

Willoughby Seago

Notes from

Representation Theory

January 13th, 2024

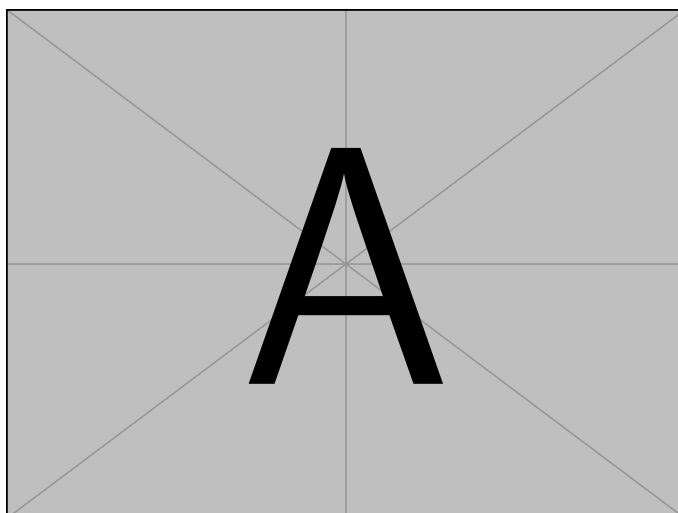
UNIVERSITY OF GLASGOW

Representation Theory

Willoughby Seago

January 13th, 2024

These are my notes from the SMSTC course *Lie Theory* taught by Prof Christian Korff. These notes were last updated at 17:56 on April 8, 2025.



Chapters

	Page
Chapters	ii
Contents	iii
1 Introduction	1
2 Initial Definitions	2
3 Tensor Products	17
4 Jacobson's Density Theorem	22
5 Character Theory	35
6 Representation Theory of Finite Groups	44
7 Applications of Characters	58
Appendices	71
A Complex, Real and Quaternionic Types	72

Contents

	Page
Chapters	ii
Contents	iii
1 Introduction	1
2 Initial Definitions	2
2.1 Algebra	2
2.2 Representations and Modules	4
2.3 Direct Sums	6
2.4 Module Homomorphisms	8
2.5 Schur's Lemma	10
2.6 Ideals and Quotients	13
2.6.1 Generators and Relations	15
2.6.2 Quotient Modules	16
3 Tensor Products	17
3.1 Tensor Product of Modules	17
3.1.1 Universal Property	19
3.2 Tensor Algebra	20
4 Jacobson's Density Theorem	22
4.1 Semisimple Representations	22
4.2 Density Theorem	26
5 Character Theory	35
5.1 Definitions	35
5.2 Jordan–Hölder and Krull–Schmidt Theorems	39
5.3 Tensor Products	42
6 Representation Theory of Finite Groups	44
6.1 Maschke's Theorem	44
6.2 Group Characters	47
6.3 Dual Representations	52
6.4 Tensor Products of Representations	52

6.5	Orthogonality of Characters	53
6.5.1	Unitary Representations	56
7	Applications of Characters	58
7.1	Computing Tensor Products	58
7.2	Frobenius–Schur Indicator	58
7.2.1	Bilinear Forms and Dual Spaces	58
7.2.2	The Frobenius–Schur Indicator	60
7.3	Burnside’s Theorem	62
7.3.1	Statement of Theorem	62
7.3.2	Algebraic Integers	63
7.3.3	Towards a Proof of Burnside’s Theorem	65
7.3.4	Proof of Burnside’s Theorem	69
	Appendices	71
A	Complex, Real and Quaternionic Types	72
A.1	Complexification	72

One

Introduction

We fix some standard notation here:

- \mathbb{k} will denote an algebraically closed field, except for when we explicitly mention that the field needn't be algebraically closed.
- A will denote an associative unital algebra.
- Letters like V , U , and W will denote vector spaces over \mathbb{k} .
- Letters like M and N will denote modules.

Two

Initial Definitions

2.1 Algebra

Definition 2.1.1 — Algebra An **algebra** is a \mathbb{k} -vector space, A , equipped with a bilinear map,

$$m : A \times A \rightarrow A \quad (2.1.2)$$

$$(a, b) \mapsto m(a, b) = ab. \quad (2.1.3)$$

If this map satisfies the condition that

$$m(a, m(b, c)) = m(m(a, b), c), \text{ or equivalently } a(bc) = (ab)c, \quad (2.1.4)$$

for all $a, b, c \in A$ then we call A an **associative algebra**.

