used.

We are given U , an $F[G]$ -submodule of M . As M is also an F -vector space, the submodule U is also an F -vector subspace of M . Since U is an F -subspace of a finite-dimensional F -vector

²Note that some definitions of completely reducible allow for infinite decompositions. However, having a finite decomposition is a stronger property than having some arbitrary decomposition, and the aim is to emphasise the utility of the group algebra in this regard.

³The statement is in fact true for fields F whose characteristic does not divide the order of the group $|G|$, but for the purposes of this thesis we restrict ourselves to fields of characteristic 0.

space M , it has some basis u_1, \dots, u_r . This can then be extended to a basis $u_1, \dots, u_r, u_{r+1}, \dots, u_n$ for the n -dimensional F -vector space M . Let $W_0 = (u_{r+1}, \dots, u_n)$, the span of the vectors u_{r+1}, \dots, u_n . We find then that $M = U \oplus W_0$, viewed as an F -vector space.

Pick $m \in M$. Then m can be uniquely decomposed as $m = u + w$, with $u \in U$ and $w \in W_0$. Let $\phi : M \rightarrow U$ be the projection of M onto U . Then in particular, by Proposition 2.15, $\ker \phi = W_0$.

We now wish to extend the F -homomorphism ϕ into an $F[G]$ -homomorphism. Define the mapping $\psi : M \rightarrow M$ by:

$$\psi(x) = \frac{1}{|G|} \sum_{g \in G} g^{-1} \phi(gx).$$

The goal is to show that this is an $F[G]$ -homomorphism as well as a projection onto U . To show that ψ is an $F[G]$ -homomorphism, it suffices to show that it is F -linear and that it agrees with multiplication from G .

Note that $|G|$ is not necessarily a natural number and is represented in the field F as the sum of $|G|$ copies of 1_F . This is then nonzero in the field F because F has characteristic 0.

That ψ is F -linear is easy to see from the fact that it is a linear combination of applications of the F -linear mapping ϕ . To show that the multiplication from G is linear, pick $h \in G$. Then:

$$\psi(hx) = \frac{1}{|G|} \sum_{g \in G} g^{-1} \phi(g hx) = \frac{1}{|G|} \sum_{g \in G} h h^{-1} g^{-1} \phi(g hx) = \frac{1}{|G|} \sum_{g \in G} h (gh)^{-1} \phi(g hx).$$

We then note that the mapping $g \mapsto gh$ is bijective, as G is a group, and hence we can reindex the sum through $\ell := gh$:

$$h \frac{1}{|G|} \sum_{\ell \in G} \ell^{-1} \phi(\ell x) = h \psi(x).$$

This establishes that ψ is an $F[G]$ -homomorphism.

Now we will show that ψ is a projection onto the set U . We do this by showing that $\psi \circ \psi = \psi$.

First we note that $\psi(x) \in U$ for all $x \in M$, since ϕ has the codomain of U and U is a closed $F[G]$ -module. Furthermore, $gu \in U$ for all $g \in G$ and $u \in U$. Hence, since ϕ is a projection onto U :

$$\psi(u) = \frac{1}{|G|} \sum_{g \in G} g^{-1} \phi(gu) = \frac{1}{|G|} \sum_{g \in G} g^{-1} gu = u.$$

We have then established that $\psi(u) = u$ for all $u \in U$. From this, and since $\psi(x) \in U$ for all $x \in M$, we find that $\psi(\psi(x)) = \psi(x)$ for all $x \in M$. In particular, we have that $\psi \circ \psi = \psi$. From this it is established that ψ is an $F[G]$ -projection of M onto U . Let $W = \ker \psi$, an $F[G]$ -submodule of M . By the properties of projections, we have:

$$M = U \oplus W.$$

Then we are done. □

Due to this statement of Maschke's theorem applying to $F[G]$ -modules such that F is a field of characteristic 0, from this point forward F always denotes a field of characteristic 0.

Corollary 7.5. [7, Theorem 8.7] *Let M be an $F[G]$ -module of F -dimension n . Then M is completely reducible as an $F[G]$ -module.*

Proof. Take $M \cong F^n$. Then every nontrivial F -subspace of M is isomorphic to F^r for some $0 < r < n$. We perform induction on n .

If $n = 1$, then M is irreducible as an F -vector space and hence also as an $F[G]$ -module; the base case is shown.

If M has no nontrivial $F[G]$ -submodules, then we are done. Otherwise, if M has a nontrivial $F[G]$ -submodule U , then by Maschke's theorem, there exists an $F[G]$ -module W such that:

$$M = U \oplus W.$$

In particular, the F -dimensions of U and W are both strictly smaller than that of M . Applying the induction hypothesis to each of these modules, we find that $U = U_1 \oplus \cdots \oplus U_r$ and $W = W_1 \oplus \cdots \oplus W_s$, for some irreducible $F[G]$ -modules U_1, \dots, U_r and W_1, \dots, W_s . Thus we have that:

$$M = (U_1 \oplus \cdots \oplus U_r) \oplus (W_1 \oplus \cdots \oplus W_s).$$

Hence, we conclude that all $F[G]$ -modules M of finite dimension as F -vector spaces are completely reducible as $F[G]$ -modules. \square

8 Schur's Lemma

The following section is dedicated to a simple yet fundamental result about irreducible modules.

Theorem 8.1. [7, Lemma 9.1(1)] (*Schur's Lemma*) *Let M, N be irreducible R -modules, and let $\phi : M \rightarrow N$ be an R -homomorphism. Then either $\phi = 0$, or ϕ is an isomorphism.*

Proof. The homomorphism $\phi = 0$ always exists between two modules, and is simply a trivial case.

Suppose then that $\phi \neq 0$. Then $\ker \phi \neq M$. Since M is irreducible and, by Proposition 2.7, $\ker \phi$ is a submodule of M , it follows that $\ker \phi = \{0\}$, and hence ϕ is injective, by Proposition 2.7. Similarly, we find that $\operatorname{im} \phi \neq \{0\}$, as $\phi \neq 0$. Thus $\operatorname{im} \phi = N$, since N is irreducible, and hence ϕ is surjective. Then we are done. \square

Schur's lemma provides a notion of individuality, up to isomorphism, of the irreducible submodules of some module. Either two irreducible modules have the same algebraic structure, or their algebraic structures are so different that there can only exist the trivial homomorphism $\phi = 0$ between them.

Of particular consequence is the following corollary.

Corollary 8.2. [7, Proposition 10.2] *Let M be a completely reducible R -module with decomposition $M = U_1 \oplus \cdots \oplus U_r$. Let W be an irreducible submodule of M . Then $W \cong U_i$ for some $1 \leq i \leq r$.*

Proof. Let W be an irreducible submodule of M . Since W is a submodule of M , an element $w \in W$ has a unique decomposition $w = u_1 + \cdots + u_r$. As W is irreducible, hence nonzero, pick some nonzero $w \in W$. Then u_i is nonzero for at least one index i . Fix one such index i .

Consider the projection ϕ_i of M onto the i 'th coordinate. In particular, the mapping ϕ_i is not the zero function by the above choices of w and i . Then the restriction of ϕ_i to W is a homomorphism $W \rightarrow U_i$. By Schur's lemma, and the fact that ϕ_i is nonzero, this restriction is an isomorphism, and we conclude that $W \cong U_i$. \square

An immediate consequence of this result is that there are finitely many irreducible submodules of any completely reducible module up to isomorphism.⁴

Throughout this section, let F be a field of characteristic 0 and let G be a finite group, such that Maschke's theorem may be applied to $F[G]$ -modules. We will now proceed to prove a significant theorem about the structure of $F[G]$ -modules and of group representations in general through the use of Schur's lemma and Maschke's theorem.

We begin with a lemma.

Lemma 8.3. [7, Proposition 10.1] *Let V, W be $F[G]$ -modules, and let $\phi : V \rightarrow W$ be an $F[G]$ -homomorphism. Then there exists an $F[G]$ -submodule U of V such that $V = \ker \phi \oplus U$, where $U \cong \operatorname{im} \phi$.*

Proof. Since $\ker \phi$ is an $F[G]$ -submodule of V , by Maschke's theorem there exists an $F[G]$ -module U such that $V = \ker \phi \oplus U$. It remains to show that $U \cong \operatorname{im} \phi$.

Let $\bar{\phi} : U \rightarrow \operatorname{im} \phi$ be the restriction of ϕ to U . We will show that $\bar{\phi}$ is an isomorphism.

⁴Note that this is only true for the definition of completely reducible given in this thesis. For a module with only infinite decompositions, this is not necessarily the case.

That $\bar{\phi}$ is a homomorphism is clear from that ϕ is. If $u \in \ker \phi \cap U$, then, since U and $\ker \phi$ are in direct sum, by Proposition 2.13 we have that $u = 0$. Hence, $\ker \bar{\phi} = \{0\}$ and $\bar{\phi}$ is injective. To show surjectivity, pick $w \in \text{im } \phi$. Then $w = \phi(v)$ for some $v \in V$. In particular, $v = k + u$, for $k \in \ker \phi$ and $u \in U$. Then $w = \phi(v) = 0 + \phi(u)$, and so $w \in \text{im } \bar{\phi}$. It follows that $\text{im } \phi = \text{im } \bar{\phi}$, which establishes surjection. Then we are done. \square

Theorem 8.4. [7, Theorem 10.5] *Consider $F[G]$ as an $F[G]$ -module, and write its decomposition:*

$$F[G] = U_1 \oplus \cdots \oplus U_r,$$

as a direct sum of irreducible $F[G]$ -modules. Then every irreducible $F[G]$ -module is isomorphic to some U_i .

Note that this is not saying that every irreducible submodule of $F[G]$ has a structure appearing in the decomposition of $F[G]$, as is a consequence of Corollary 8.2, but that every irreducible $F[G]$ -module has a structure appearing in the decomposition of $F[G]$.

Proof. Let W be an arbitrary irreducible $F[G]$ -module, and pick some arbitrary nonzero $w \in W$. Define the $F[G]$ -homomorphism:

$$\begin{aligned} \phi : F[G] &\rightarrow W, \\ r &\mapsto rw. \end{aligned}$$

In particular, the homomorphism ϕ is not the zero map. This homomorphism will act as the link between the otherwise separate module structures of $F[G]$ and W .

Since W is irreducible and $\text{im } \phi$ is a nonzero $F[G]$ -submodule thereof, we have that $W = \text{im } \phi$. By Lemma 8.3, there exists an $F[G]$ -submodule U of $F[G]$ such that:

$$F[G] = \ker \phi \oplus U,$$

with:

$$U \cong \text{im } \phi = W.$$

Since W is irreducible, the submodule U is also irreducible. Thus W is isomorphic to an irreducible submodule of $F[G]$. By Corollary 8.2, we find that $U \cong U_i$ for some index i , and so $W \cong U_i$. \square

Corollary 8.5. [7, Corollary 10.7] *There are finitely many irreducible $F[G]$ -modules, up to isomorphism.*

In the language of representations, this means that there are finitely many irreducible F -representations of a group G , up to equivalence.

Due to Theorem 8.4 we can now speak of the irreducible representations of a group as a whole, rather than of the irreducible subrepresentations of some already known representation.

Definition 8.6. By Maschke's theorem, every $F[G]$ -module, for F a field of characteristic 0 and G a finite group, is completely reducible: that is, if M is an $F[G]$ -module then there exist irreducible $F[G]$ -submodules U_1, \dots, U_r of M such that:

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

The irreducible submodules U_1, \dots, U_r of M are called the *composition factors* of the $F[G]$ -module M .

In particular, by Corollary 8.2, the composition factors of M are representative of the structures of all irreducible $F[G]$ -submodules of M . Theorem 8.4 says precisely that every irreducible $F[G]$ -module is isomorphic to some composition factor of $F[G]$ itself.

Two $F[G]$ -modules $M = U_1 \oplus \cdots \oplus U_r$ and $N = V_1 \oplus \cdots \oplus V_s$ are said to have a *common composition factor* if there exists some U_i and some V_j , composition factors of M and N , respectively, such that $U_i \cong V_j$.

We will now often speak of the composition factors of $F[G]$ -modules; when doing so, we will always be referring to an irreducible $F[G]$ -submodule thereof.

With the help of Maschke's theorem and Schur's lemma and their consequences we can now begin to finalize our understanding of the structures of representations.

Definition 8.7. [6, pg. 6] Let F be a field of characteristic 0 and let G be a finite group. A *complete set of representatives* of irreducible $F[G]$ -modules is a collection \mathcal{M} of irreducible $F[G]$ -modules that are each distinct up to isomorphism. That is, for $V, W \in \mathcal{M}$

$$V \cong W \iff V = W.$$

A complete set of representatives is then a collection of the different possible $F[G]$ -module structures that can exist.

We can compile the previous results of this section into a proposition about the complete sets of representatives of irreducible $F[G]$ -modules and in this way formalize these results about the structure of $F[G]$ -modules in general. We have already demonstrated these results, but they are now reformulated in more concise language.

Proposition 8.8. [Corollary 8.2, reformulated] Let F be a field of characteristic 0 and let G be a finite group. Let \mathcal{M} be a complete set of representatives of irreducible $F[G]$ -modules.

- (1) If U is an irreducible $F[G]$ -module, then there exists exactly one $W \in \mathcal{M}$ such that $U \cong W$.
- (2) \mathcal{M} is finite.

To begin a deeper discussion of the structure of representations, we remark on the ways in which isomorphism is weaker than equality. Consider the example of the finite-dimensional vector space F^n . This has the irreducible subspaces F_i^n , for i ranging from 1 to n , where F_i^n is the F -vector space consisting of the points of coordinates all zero except for in position i . As F -vector spaces, we have that $F_i^n \cong F_j^n$ for all indices i and j , but they are all distinct; they are in fact distinct enough to be in direct sum with one another.

From this example we see the possibility that a module decomposition $M = U_1 \oplus \cdots \oplus U_r$ into its irreducible components has many such components that are isomorphic to each other, though not equal, and in fact are in direct sum with one another. This is important because two isomorphic $F[G]$ -modules induce equivalent representations; and, as we will later see, they have the same character.

Definition 8.9. [6, Definition 1.12] Let W be an irreducible $F[G]$ -module, and let $F[G]$ have the decomposition $F[G] = U_1 \oplus \cdots \oplus U_r$ into irreducible submodules.

The *W -homogeneous part* of $F[G]$, written $W(F[G])$, is the module defined as the direct sum of those composition factors of $F[G]$ which are isomorphic to W . That is:

$$W(F[G]) = \bigoplus_{U_i \cong W} U_i.$$

Let M be an $F[G]$ -module, and let \mathcal{M} be a complete set of representatives of irreducible $F[G]$ -submodules of M . By Maschke's theorem, we have the decomposition:

$$M = U_1 \oplus \cdots \oplus U_n,$$

where each U_i is an irreducible $F[G]$ -submodule of M . In particular, for each U_i , there exists exactly one $W \in \mathcal{M}$ such that $U_i \cong W$, while there may be multiple composition factors of M isomorphic to this same W . Write now $\mathcal{M} = \{W_1, \dots, W_r\}$. We can then group the composition factors of M by which element of \mathcal{M} they are isomorphic to. Then, the sums of such composition factors are precisely the W_i -homogeneous parts of M . We can hence rewrite the decomposition of M as:

$$M = \bigoplus_{i=1}^r W_i(M).$$

Note also that r is the number of equivalence classes of irreducible subrepresentations of M , since it is, by definition of a complete set of representatives, the number of isomorphism classes of the irreducible $F[G]$ -submodules of M .

9 Dimensions of Composition Factors

From this point forward we will only consider the field $F = \mathbb{C}$. The reason to consider this field is that it is a particularly nice field: it has characteristic zero, and it is an algebraically closed field.

The following section is dedicated to an important result on understanding the composition factors of $\mathbb{C}[G]$ -modules, and, in turn, the general structures of irreducible $\mathbb{C}[G]$ -modules.

We begin with a useful proposition extending the result of Schur's lemma.

Proposition 9.1. *[7, Proposition 11.3] Let V and W be two $\mathbb{C}[G]$ -modules. Then, if the modules V and W have no common composition factors, the only $\mathbb{C}[G]$ -homomorphism $V \rightarrow W$ is the zero map.*

Proof. We prove the contrapositive of the statement. Suppose that there exists a nonzero $\mathbb{C}[G]$ -homomorphism $\phi : V \rightarrow W$. Then $\ker \phi$ is a strict submodule of V . By Maschke's theorem (Theorem 7.4) there exists a nonzero complementary $\mathbb{C}[G]$ -module U such that $V = \ker \phi \oplus U$.

As a consequence of Corollary 7.5, there exists at least one irreducible $\mathbb{C}[G]$ -submodule of U , possibly U itself. Let X be such an irreducible submodule. If $\phi(X) = \{0\}$, then $X \subseteq \ker \phi$. But $X \subseteq U$, and, by Proposition 2.13, $U \cap \ker \phi = \{0\}$. Hence $X \subseteq \{0\}$, contradicting that X is irreducible. It follows that the image of ϕ in X is nonzero. Hence, by Schur's lemma, ϕ restricted to the domain X is an isomorphism, and so $\phi(X) \cong X$. We have then found that $\phi(X)$ is an irreducible submodule of W isomorphic to an irreducible submodule of V . By Corollary 8.2, there exists at least one composition factor of W isomorphic to $\phi(X)$, and at least one composition factor of V isomorphic to X , which, by transitivity, establishes that V and W have a common composition factor. \square

The results of this section center around the sets $\text{Hom}_R(U, V)$ of homomorphisms between R -modules; see Example 2.4(6). If the ring R is the group algebra $\mathbb{C}[G]$ for some finite group G , then the set $\text{Hom}_{\mathbb{C}[G]}(U, V)$, being a $\mathbb{C}[G]$ -module, also has the structure of a \mathbb{C} -vector space.

Proposition 9.2. *[7, Proposition 11.4] Let V_1, V_2, W_1, W_2 be $\mathbb{C}[G]$ -modules. Then:*

- (1) $\dim \text{Hom}_{\mathbb{C}[G]}(V_1, W_1 \oplus W_2) = \dim \text{Hom}_{\mathbb{C}[G]}(V_1, W_1) + \dim \text{Hom}_{\mathbb{C}[G]}(V_1, W_2),$
- (2) $\dim \text{Hom}_{\mathbb{C}[G]}(V_1 \oplus V_2, W_1) = \dim \text{Hom}_{\mathbb{C}[G]}(V_1, W_1) + \dim \text{Hom}_{\mathbb{C}[G]}(V_2, W_1).$

Proof. Let π_1 and π_2 be the projections of $W_1 \oplus W_2$ onto W_1 and W_2 , respectively. Define the mapping:

$$\begin{aligned} f : \text{Hom}_{\mathbb{C}[G]}(V_1, W_1 \oplus W_2) &\rightarrow \text{Hom}_{\mathbb{C}[G]}(V_1, W_1) \oplus \text{Hom}_{\mathbb{C}[G]}(V_1, W_2) \\ \phi &\mapsto (\pi_1 \circ \phi, \pi_2 \circ \phi). \end{aligned}$$

Note that the direct sum $\text{Hom}_{\mathbb{C}[G]}(V_1, W_1) \oplus \text{Hom}_{\mathbb{C}[G]}(V_1, W_2)$ is external. We demonstrate that f is a \mathbb{C} -isomorphism.