If A possesses a distinguished element, $1 \in A$, such that $m(1, a) = a = m(a, 1)$, or equivalently $1a = a = a1$ for all $a \in A$ then we say that A is a **unital algebra**.

If $m(a, b) = m(b, a)$, or equivalently $ab = ba$, for all $a, b \in A$ then we say that A is a **commutative algebra**.

Whenever we say, otherwise unqualified, “algebra” we will mean associative unital algebra unless we specify otherwise. We will not assume commutativity of a general algebra.

The condition of associativity can be written as a commutative diagram,

$$\begin{array}{ccc} A \times A \times A & \xrightarrow{m \times \text{id}_A} & A \times A \\ \text{id}_A \times m \downarrow & & \downarrow m \\ A \times A & \xrightarrow{m} & A, \end{array} \quad (2.1.5)$$

Remark 2.1.6 This diagram goes part of the way to the more abstract definition that “an associative unital (commutative) algebra is a (commutative) monoid in the category of vector spaces”. This definition is nice because it is both very general and dualises to the notion of a coalgebra. See the *Hopf Algebra* notes for more details.

Example 2.1.7

- $A = \mathbb{k}$ is an algebra with the product given by the product in the field;
- $A = \mathbb{k}[x_1, \dots, x_n]$, the ring of polynomials in the variables x_i with coefficients in \mathbb{k} , is an algebra under the addition and multiplication of polynomials.
- $A = \mathbb{k}\langle x_1, \dots, x_n \rangle$, the free algebra on x_i , may be considered as the algebra of polynomials in non-commuting variables, x_i .
- $A = \text{End } V$ for V a \mathbb{k} -vector space is an algebra with multiplication given by composition of morphisms.

Definition 2.1.8 — Group Algebra Let G be a group. The **group algebra** or **group ring** $\mathbb{k}G = \mathbb{k}[G]$ is defined to be the set of finite formal linear combinations

$$\sum_{g \in G} c_g g \quad (2.1.9)$$

where $c_g \in \mathbb{k}$ is nonzero for only finitely many values g . Addition is defined by

$$\sum_{g \in G} c_g g + \sum_{g \in G} d_g g = \sum_{g \in G} (c_g + d_g)g. \quad (2.1.10)$$

Multiplication is defined by requiring that it distributes over addition and that the product of two terms in the above sums is given by

$$(c_g g)(d_h h) = (c_g d_h)(gh) \quad (2.1.11)$$

where multiplication on the left is in $\mathbb{k}G$, the multiplication $c_g d_h$ is in \mathbb{k} , and the multiplication gh is in G .

If we do the same construction replacing \mathbb{k} with a ring, R , then we get the group ring, RG , which is not an algebra but instead an R -module.

Definition 2.1.12 — Algebra Homomorphism Let A and B be \mathbb{k} -algebras. An **algebra homomorphism** is a linear map $f : A \rightarrow B$ such that $f(ab) = f(a)f(b)$ for all $a, b \in A$.

If A and B are unital, with units 1_A and 1_B respectively, then we further require that $f(1_A) = 1_B$.

We denote by $\text{Hom}(A, B)$ or $\text{Hom}_{\mathbb{k}}(A, B)$ the set of all algebra homomorphisms $A \rightarrow B$.

If m_A and m_B denote the multiplication maps of A and B respectively then we may think of a homomorphism, f , as a linear map which “commutes” with the multiplication map, that is $f \circ m_A = m_B \circ f$.

Alternatively, an algebra, A is both an abelian group under addition, and a monoid under multiplication, and an algebra homomorphism is both a group and monoid homomorphism with respect to these structures.

2.2 Representations and Modules

There are two competing terminologies in the field, with slightly different notation and emphasis depending on which we use. We'll use the more modern notion of modules most of the time, but will occasionally and interchangeably use the notion of representations as well.

Definition 2.2.1 — Representation Let V be a \mathbb{k} -vector space and A a \mathbb{k} -algebra. Any $\rho \in \text{Hom}(A, \text{End } V)$ is called a **representation** of A . That is, a representation of A is an algebra homomorphism $\rho : A \rightarrow \text{End } V$.