That f is a \mathbb{C} -homomorphism is clear, defined as it is through a composition of \mathbb{C} -homomorphisms. Pick $(\phi_1, \phi_2) \in \text{Hom}_{\mathbb{C}[G]}(V_1, W_1) \oplus \text{Hom}_{\mathbb{C}[G]}(V_1, W_2)$. We consider the homomorphism $\phi_1 + \phi_2$. The mapping ϕ_1 has the codomain W_1 , and ϕ_2 has the codomain W_2 , so $\pi_1 \circ (\phi_1 + \phi_2) = \phi_1$, and $\pi_2 \circ (\phi_1 + \phi_2) = \phi_2$. Hence, the homomorphism $\phi_1 + \phi_2$ has the image of (ϕ_1, ϕ_2) under f . This establishes surjection.

Suppose now $\phi \in \ker f$. Then $(\pi_1 \circ \phi)(v) = 0$ and $(\pi_2 \circ \phi)(v) = 0$ for all $v \in V_1$, and so $\phi(v) = (\pi_1 \circ \phi)(v) + (\pi_2 \circ \phi)(v) = 0$ for all $v \in V_1$. This establishes that $\ker f = \{0\}$, and thus, by Proposition 2.7, that f is injective.

We have then established that f is a \mathbb{C} -isomorphism. From elementary linear algebra, we know that $\dim(X \oplus Y) = \dim X + \dim Y$ for vector spaces X and Y , and, furthermore, that dimension is preserved over isomorphism. This establishes (1).

Now pick an arbitrary homomorphism ϕ from $\text{Hom}_{\mathbb{C}[G]}(V_1 \oplus V_2, W_1)$, and write ϕ_1 and ϕ_2 to mean the restrictions of ϕ to the spaces V_1 and V_2 , respectively. We define the mapping:

$$\begin{aligned} h : \text{Hom}_{\mathbb{C}[G]}(V_1 \oplus V_2, W_1) &\rightarrow \text{Hom}_{\mathbb{C}[G]}(V_1, W_1) \oplus \text{Hom}_{\mathbb{C}[G]}(V_2, W_1) \\ \phi &\mapsto (\phi_1, \phi_2). \end{aligned}$$

It is again clear that h is a \mathbb{C} -homomorphism. Let $(\phi^{(1)}, \phi^{(2)}) \in \text{Hom}_{\mathbb{C}[G]}(V_1, W_1) \oplus \text{Hom}_{\mathbb{C}[G]}(V_2, W_1)$. Then the mapping ϕ defined by:

$$\begin{aligned} \phi : V_1 \oplus V_2 &\rightarrow W \\ v_1 + v_2 &\mapsto \phi^{(1)}(v_1) + \phi^{(2)}(v_2) \end{aligned}$$

has the image $(\phi^{(1)}, \phi^{(2)})$ under h . This establishes that h is surjective.

If both the restrictions of a homomorphism $\phi : V_1 \oplus V_2 \rightarrow W_1$ to V_1 and V_2 equal zero, then it must be that ϕ is the zero mapping. Hence h is injective, and a \mathbb{C} -isomorphism. By the same reasoning as that used to establish (1), we establish (2). \square

Corollary 9.3. *[7, Result (11.5)] Let $V = V_1 \oplus \cdots \oplus V_r$, and let $W = W_1 \oplus \cdots \oplus W_s$ be $\mathbb{C}[G]$ -modules decomposed into their irreducible factors. Then:*

$$\dim \text{Hom}_{\mathbb{C}[G]}(V, W) = \sum_{i=1}^r \sum_{j=1}^s \dim \text{Hom}_{\mathbb{C}[G]}(V_i, W_j).$$

Proof. The proof given is my own. We proceed by induction on $r + s$, with $r, s \geq 1$.

The base case of $r + s = 2$ is trivial, as then $r = s = 1$.

Suppose true for all cases where $r + s < n$ for some $n \geq 2$. Suppose then that $r + s = n$. If $r = n - 1$ and $s = 1$, then we find, by Proposition 9.2:

$$\begin{aligned} \dim \text{Hom}_{\mathbb{C}[G]}(V, W) &= \dim \text{Hom}_{\mathbb{C}[G]}(V_1 \oplus \cdots \oplus V_{n-2} \oplus V_{n-1}, W) \\ &= \dim \text{Hom}_{\mathbb{C}[G]}(V_1 \oplus \cdots \oplus V_{n-2}, W) + \dim \text{Hom}_{\mathbb{C}[G]}(V_{n-1}, W). \end{aligned}$$

Then applying the induction hypothesis, we find that:

$$\begin{aligned} \dim \text{Hom}_{\mathbb{C}[G]}(V, W) &= \sum_{i=1}^{n-2} \dim \text{Hom}_{\mathbb{C}[G]}(V_i, W) + \dim \text{Hom}_{\mathbb{C}[G]}(V_{n-1}, W) \\ &= \sum_{i=1}^{n-1} \dim \text{Hom}_{\mathbb{C}[G]}(V_i, W). \end{aligned}$$

Otherwise, suppose $s > 1$. We repeat then a similar argument:

$$\begin{aligned}
& \dim \operatorname{Hom}_{\mathbb{C}[G]}(V, W) \\
&= \dim \operatorname{Hom}_{\mathbb{C}[G]}(V_1 \oplus \cdots \oplus V_r, W_1 \oplus \cdots \oplus W_{s-1} \oplus W_s) \\
&= \dim \operatorname{Hom}_{\mathbb{C}[G]}(V_1 \oplus \cdots \oplus V_r, W_1 \oplus \cdots \oplus W_{s-1}) + \dim \operatorname{Hom}_{\mathbb{C}[G]}(V_1 \oplus \cdots \oplus V_r, W_s) \\
&= \sum_{i=1}^r \sum_{j=1}^{s-1} \dim \operatorname{Hom}_{\mathbb{C}[G]}(V_i, W_j) + \dim \operatorname{Hom}_{\mathbb{C}[G]}(V_1 \oplus \cdots \oplus V_r, W_s) \\
&= \sum_{i=1}^r \sum_{j=1}^s \dim \operatorname{Hom}_{\mathbb{C}[G]}(V_i, W_j).
\end{aligned}$$

Then we are done. \square

Corollary 9.4. [7, Corollary 11.6] *Let $M = U_1 \oplus \cdots \oplus U_r$ be a $\mathbb{C}[G]$ -module decomposed into its irreducible factors. Let V be some irreducible $\mathbb{C}[G]$ -module. Then both $\dim \operatorname{Hom}_{\mathbb{C}[G]}(M, V)$ and $\dim \operatorname{Hom}_{\mathbb{C}[G]}(V, M)$ equal the number of composition factors U_i of M that are isomorphic to V .*

Proof. Let V and W be irreducible $\mathbb{C}[G]$ -modules. If $V \not\cong W$, then by Schur's lemma, $\operatorname{Hom}_{\mathbb{C}[G]}(V, W) = \{0\}$, and so $\dim \operatorname{Hom}_{\mathbb{C}[G]}(V, W) = \dim \{0\} = 0$.

Otherwise, if $V \cong W$, let $\phi : V \rightarrow W$. Since V and W are isomorphic as $\mathbb{C}[G]$ -modules, they are also isomorphic as \mathbb{C} -vector spaces. In particular, $n = \dim V = \dim W$, hence there exist isomorphisms $f : V \rightarrow \mathbb{C}^n$ and $h : W \rightarrow \mathbb{C}^n$.

Define the mapping $\psi : \mathbb{C}^n \rightarrow \mathbb{C}^n$ by $v \mapsto h(\phi(f^{-1}(v)))$. As a complex endomorphism, the mapping ψ has some eigenvalue λ ; [7, Result (2.26)]. By definition of an eigenvalue, we have that $\psi(v) = \lambda v$ for some nonzero $v \in V$. In particular, $\ker(\psi - \lambda \cdot \operatorname{id}) \neq \{0\}$. Thus, as a submodule of an irreducible module V , by Schur's lemma, $\ker(\psi - \lambda \cdot \operatorname{id}) = V$, and so $\psi - \lambda \cdot \operatorname{id} = 0$. Hence $\psi = \lambda \cdot \operatorname{id}$.

Since $\psi = h(\phi(f^{-1}))$, we have that $h(\phi(f^{-1})) = \lambda \cdot \operatorname{id}$, which, since f, h are bijective \mathbb{C} -homomorphisms, gives that $\phi = \lambda h(\operatorname{id}(f))$. Hence, $\operatorname{Hom}_{\mathbb{C}[G]}(V, W) \subseteq \{\lambda h(\operatorname{id}(f)) \mid \lambda \in \mathbb{C}\}$. We know that $\operatorname{Hom}_{\mathbb{C}[G]}(V, W)$ is a \mathbb{C} -vector space and has at least one nonzero element, being an isomorphism $V \rightarrow W$, and so $\dim \operatorname{Hom}_{\mathbb{C}[G]}(V, W) = 1$.