Definition 2.2.2 — Module Let A be a \mathbb{k} -algebra. A **left A -module**, M , is an abelian group, with the binary operation denoted $+$, equipped with a **left action**

$$\cdot : A \times M \rightarrow M \quad (2.2.3)$$

$$(a, m) \mapsto a \cdot m \quad (2.2.4)$$

such that for all $a, b \in A$ and $m, n \in M$ we have^a

$$\text{M1 } (ab) \cdot m = a \cdot (b \cdot m) \text{ (note that } (ab) \text{ is the product in } A);$$

$$\text{M2 } 1 \cdot m = m.$$

$$\text{M3 } a \cdot (m + n) = a \cdot m + a \cdot n;$$

$$\text{M4 } (a + b) \cdot m = a \cdot m + b \cdot m;$$

One can similarly define a **right A -module**, M , as an abelian group with a **right action**

$$\cdot : M \times A \rightarrow M \quad (2.2.5)$$

$$(m, a) \mapsto m \cdot a \quad (2.2.6)$$

such that for all $a, b \in A$ and $m, n \in M$ we have

$$\text{M1 } (m + n) \cdot a = m \cdot a + n \cdot a;$$

$$\text{M2 } m \cdot (a + b) = m \cdot a + m \cdot b;$$

$$\text{M3 } m \cdot (ab) = (m \cdot a) \cdot b;$$

$$\text{M4 } m \cdot 1 = m.$$

A **two-sided A -module** is then an abelian group, M , which is simultaneously a left and right A -module satisfying

$$a \cdot (m \cdot b) = (a \cdot m) \cdot b \quad (2.2.7)$$

for all $a, b \in A$ and $m \in M$.

^aNote that M1 and M2 simply say that this is a group action on the set M , and M3 and M4 two impose that this group action is compatible with both the group operation and addition in the algebra.

When it doesn't risk confusion we will write $a \cdot m$ as am and $m \cdot a$ as ma .

Note that a module is a generalisation of the notion of a vector space. In fact, if $A = \mathbb{k}$ then a module is exactly a vector space.

More compactly, one can define a right A -module as a left A^{op} -module, where A^{op} is the **opposite algebra** of A , defined to be the same underlying vector space with multiplication $*$ defined by $a * b = ba$, where ba is the multiplication in A . Because of this we will almost never have reason to work with right modules, we can always turn them into a left module over the opposite algebra instead.

Note that if A is commutative every left A -module is a right A -module and vice versa, and also a two-sided module.

Without further clarification the term “module” will mean

- a left module if A is not necessarily commutative;
- a two sided module if A is commutative.

A representation of A and an A -module carry exactly the same information. Given a representation, $\rho : A \rightarrow \text{End } V$ we may define a group action on V by $a \cdot v = \rho(a)v$. Composition in $\text{End } V$ is exactly repeated application of this action: $[\rho(a)\rho(b)]v = \rho(a)[\rho(b)v]$ (M1). The unit of $\text{End } V$ is the identity morphism, id_V , and $1 \in A$ must map to id_V , so $\rho(1)v = \text{id}_V v = v$ (M2). Linearity of $\rho(a)$ means that $\rho(a)(v + w) = \rho(a)v + \rho(a)w$ (M3). Linearity of ρ means that $\rho(a + b)v = \rho(a)v + \rho(b)v$ (M4).

Conversely, given an A -module, M , we can define scalar multiplication by $\lambda \in \mathbb{k}$ on M by $\lambda m = (\lambda 1)m$ where $\lambda 1$ is scalar multiplication in A . This makes M a vector space, and we may define a morphism $\rho : A \rightarrow \text{End } M$ by defining $\rho(a)$ by $\rho(a) = a \cdot m$, which uniquely determines $\rho(a)$, say by considering the action on some fixed basis of M .

Further, these two constructions are inverse, given a module if we construct the corresponding representation then construct the corresponding module from that we get back the original module, and vice versa. This means that the notion of a representation and a module really are the same, and we don't need to distinguish between them. We will use whichever terminology and notation is better suited to the problem, which is usually the module terminology and notation.

Proposition 2.2.8 Let V be a \mathbb{k} -vector space, G a group, and $\rho : G \rightarrow \text{GL}(V)$ a group homomorphism. We may define a $\mathbb{k}G$ -module by extending this map linearly, defining

$$\left(\sum_{g \in G} c_g g \right) \cdot v = \sum_{g \in G} c_g \rho(g)v. \quad (2.2.9)$$

Conversely, given a left $\mathbb{k}G$ -module on V we may define a group homomorphism $\rho : G \rightarrow \text{GL}(V)$ by defining $\rho(g)$ to be the linear operation $v \mapsto g \cdot v$.