By Corollary 9.3, we have:

$$\begin{aligned}
\dim \operatorname{Hom}_{\mathbb{C}[G]}(M, V) &= \sum_{i=1}^r \dim \operatorname{Hom}_{\mathbb{C}[G]}(U_i, V), \\
\dim \operatorname{Hom}_{\mathbb{C}[G]}(V, M) &= \sum_{i=1}^r \dim \operatorname{Hom}_{\mathbb{C}[G]}(V, U_i).
\end{aligned}$$

In particular, the module V and all of the composition factors U_i are irreducible, so both of these sums equal the number of U_i that are isomorphic to V . \square

We finish this section with the main result of interest.

Theorem 9.5. [7, Theorem 11.9] *Write $\mathbb{C}[G] = U_1 \oplus \cdots \oplus U_r$, decomposed into irreducible submodules. Let V be an irreducible $\mathbb{C}[G]$ -module. Then $\dim V$ equals the number of U_i such that $U_i \cong V$.*

Proof. This proof is taken from the proof of [7, Theorem 11.9] combined with that of [7, Proposition 11.8].

First, we show that $\dim \operatorname{Hom}_{\mathbb{C}[G]}(\mathbb{C}[G], V) = \dim V$. Let $d = \dim V$, and let u_1, \dots, u_d be a basis of the \mathbb{C} -vector space V . We then define the mappings:

$$\begin{aligned}\phi_i : \mathbb{C}[G] &\rightarrow V \\ r &\mapsto ru_i,\end{aligned}$$

for $1 \leq i \leq d$. We show then that ϕ_1, \dots, ϕ_d form a basis for $\operatorname{Hom}_{\mathbb{C}[G]}(\mathbb{C}[G], V)$.

Let $\phi \in \operatorname{Hom}_{\mathbb{C}[G]}(\mathbb{C}[G], V)$. Then there exist $\lambda_1, \dots, \lambda_d \in \mathbb{C}$ such that $\phi(1e) = \lambda_1 u_1 + \dots + \lambda_d u_d$, since $\phi(1e) \in V$ and u_1, \dots, u_d form a basis for V . Then, if $r \in \mathbb{C}[G]$ is some arbitrary scalar element, we find that:

$$\phi(r) = r\phi(1e) = \lambda_1 ru_1 + \dots + \lambda_d ru_d = \lambda_1 \phi_1(r) + \dots + \lambda_d \phi_d(r).$$

Hence, $\phi = \lambda_1 \phi_1 + \dots + \lambda_d \phi_d$. We have then established that ϕ_1, \dots, ϕ_d span the space $\operatorname{Hom}_{\mathbb{C}[G]}(\mathbb{C}[G], V)$.

Suppose now that $\lambda_1 \phi_1 + \dots + \lambda_d \phi_d = 0$ for some scalars $\lambda_1, \dots, \lambda_d$. Evaluating both sides of this equation at the identity element $1e$, we get:

$$\lambda_1 u_1 + \dots + \lambda_d u_d = 0.$$

Since u_1, \dots, u_d are a basis, they are linearly independent. It follows then that $\lambda_1 = \lambda_2 = \dots = \lambda_d = 0$. This establishes linear independence of ϕ_1, \dots, ϕ_d . We have then showed that $d = \dim \operatorname{Hom}_{\mathbb{C}[G]}(\mathbb{C}[G], V) = \dim V$.

We now proceed to conclude the theorem. By Corollary 9.4, $\dim \operatorname{Hom}_{\mathbb{C}[G]}(\mathbb{C}[G], V)$ equals the number of composition factors U_i of $\mathbb{C}[G]$ that are isomorphic to V . This is then precisely $\dim V$, and we are done. \square

While the statement of Theorem 9.5 applies specifically to irreducible submodules of $\mathbb{C}[G]$, it also applies to all irreducible $\mathbb{C}[G]$ -modules. By Theorem 8.4, each irreducible $\mathbb{C}[G]$ -module is isomorphic to a composition factor of $\mathbb{C}[G]$, hence to an irreducible submodule of $\mathbb{C}[G]$. However, if we consider U as an irreducible $\mathbb{C}[G]$ -submodule of some $\mathbb{C}[G]$ -module M , then $\dim U$ is not necessarily the same as the number of composition factors of M that are isomorphic to U .

While the utility of this theorem is not immediately obvious, it allows for a more complete understanding of the composition factors of a representation.

10 Characters

The following section is dedicated to characters, a related study to that of representations. The definition of a character is more easily understood when considering representations as homomorphisms, but can also apply to representations considered as modules.

Before defining characters, we review conjugacy classes of groups, which, as will be seen, are key to the study of characters.

Definition 10.1. Let G be a group. Two elements x, y of G are called *conjugates* if there exists $g \in G$ for which:

$$x = gyg^{-1}.$$

This is an equivalence relation: for reflexivity, pick $g = e$; for symmetry, if $x = gyg^{-1}$ then $y = g^{-1}xg$; for transitivity, if $x = gyg^{-1}$ and $y = hzh^{-1}$, then $x = (gh)z(gh)^{-1}$.

The equivalence classes for this relation are called the *conjugacy classes* of G . As equivalence classes, furthermore, the conjugacy classes of a group form a partition of the set G . An element of a conjugacy class will be called a *representative* of the conjugacy class.

A pertinent example of conjugacy classes will follow after the proposition.

Proposition 10.2. Let G a group, and let C be a conjugacy class in G with representative x . Then:

$$C = \{gxg^{-1} \mid g \in G\}.$$

Proof. (\supseteq) Pick arbitrary $g \in G$. Then x and gxg^{-1} are conjugates, since $x = g^{-1}gxg^{-1}g$, and so gxg^{-1} is a member of the equivalence class C .

(\subseteq) If x, y are conjugates, then $x = gyg^{-1}$ for some $g \in G$. Then $y = g^{-1}xg$, and hence $y \in \{gxg^{-1} \mid g \in G\}$. \square

Example 10.3. In \mathcal{S}_n , the conjugacy classes are the sets of permutations of the same form; for example, the set of transpositions, the set of 3-cycles, the set of products of transpositions, etc. This can be observed through the following identities:

$$\begin{aligned}\sigma(a_1 \cdots a_r)\sigma^{-1} &= (\sigma(a_1) \cdots \sigma(a_r)); \\ \sigma\tau_1\tau_2\sigma^{-1} &= \sigma\tau_1\sigma\sigma^{-1}\tau_2\sigma^{-1},\end{aligned}$$

where τ_1 and τ_2 are disjoint cycles in \mathcal{S}_n . This makes it relatively easy to count the number of conjugacy classes of \mathcal{S}_n . The group \mathcal{S}_3 has three conjugacy classes: the set $\{e\}$, which is always a conjugacy class; the set of transpositions, that is, 2-cycles; and the set of 3-cycles. The group \mathcal{S}_4 has five conjugacy classes: $\{e\}$, transpositions, 3-cycles, 4-cycles, and products of two transpositions.

Having reviewed conjugacy classes of groups, we proceed to define the character of a group, beginning by recalling the definition of the trace of a matrix.

Definition 10.4. Let A be an $n \times n$ matrix over a field F . Then the *trace* of A , written $\text{tr } A$, is defined as the sum of all of the diagonal entries of A . That is:

$$\text{tr } A = \sum_{k=1}^n A_{kk}.$$

Definition 10.5. [7, Definition 13.3] Let $\rho : G \rightarrow GL_n(\mathbb{C})$ be a representation. Then the *character* of ρ is the function $\chi : G \rightarrow \mathbb{C}$ defined by:

$$\chi(g) = \text{tr } \rho(g).$$

Any arbitrary function $G \rightarrow \mathbb{C}$ is called a character if it is the character of some representation. The character then inherits many of its properties directly from the representation: the *degree* of a character is the degree of the representation of which it is a character; and a character is called *irreducible* if it is the character of an irreducible representation.

Example 10.6.

- (1) If ρ is a representation of degree 1, such as the trivial representation of (\mathbb{Q}^*, \cdot) defined $\rho : a \mapsto [a]$, then the character χ of ρ is the same as ρ . Such characters of degree 1 are called *linear characters*.
- (2) Consider the geometric representation of degree 2 of the group D_8 . Let $\tau \in D_8$ denote the symmetry of rotation counter-clockwise by $\frac{\pi}{2}$, and let σ denote the symmetry over the y -axis. From Example 4.3(3), we find a representation, ρ , defined through:

$$\rho(\tau) = T; \quad \rho(\sigma) = S,$$

with the matrices T and S being:

$$T = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}; \quad S = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Then we can see that $\text{tr } T = 0$ and $\text{tr } S = 0$. Hence, the character χ of the representation ρ takes the values:

$$\chi(\tau) = \text{tr } \rho(\tau) = 0; \quad \chi(\sigma) = \text{tr } \rho(\sigma) = 0.$$

Unlike with representations, the character of a group cannot be understood in general through a set of generators for a group. However there is a more condensed way of looking at the characters of a group through its conjugacy classes that will be explored further in the section.

- (3) Consider the canonical representation of degree n of the group \mathcal{S}_n . From Example 4.3(6), we observe that the 1's on the diagonal of the canonical matrix representation of a permutation σ are precisely those indices which remain fixed under the permutation. Hence, $\chi(\sigma)$ equals the number of elements that remain fixed under the permutation σ .
- (4) Consider the group \mathcal{S}_3 . The cycles of this group can have length 1, 2, or 3, and so the character of the canonical representation of a cycle $\sigma \in \mathcal{S}_3$ is $3 - \ell$, where ℓ is the length of the cycle. We can see this through the following example:

$$\begin{aligned} \chi(e) &= \text{tr} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = 3; & \chi((12)) &= \text{tr} \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} = 1; \\ \chi((123)) &= \text{tr} \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} = 0. \end{aligned}$$

A further consequence is that the character of the group \mathcal{S}_3 is constant on its conjugacy classes, which are the sets of cycles of the same form (see Example 10.3). This is in fact true in general of all group characters, as will be proven shortly.

We will now prove a few properties of trace, which translate directly to properties of characters.

Proposition 10.7. [7, Proposition 13.2] *Let A, B be $n \times n$ matrices. Then:*

- $\text{tr}(A + B) = \text{tr } A + \text{tr } B$;
- $\text{tr}(AB) = \text{tr}(BA)$.

Proof. The first point is almost immediate.

For the second point, we apply the formal definition of matrix multiplication:

$$\text{tr}(AB) = \sum_{r=1}^n \sum_{s=1}^n A_{rs} B_{sr}.$$

Then the order of the summations does not matter here, so they can be exchanged:

$$\text{tr}(AB) = \sum_{s=1}^n \sum_{r=1}^n A_{rs} B_{sr} = \sum_{s=1}^n \sum_{r=1}^n B_{sr} A_{rs} = \text{tr}(BA). \quad \square$$

There is an immediate and quite useful corollary to this proposition. Suppose that ρ and τ are two equivalent representations of a group G . Then that means that there exists an invertible matrix T such that:

$$\rho(g) = T\tau(g)T^{-1}.$$

Then by Proposition 10.7 and associativity of matrix multiplication:

$$\text{tr } \rho(g) = \text{tr}((T\tau(g))T^{-1}) = \text{tr}(T^{-1}T\tau(g)) = \text{tr } \tau(g).$$

The conclusion is that equivalent representations have the same character. In particular, since there are finitely many irreducible $\mathbb{C}[G]$ -modules for any finite group G , there are finitely many irreducible representations up to equivalence, and hence finitely many irreducible characters of a group. Viewed as modules, equivalent representations are isomorphic modules (Proposition 5.7), and, as such, isomorphic representations viewed as modules have the same character.

Another consequence of Proposition 10.7 is the following:

Proposition 10.8. [7, Proposition 13.5(2)] *Let G be a finite group, and let C be some conjugacy class in G . Let ρ be a representation of G and let χ be its character. Then χ is constant on C .*

Proof. Pick $x, y \in C$. Then there exists $g \in G$ such that $x = gyg^{-1}$. Since ρ is a homomorphism, $\rho(x) = \rho(g)\rho(y)\rho(g)^{-1}$. Hence $\text{tr } \rho(x) = \text{tr } \rho(y)$, so $\chi(x) = \chi(y)$. \square

It is for this reason that conjugacy classes are important to consider in the study of characters, leading us to the following definition.

Definition 10.9. [8, Definition 6.1] Let G be a group and let T be some set. Then a function $\psi : G \rightarrow T$ is called a *class function* if $\psi(x) = \psi(y)$ whenever x and y are conjugate elements.

The set of class functions $G \rightarrow T$ is denoted $T_{\text{class}}(G)$. For the purposes of this thesis we will consider the set $\mathbb{C}_{\text{class}}(G)$.

Example 10.10. Let G be a finite group with conjugacy classes C_1, \dots, C_r . Then the mapping which maps each element of G to the index i of the conjugacy class to which it belongs is a class function.

If G is a finite group, then G also has finitely many conjugacy classes. As such, each character of G can be identified by its value on each conjugacy class of G , and so, a character of a group can be expressed in a tabular manner.

Let G be a group with conjugacy classes C_1, \dots, C_r , and let χ be a character of G such that χ takes the value x_i on the conjugacy class C_i . Then the character χ can be expressed thusly:

$$\begin{array}{c|cccc} & C_1 & C_2 & \cdots & C_r \\ \hline \chi & x_1 & x_2 & \cdots & x_r \end{array}.$$

In fact, we can extend this table to list all of the irreducible characters of a group, of which there are finitely many. Let χ_1, \dots, χ_s be the irreducible characters of the group G . Then:

$$\begin{array}{c|cccc} & C_1 & C_2 & \cdots & C_r \\ \hline \chi_1 & x_1^{(1)} & x_2^{(1)} & \cdots & x_r^{(1)} \\ \chi_2 & x_1^{(2)} & x_2^{(2)} & \cdots & x_r^{(2)} \\ \vdots & \vdots & \vdots & & \vdots \\ \chi_s & x_1^{(s)} & x_2^{(s)} & \cdots & x_r^{(s)} \end{array}$$

is the *character table* of G .

Example 10.11. [7, modified from Example 13.6(4)] We present, without proof, the character table for the symmetric group \mathcal{S}_3 :

$$\begin{array}{c|ccc} & \{e\} & \{(1\ 2\ 3), (2\ 1\ 3)\} & \{(1\ 2), (1\ 3), (2\ 3)\} \\ \hline \chi_1 & 1 & 1 & 1 \\ \chi_2 & 1 & 1 & -1 \\ \chi_3 & 2 & -1 & 0 \end{array}$$

The groups \mathcal{S}_3 and D_6 are isomorphic, which one can find through observing that all permutations of 3 elements are rigid permutations (see Example 4.3(7)). The geometric representation ρ of D_6 , with conjugacy classes $\{e\}$, $\{r, r^2\}$, and $\{s, sr, sr^2\}$, for r a rotation by $\frac{2\pi}{3}$ counterclockwise and s a reflection over the x -axis, takes values:

$$\rho(e) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}; \quad \rho(r) = \begin{bmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{bmatrix}; \quad \rho(sr) = \begin{bmatrix} \frac{1}{2} & \frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{bmatrix}.$$

From this, we find that the character of the representation ρ is the character χ_3 from the table.

Character tables are key to the study of character theory, though are not explored in depth in this thesis. The reader may read further about the *orthogonality relations* if further interested in the computation of character tables.

We finish the section with some properties of characters and how they can be understood through the decompositions of representations.

Proposition 10.12. [7, Proposition 13.20] Let G be a finite group, and let χ be the character of the representation $\mathbb{C}[G]$ itself. Then:

$$\begin{aligned} \chi(e) &= |G|; \\ \chi(g) &= 0 \text{ for } g \neq e. \end{aligned}$$

Proof. Write $G = \{g_1, \dots, g_n\}$. Then since the \mathbb{C} -dimension of $\mathbb{C}[G]$ is n , the character χ evaluated at the identity element e equals the trace of the $n \times n$ identity matrix, which is $n = |G|$.

Now pick $g \in G \setminus \{e\}$. Then for all indices $1 \leq i \leq n$, we have that $gg_i = g_j$, where $i \neq j$ (otherwise, by cancellation, g would necessarily be the identity element). Thus the matrix of the \mathbb{C} -endomorphism $v \mapsto g \cdot v$ in the basis G consists of a 1 in row i column j if $gg_i = g_j$, and 0 otherwise. But since $i \neq j$, all elements on the diagonal are 0, and it follows that the trace of this matrix is 0. Hence, by definition of the character of g , we have that $\chi(g) = 0$ for all $g \neq e$. \square

Proposition 10.13. [8, Proposition 6.4] Let M be a $\mathbb{C}[G]$ -module with decomposition into $M = U_1 \oplus \cdots \oplus U_r$. Then the character of M is given by:

$$\chi_M = \chi_1 + \cdots + \chi_r,$$

where each χ_i is the irreducible character of the $\mathbb{C}[G]$ -module U_i .

Proof. As M has this decomposition, its representation as a homomorphism takes the block diagonal form:

$$\begin{bmatrix} \boxed{\rho_1} & & 0 \\ & \ddots & \\ 0 & & \boxed{\rho_r} \end{bmatrix},$$

where ρ_i is the representation as a homomorphism of the $\mathbb{C}[G]$ -module U_i . In this form it is easy to see that the trace of this matrix is the sum of the traces of the blocks in the diagonal, which are precisely χ_1, \dots, χ_r . \square

Note however that not every one of these irreducible characters is necessarily distinct. Given the decomposition $M = U_1 \oplus \cdots \oplus U_r$, if $U_i \cong U_j$, then their characters χ_i and χ_j , respectively, are equal. Hence there exists some $s \leq r$ and some natural numbered coefficients n_1, \dots, n_s such that:

$$\chi = n_1\chi_1 + \cdots + n_s\chi_s,$$

where here, in this case, the characters χ_1, \dots, χ_s are the distinct irreducible characters among those of U_1, \dots, U_r . In particular, χ_1, \dots, χ_s are the characters of the elements of \mathcal{M} , where \mathcal{M} is a complete set of representatives of the irreducible submodules of the $\mathbb{C}[G]$ -module M .

Example 10.14. Consider the group \mathcal{S}_3 and let ρ be its canonical representation. From Example 10.6(4) we know that the character χ of ρ evaluated at a permutation $\sigma \in \mathcal{S}_3$ equals $3 - \ell$, where ℓ is the length of the cycle σ . Picking appropriate representatives for the conjugacy classes \mathcal{S}_3 , we have:

$$\chi(e) = 3; \quad \chi((12)) = 1; \quad \chi((123)) = 0.$$

From Example 10.11 we have the character table of \mathcal{S}_3 , from which we can observe that $\chi = \chi_3 + \chi_1$.

Example 10.15. [7, modified from Example 13.21] From Example 10.11, the character table for the group \mathcal{S}_3 shows the irreducible characters χ_1, χ_2 , and χ_3 of the group and their values on each conjugacy class of \mathcal{S}_3 . We demonstrate that the character of the representation $\mathbb{C}[\mathcal{S}_3]$ is $\chi_1 + \chi_2 + 2\chi_3$. By Proposition 10.12, the character of the representation $\mathbb{C}[\mathcal{S}_3]$ is $6 = |\mathcal{S}_3|$ at e , the identity element, and 0 otherwise. We test this for the three conjugacy classes of \mathcal{S}_3 :

$$\begin{aligned} \chi_1(e) + \chi_2(e) + 2\chi_3(e) &= 1 + 1 + 2(2) = 6; \\ \chi_1((123)) + \chi_2((123)) + 2\chi_3((123)) &= 1 + 1 + 2(-1) = 0; \\ \chi_1((12)) + \chi_2((12)) + 2\chi_3((12)) &= 1 + (-1) + 2(0) = 0. \end{aligned}$$

This gives a few hints about the structure of the representations of \mathcal{S}_3 : first, that there are some irreducible representations U_1 , U_2 , and U_3 with respective characters χ_1 , χ_2 and χ_3 . This hints also that there are two isomorphic distinct representations with the character χ_3 , and so there is a representation U_4 that is isomorphic, but not equal to, U_3 . By Theorem 9.5, both U_3 and U_4 have dimension 2, while U_1 and U_2 each have dimension 1. The total dimension is then 6, being the dimension of the group algebra $\mathbb{C}[\mathcal{S}_3]$.

We have not reviewed and will not review the precise details of how these results are derived, but it is an informal demonstration of how characters help to understand the structure of the representations of a group.

11 Inner Products of Characters

Let G be a finite group. Consider the set $\mathbb{C}_{\text{class}}(G)$ of complex-valued class functions on G . This has the structure of a \mathbb{C} -vector space through usual addition of functions:

$$(\phi + \psi)(x) = \phi(x) + \psi(x),$$

and scalar multiplication defined as:

$$(\lambda\phi)(x) = \lambda(\phi(x)).$$

It is easy to see that this vector space is closed under both operations: a sum of class functions remains a class function, and a scalar multiple of a class function also remains a class function.

Proposition 11.1. *Let G be a finite group. Then the dimension of $\mathbb{C}_{\text{class}}(G)$ is equal to the number of conjugacy classes of G .*

Proof. Suppose that G has r conjugacy classes. We will proceed by demonstrating an isomorphism $\mathbb{C}_{\text{class}}(G) \rightarrow \mathbb{C}^r$. Let g_1, \dots, g_r be a complete set of representatives for the conjugacy classes C_1, \dots, C_r of G . Define the mapping $\Phi : \mathbb{C}_{\text{class}}(G) \rightarrow \mathbb{C}^r$ by:

$$\Phi(\psi) = (\psi(g_1), \psi(g_2), \dots, \psi(g_r)).$$

It is easy to see that Φ is a \mathbb{C} -homomorphism.

Let ψ, ϕ be two complex class functions on G . To show that Φ is injective, we note first that $\psi = \phi \iff \psi(g_i) = \phi(g_i)$ for all $1 \leq i \leq r$. This fact comes from that the functions are class functions: we need only check their equality on each representative of the conjugacy classes of G . That $\psi(g_i) = \phi(g_i)$ for all $1 \leq i \leq r$ is equivalent to saying that the vectors $(\psi(g_1), \dots, \psi(g_r))$ and $(\phi(g_1), \dots, \phi(g_r))$ are equal. This establishes injectivity.

To show that Φ is surjective, it suffices to note that given a vector $(z_1, \dots, z_r) \in \mathbb{C}^r$, the function which maps each element of C_i to z_i for $1 \leq i \leq r$, is a class function. Then we have shown that $\mathbb{C}_{\text{class}}(G) \cong \mathbb{C}^r$, and hence $\dim \mathbb{C}_{\text{class}}(G) = r$. \square

We will now proceed to recall the definition of a complex inner product:

Definition 11.2. Let V be a \mathbb{C} -vector space. A function $V \times V \rightarrow \mathbb{C}$, written $(x, y) \mapsto \langle x, y \rangle$ is called an *inner product* on V if it satisfies, for all $x, y \in V$, $a \in \mathbb{C}$:

- (1) $\langle x, y \rangle = \overline{\langle y, x \rangle}$;
- (2) $a \langle x, y \rangle = \langle ax, y \rangle = \langle x, \bar{a}y \rangle$;⁵
- (3) $\langle x, y \rangle + \langle z, y \rangle = \langle x + z, y \rangle$;
- (4) $\langle x, x \rangle > 0$; and $\langle x, x \rangle = 0 \iff x = 0$.

The vector space V equipped with this inner product is called an *inner product space*. Two elements x and y of an inner product space V are called *orthogonal* if $\langle x, y \rangle = 0$. A collection x_1, \dots, x_n of elements of V is called an *orthonormal set* if $\langle x_i, x_j \rangle = 1$ when $i = j$, and $\langle x_i, x_j \rangle = 0$ otherwise.

⁵Note that the second equals sign in (2) is a consequence of the first equals sign of (2) and property (1), though for clarity it is included in the definition.

Example 11.3. Consider the \mathbb{C} -vector space \mathbb{C}^n . Then the mapping defined, for $x := (x_1, \dots, x_n)$, $y := (y_1, \dots, y_n) \in \mathbb{C}^n$, by:

$$\langle x, y \rangle = \sum_{i=1}^n x_i \overline{y_i}$$

is a complex inner product in \mathbb{C}^n . The vectors $(1, 0, 0, \dots, 0)$ and $(0, 1, 0, \dots, 0)$ are orthogonal in this inner product space. The vectors $e_i \in \mathbb{C}^n$ defined as the vectors with 1 as the i 'th coordinate and 0 in all other coordinates form an orthonormal set in this inner product space. They furthermore form a basis for \mathbb{C}^n , and as such are called an *orthonormal basis*.

We now proceed to define an inner product on the set of complex class functions of a group G .

Definition 11.4. [7, Definition 14.3] Let G be a finite group, and consider the complex vector space $\mathbb{C}_{\text{class}}(G)$. We define an inner product on this space by:

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

We show that this is a complex inner product space. Properties (1), (2), and (3) are quite immediate from the definition.

For (4), we observe that $z\overline{z} = |z|^2$, which is real, and it is equal to zero if and only if $z = 0$. Letting $\phi \in \mathbb{C}_{\text{class}}(G)$, we have:

$$\langle \phi, \phi \rangle = \frac{1}{|G|} \sum_{g \in G} |\phi(g)|^2.$$

Since $|\phi(g)|^2 \geq 0$, with equality only when $\phi(g) = 0$, we can see that the sum will equal zero only when $\phi(g) = 0$ for all $g \in G$; that is, when ϕ is the zero function. This proves property (4).

One may note the similarity of this inner product to that of the typical scalar product in \mathbb{C}^n shown in Example 11.3, with class functions treated as vectors whose coordinates are the elements of the group G . One can see in the definition that the value of the class function on a conjugacy class with more elements is “weighted” more in the inner product.

The remainder of the section is dedicated to proving a useful result about the irreducible characters of a group: that they form an orthonormal basis for the inner product space $\mathbb{C}_{\text{class}}(G)$. We prove this through two involved theorems: first, that the irreducible characters form an orthonormal set in the inner product space $\mathbb{C}_{\text{class}}(G)$; and second, that the number of distinct irreducible characters of G is precisely $\dim \mathbb{C}_{\text{class}}(G)$.

Lemma 11.5. [[5, Corollary 13.19] and [7, Proposition 14.5]] Let χ, ψ be characters of a finite group G . Then the following hold:

- (1) $\chi(g^{-1}) = \overline{\chi(g)}$ for all $g \in G$;
- (2) $\langle \chi, \psi \rangle = \langle \psi, \chi \rangle$.

Proof. To prove (1), we will apply, without proof, some nontrivial results from linear algebra:

- If A is an $n \times n$ complex matrix of finite order k , then the eigenvalues of A are all k 'th roots of unity; that is, $\omega \in \mathbb{C}$ such that $\omega^k = 1$; [5, Corollary 13.15].
- If A is an invertible $n \times n$ complex matrix with eigenvalues $\lambda_1, \dots, \lambda_n$, then the eigenvalues of A^{-1} are $\lambda_1^{-1}, \dots, \lambda_n^{-1}$; [5, Corollary 13.14].

- If A is an $n \times n$ complex matrix, then the trace of A equals the sum of its (possibly repeated) eigenvalues; [5, Proposition 13.11].

The proofs are omitted, as they are purely linear algebraic results outside of the scope of the thesis; the reader may read through Chapter 13 of [5] if interested in the details.

Let $g \in G$. Since G is a finite group, the element g has finite order $\ell \in \mathbb{Z}^+$. Let ρ be a representation that has the character χ . Then $\rho(g)$ is a matrix of finite order k dividing ℓ , since $(\rho(g))^\ell = \rho(g^\ell) = \rho(e) = I_n$.

Let $\omega \in \mathbb{C}$ such that $\omega^k = 1$. Then $|\omega^k| = |\omega|^k = 1$, and so, since the modulus of a complex number is real and positive, it must be that $|\omega| = 1$. Then $\omega\bar{\omega} = |\omega| = 1$, and we have then that $\omega^{-1} = \bar{\omega}$.

Let $\omega_1, \dots, \omega_n$ be the eigenvalues of the finite-order matrix $\rho(g)$. Then the eigenvalues of $\rho(g)^{-1} = \rho(g^{-1})$ are $\omega_1^{-1}, \dots, \omega_n^{-1}$. Then the traces of these matrices are the sums of their respective eigenvalues. In particular, we have:

$$\chi(g) = \omega_1 + \dots + \omega_n; \quad \chi(g^{-1}) = \omega_1^{-1} + \dots + \omega_n^{-1}.$$

But then each ω_i is a k 'th root of unity, and so $\omega_i^{-1} = \bar{\omega}_i$. This gives:

$$\chi(g^{-1}) = \bar{\omega}_1 + \dots + \bar{\omega}_n = \overline{\omega_1 + \dots + \omega_n} = \overline{\chi(g)}.$$

This establishes (1). To show (2), we write the inner product of the characters χ and ψ :

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

Reindexing the sum to $h = g^{-1}$, we find:

$$\frac{1}{|G|} \sum_{g \in G} \chi(g) \overline{\psi(g)} = \frac{1}{|G|} \sum_{h \in G} \overline{\psi(h^{-1})} \chi(h^{-1}).$$

Lastly, applying (1), we have:

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

Then we have established (2). □

Lemma 11.6. [7, Corollary 14.11] *Let G be a finite group. Suppose that there exist $\mathbb{C}[G]$ -submodules W_1 and W_2 of $\mathbb{C}[G]$ such that:*

- $\mathbb{C}[G] = W_1 \oplus W_2$;
- W_1 and W_2 have no common composition factors.

Then the character χ of the representation W_1 satisfies that:

$$\langle \chi, \chi \rangle = \chi(e).$$

Proof. Write $1e$, the multiplicative identity element of the ring $\mathbb{C}[G]$, as $1e = e_1 + e_2$, where $e_1 \in W_1$ and $e_2 \in W_2$.

Pick arbitrary $w_2 \in W_2$, and consider the $\mathbb{C}[G]$ -homomorphism:

$$\begin{aligned} f : W_1 &\rightarrow W_2 \\ w_1 &\mapsto w_1 \cdot w_2. \end{aligned}$$

By Proposition 9.1, since W_1 and W_2 have no common composition factors, it must be that f is the zero map. Hence $w_1 \cdot w_2 = 0$ for all $w_1 \in W_1$. Then we repeat this argument for all $w_2 \in W_2$ to find that $w_1 \cdot w_2 = 0$ for all $w_1 \in W_1$ and all $w_2 \in W_2$. We also find, by the same argument, that $w_2 \cdot w_1 = 0$ for all $w_1 \in W_1$ and $w_2 \in W_2$, by instead defining the mapping $h : w_1 \mapsto w_2 \cdot w_1$.

Now pick arbitrary $w_1 \in W_1$ and $w_2 \in W_2$. Then:

$$w_1 = (1e)w_1 = (e_1 + e_2)w_1 = e_1w_1 + e_2w_1 = e_1w_1,$$

and so $e_1w_1 = w_1$. Similarly we find that $e_2w_2 = w_2$.

In particular, we have the following three identities:

$$\begin{aligned} e_1e_2 &= e_2e_1 = 0; \\ e_1^2 &= e_1; \\ e_2^2 &= e_2. \end{aligned}$$

Having established some properties of e_1 and e_2 , we proceed to find an expression for the element e_1 .

Pick $x \in G$. Then we consider the mapping $\phi : \mathbb{C}[G] \rightarrow \mathbb{C}[G]$ defined as $w \mapsto x^{-1}e_1w$. We show that this is a \mathbb{C} -endomorphism. If $v, w \in \mathbb{C}[G]$, then we have:

$$\phi(v + w) = x^{-1}e_1(v + w) = x^{-1}e_1v + x^{-1}e_1w = \phi(v) + \phi(w).$$

If $\lambda \in \mathbb{C}$, then by property (1) of algebras over a field (Definition 3.1(1)), we have that $\lambda((x^{-1}e_1)w) = (x^{-1}e_1)(\lambda w)$, and so $\lambda\phi(w) = \phi(\lambda w)$.

We now consider what the \mathbb{C} -endomorphism ϕ looks like on the spaces W_1 and W_2 . Pick $w_1 \in W_1$ and $w_2 \in W_2$. Then:

$$\begin{aligned} \phi(w_1) &= x^{-1}e_1w_1 = x^{-1}w_1; \\ \phi(w_2) &= x^{-1}e_1w_2 = 0. \end{aligned}$$

Thus ϕ is zero on W_2 , and $\phi(w_1)$ is $x^{-1}w_1$ for all $w_1 \in W_1$. The matrix of the \mathbb{C} -endomorphism ϕ is then:

$$\left[\begin{array}{c|c} \rho_1(x^{-1}) & 0 \\ \hline 0 & 0 \end{array} \right],$$

where ρ_1 is the representation as a homomorphism of the $\mathbb{C}[G]$ -module W_1 . The trace of this matrix is then $\chi(x^{-1})$, where χ is the character of the representation W_1 .

Since $e_1 \in \mathbb{C}[G]$, there exist $\lambda_g \in \mathbb{C}$ such that $e_1 = \sum_{g \in G} \lambda_g g$. Then:

$$\phi(w) = x^{-1} \left(\sum_{g \in G} \lambda_g g \right) w = \left(\sum_{g \in G} \lambda_g x^{-1}g \right) w.$$

Write $G = \{g_1, \dots, g_n\}$. The homomorphism ϕ can then be expressed as a sum of homomorphisms $\phi = \lambda_{g_1}\mu_{x^{-1}g_1} + \dots + \lambda_{g_n}\mu_{x^{-1}g_n}$, where the mappings μ_h are defined by $\mu_h : w \mapsto hw$ for $h \in G$. The matrix of ϕ in the basis G is thus the sum:

$$\lambda_{g_1}\rho(x^{-1}g_1) + \lambda_{g_2}\rho(x^{-1}g_2) + \dots + \lambda_{g_n}\rho(x^{-1}g_n),$$

where ρ is the representation $\mathbb{C}[G]$ viewed as a homomorphism of groups. By Proposition 10.7, the trace of this matrix is the sum of the traces of each $\lambda_{g_i}\rho(x^{-1}g_i)$. Thus:

$$\text{tr } \phi = \lambda_{g_1}\psi(x^{-1}g_1) + \lambda_{g_2}\psi(x^{-1}g_2) + \dots + \lambda_{g_n}\psi(x^{-1}g_n),$$

where ψ is the character of the representation ρ . By Proposition 10.12, we have that $\psi(g) = 0$ if $g \neq e$, and $\psi(e) = n = |G|$. In particular, $x^{-1}g_i = e$ if and only if $g_i = x$. From these results, we find that $\text{tr } \phi = \lambda_x|G|$. Thus, identifying the two determined expressions for the trace of the mapping ϕ , we find that $\lambda_x|G| = \chi(x^{-1})$, where χ is the character of the representation W_1 . Repeating the argument for all $x \in G$, we determine that $\lambda_x = \frac{\chi(x^{-1})}{|G|}$. Hence, we have:

$$e_1 = \frac{1}{|G|} \sum_{g \in G} \chi(g^{-1})g.$$

We now show that $\langle \chi, \chi \rangle = \chi(e)$ by evaluating e_1^2 in this form:

$$e_1^2 = \frac{1}{|G|^2} \sum_{g, h \in G} \chi(h^{-1})\chi(g^{-1})gh.$$

Write $e_1 = \sum_{g \in G} \lambda_g g$ and $e_1^2 = \sum_{g \in G} \mu_g g$. Then the coefficient μ_e in the expansion of e_1^2 of e , the identity in G , is precisely composed of the choices of $g, h \in G$ such that $h = g^{-1}$. We thus find the coefficient of e in e_1^2 to be the following:

$$\mu_e = \frac{1}{|G|^2} \sum_{g \in G} \chi(g)\chi(g^{-1}).$$

By Lemma 11.5, $\chi(g^{-1}) = \overline{\chi(g)}$, and so we find:

$$\mu_e = \frac{1}{|G|^2} \sum_{g \in G} \chi(g)\chi(g^{-1}) = \frac{1}{|G|^2} \sum_{g \in G} \chi(g)\overline{\chi(g)} = \frac{1}{|G|} \langle \chi, \chi \rangle.$$

Furthermore, we have that $e_1^2 = e_1$. By linear independence of the elements of G , the equation $e_1 = e_1^2$ gives $\lambda_e = \mu_e$. We have already that $\lambda_e = \frac{1}{|G|}\chi(e)$, and so we determine:

$$\frac{1}{|G|}\chi(e) = \frac{1}{|G|} \langle \chi, \chi \rangle \iff \chi(e) = \langle \chi, \chi \rangle.$$

Then we are done. □

Theorem 11.7. [7, Theorem 14.12] *Let G be a finite group, and let χ_1, \dots, χ_s be its irreducible characters. Then χ_1, \dots, χ_s form an orthonormal set in the complex inner product space $\mathbb{C}_{\text{class}}(G)$.*

Proof. Let χ be an irreducible character of G , and let W be the sum of all of the composition factors of $\mathbb{C}[G]$ that have the character χ . Then by Maschke's theorem, there exists a submodule X such that $\mathbb{C}[G] = W \oplus X$. If X has a composition factor U isomorphic to a composition factor V of W , then the representation U has the same character as V , being χ . Hence, W and X have no common composition factors. We have then determined a decomposition of $\mathbb{C}[G]$ as a direct sum of two submodules with no common composition factors, and so we can apply Lemma 11.6.

By Proposition 10.13, the module W has the character $m\chi$, where m is the number of irreducible $\mathbb{C}[G]$ -modules with the character χ . By Lemma 11.6 and property (2) of the inner product, we have:

$$m\chi(e) = (m\chi)(e) = \langle m\chi, m\chi \rangle = m^2 \langle \chi, \chi \rangle.$$

Next, $\chi(e) = \dim U$, where U is some irreducible representation of G with character χ . By Theorem 9.5 we find then that $\chi(e)$ equals m , the number of composition factors with the character χ . We then find:

$$m^2 = m^2 \langle \chi, \chi \rangle.$$

We hence deduce that $\langle \chi, \chi \rangle = 1$.

Now let ψ be an irreducible character of G distinct from χ . We will show that $\langle \chi, \psi \rangle = 0$. Let Y be the sum of W with additionally all of the composition factors of $\mathbb{C}[G]$ with the character ψ . Again, we find that there exists a complementary module Z with no common composition factors with Y , and $\mathbb{C}[G] = Y \oplus Z$. The representation Y then has the character $m\chi + k\psi$, where k is the number of composition factors with the character ψ . Applying Lemma 11.6 to the representation Y , we get:

$$\begin{aligned} m\chi(e) + k\psi(e) &= \langle m\chi + k\psi, m\chi + k\psi \rangle \\ &= m^2 \langle \chi, \chi \rangle + k^2 \langle \psi, \psi \rangle + mk(\langle \chi, \psi \rangle + \langle \psi, \chi \rangle). \end{aligned}$$

Then we have furthermore that $\chi(e) = m$ and $\psi(e) = k$. Applying that $\langle \chi, \chi \rangle = \langle \psi, \psi \rangle = 1$, Lemma 11.5, cancelling, and applying properties of the complex inner product, we find that:

$$0 = mk(\langle \chi, \psi \rangle + \langle \psi, \chi \rangle) \iff 2 \langle \chi, \psi \rangle = 0 \iff \langle \chi, \psi \rangle = 0.$$

Then we are done. □

We will now proceed to prove that the irreducible characters of a group in fact form not just an orthonormal set but an orthonormal basis for the inner product space $\mathbb{C}_{\text{class}}(G)$.

Lemma 11.8. *[Adapted from [6, Theorem 2.4] and [8, Theorem 6.19]] Recall that the center $Z(\mathbb{C}[G])$ of the ring $\mathbb{C}[G]$ is the set of elements of $\mathbb{C}[G]$ which commute with every other element of the ring in multiplication. Write s to mean the number of irreducible characters of G . Then, viewed as \mathbb{C} -vector spaces, we have:*

$$\dim Z(\mathbb{C}[G]) = s = \dim \mathbb{C}_{\text{class}}(G).$$

Proof. The proof of this lemma is adapted from pieces of [6, Theorem 2.4] and [8, Theorem 6.19].

Let $\mathcal{M} = \{W_1, \dots, W_s\}$ be a complete set of representatives of irreducible $\mathbb{C}[G]$ -modules. Then there exists a decomposition of $\mathbb{C}[G]$ into:

$$\mathbb{C}[G] = U_1 \oplus \dots \oplus U_s,$$

where each U_i is the sum of all irreducible $\mathbb{C}[G]$ -modules isomorphic to W_i (see Definition 8.9).

Pick $u_i \in U_i$ for some index i , and let $z \in Z(\mathbb{C}[G])$. Then the multiplication zu_i is equivalent to a multiplication of the vector u_i by the matrix $\rho(z)$, where ρ is the representation of $\mathbb{C}[G]$ viewed as a homomorphism of groups. The mapping $\phi : U_i \rightarrow U_i$ defined by $u_i \mapsto \rho(z)u_i$ is then a \mathbb{C} -endomorphism, and thus has some eigenvalue $\lambda \in \mathbb{C}$; [7, Result (2.26)]. As such, there exists some nonzero $v \in U_i$ for which $\phi(v) = \lambda v$. Thus the matrix $\phi - \lambda \text{id}$ on the irreducible \mathbb{C} -vector space U_i has a nontrivial kernel containing v , and so, by Schur's lemma, it must be that $\phi - \lambda \text{id}$ is the zero map. Hence $\phi = \lambda \text{id}$. We conclude that there exist complex numbers $\lambda_1, \dots, \lambda_s$ such that $\rho(z)u_i = \lambda_i u_i$ whenever $u_i \in U_i$.

Consider $1e \in \mathbb{C}[G]$, the multiplicative identity element. Then there exist u_1, \dots, u_s such that $1e = u_1 + \dots + u_s$. Thus:

$$z = z \cdot 1e = z \cdot (u_1 + \dots + u_s) = \sum_{i=1}^s \lambda_i u_i.$$

Since U_1, \dots, U_s are in direct sum, the vectors u_1, \dots, u_s are linearly independent. We conclude that u_1, \dots, u_s form a basis for $Z(\mathbb{C}[G])$ as a \mathbb{C} -vector space, and hence that $\dim Z(\mathbb{C}[G]) = s$, the number of irreducible characters of G .

Now, we will show that s is also the number of conjugacy classes of G . Let C_1, \dots, C_r be the conjugacy classes of G , and define:

$$K_i = \sum_{g \in C_i} g.$$

First, we determine that $K_i \in Z(\mathbb{C}[G])$. It suffices to show that K_i commutes with every element of G . By Proposition 10.2, we can equivalently write K_i as:

$$K_i = \sum_{h \in G} h g_i h^{-1},$$

where g_i is some representative of the conjugacy class C_i . Pick $x \in G$. Then we have:

$$xK_i = \sum_{h \in G} x h g_i h^{-1} = \sum_{h \in G} x h g_i h^{-1} x^{-1} x.$$

Then by reindexing h to xh , we find:

$$xK_i = \sum_{xh \in G} (xh) g_i (xh)^{-1} x = K_i x.$$

This establishes that $K_i \in Z(\mathbb{C}[G])$. Now pick $z = \sum_{g \in G} a_g g \in Z(\mathbb{C}[G])$. Then, being in the center, z is invariant under conjugation, so $z = hzh^{-1}$ for all $h \in G$. From this we determine that $z = \sum_{g \in G} a_g hgh^{-1}$. We find hence, by linear independence of the elements of G , that $a_g = a_{hgh^{-1}}$ for all $h \in G$, meaning that the coefficients a_g are constant on each conjugacy class of G . We then conclude that $z = \sum_{i=1}^r a_{g_i} K_i$, and that the K_i span $Z(\mathbb{C}[G])$. That the K_i are linearly independent follows from the linear independence of the elements of G and that the conjugacy classes of G partition the set G . Then we are done. \square

Theorem 11.9. [8, Theorem 6.19] *The irreducible characters χ_1, \dots, χ_r form an orthonormal basis for $\mathbb{C}_{\text{class}}(G)$.*

Proof. By Theorem 11.7, the set χ_1, \dots, χ_r is an orthonormal set. It remains to show that χ_1, \dots, χ_r form a basis for the space $\mathbb{C}_{\text{class}}(G)$.

By Lemma 11.8, we have that $\dim \mathbb{C}_{\text{class}}(G) = r$; hence, by the properties of bases of vector spaces, it suffices to show that χ_1, \dots, χ_r are linearly independent.

Suppose that $0 = a_1\chi_1 + \dots + a_r\chi_r$. We apply the inner product with χ_i to both sides:

$$\langle 0, \chi_i \rangle = \langle a_1\chi_1 + \dots + a_r\chi_r, \chi_i \rangle \quad \Longleftrightarrow \quad 0 = a_i,$$

as follows by the linearity of the inner product and the fact that χ_1, \dots, χ_r form an orthonormal set. We conclude hence that $a_i = 0$ for all indices i , and this establishes linear independence. \square

12 Conclusion

The study of representations and characters of groups is very broad, though it has many applications to mathematical research. In this thesis we have explored different ways of understanding representations and characters with particular focus on their structure.

There is much more to be said about both representations and characters of groups through looking at the particular case of abelian groups, and there is more to be said about the inner products of characters. This thesis has also been limited to fields of characteristic 0 and finite groups, while one may also study the representations over fields of characteristic p as well as the representations of infinite groups.

References

- [1] P. B. Bhattacharya, S. K. Jain, and S.R. Nagpaul, *Basic Abstract Algebra*, Second Edition, Cambridge University Press, Cambridge (1995).
- [2] D. S. Dummit and R. M. Foote, *Abstract Algebra*, Third Edition, John Wiley and Sons, Hoboken (2004).
- [3] D. Harari, *Cours d'algèbre M1, Orsay, 2021-2022*, Université de Paris-Saclay (2021).
- [4] T. Hawkes, The Origins of the Theory of Group Characters, *Arch. Hist. Exact Sci.* **7(2)** (1971), 142–170.
- [5] V. E. Hill, *Groups and Characters*, Chapman and Hall, London (1999).
- [6] I. M. Isaacs, *Character Theory of Finite Groups*, Academic Press, New York (1976).
- [7] G. James and M. Liebeck, *Representations and Characters of Groups*, Second Edition, Cambridge University Press, Cambridge (2001).
- [8] D. Kang, *Group Representations and Character Theory*, University of Chicago (2011).