Proof. This is just a special case of the equivalence of representations and modules discussed above. \square

Note that a **group representation** is defined to be a group homomorphism $\rho : G \rightarrow \text{GL}(V)$. The above result shows that a group representation of G is exactly the same as an algebra representation of $\mathbb{k}G$, so we can just study algebras.

Definition 2.2.10 — Regular Representation Let $V = A$ be an algebra and define $\rho : A \rightarrow \text{End } A$ by $\rho(a)b = ab$. This is called the **left regular representation**. Similarly, the **right regular representation** is given by defining $\rho(a)b = ba$.

2.3 Direct Sums

The goal of much of representation theory is to classify possible representations. To do this we usually decompose representations into smaller parts that can be more easily classified. This decomposition is done by the direct sum.

Definition 2.3.1 — Direct Sum Let M and N be A -modules. The **direct sum**, $M \oplus N$, is the A -module given by the direct sum of the underlying abelian groups equipped with the action

$$a(m \oplus n) = am \oplus an \quad (2.3.2)$$

for all $a \in A$, $m \in M$ and $n \in N$.

The required properties follow immediately from the definition:

$$\text{M1 } (ab)(m \oplus n) = (ab)m \oplus (ab)n = a(bm) \oplus a(bn) = a(bm \oplus bn) = a(b(m \oplus n));$$

$$\text{M2 } 1(m \oplus n) = 1m \oplus 1n = m \oplus n;$$

$$\text{M3 } a((m \oplus n) + (m' \oplus n')) = a((m + m') \oplus (n + n')) = a(m + m') \oplus a(n + n') = (am + am') \oplus (an + an') = (am \oplus an) + (am' \oplus an') = a(m \oplus n) + a(m' \oplus n');$$

$$\text{M4 } (a + b)(m \oplus n) = (a + b)m \oplus (a + b)n = (am + bm) \oplus (an + bn) = (am \oplus an) + (bm \oplus bn) = a(m \oplus n) + b(m \oplus n).$$

Definition 2.3.3 — Submodule Let M be a left A -module. An abelian subgroup $N \leq M$ is a **A -submodule** if $AN \subseteq N$. In this case we say that N is **invariant** under the action of A .

Note that by AN we mean

$$AN = \{an \mid a \in A, n \in N\}. \quad (2.3.4)$$

So $AN \subseteq N$ means that $an \in N$ for all $a \in A$ and $n \in N$. Thus, invariance means that no element of N leaves N under the action of A .

Definition 2.3.5 — Trivial Submodule Every A -module, M , admits two submodules, M itself and the zero module, 0 , which contains only 0 . We call these **trivial submodules**.

Note that some texts call only 0 the trivial submodule, and make the distinction of a submodule vs a *proper* submodule, the distinction being that M is not a proper submodule of M . Then when we say “nontrivial submodule” these texts will say “nontrivial proper submodule”.

Definition 2.3.6 — Simple Submodule Let M be an A -module. We say that M is **simple** or **irreducible** if it contains no nontrivial submodules.

Typically “simple” is used for modules and “irreducible” is used more for representations, although irreducible is used for both.

Definition 2.3.7 — Semisimple Let M be an A -module. Then M is **semisimple** or **completely reducible** if it can be written as a direct sum of finitely many simple modules.

That is, M is semisimple if

$$M = \bigoplus_{i=1}^n N_i = N_1 \oplus \cdots \oplus N_n \quad (2.3.8)$$

where each N_i is simple. Note that we define the empty sum to be the zero module, so the zero module is considered semisimple (and also simple, since it contains only itself as a submodule).

Again, “semisimple” is typically used only for modules, and “completely reducible” is used primarily for representations.

Definition 2.3.9 — Indecomposable Let M be an A -module. Then M is **indecomposable** if M cannot be written as a direct sum of nontrivial modules.

The nontrivial requirement here just rules out decompositions of the form¹ $M = M \oplus 0$.

Note that every simple (irreducible) module is indecomposable, since if it had a decomposition $M = N_1 \oplus N_2$ with N_i nontrivial then there is a canonical copy of each N_i as a submodule of M . The converse does not hold in general, not all indecomposable modules are irreducible. It is possible that M contains a submodule, N , but that there is no submodule N' such that $M = N \oplus N'$. Contrast this to finite dimensional vector spaces where we can take N' to be the orthogonal complement (with respect to some inner product) of N and this direct sum holds. We can still form the orthogonal complement of a submodule, but it will not, in general, be a submodule. There are, however, many special cases, such as finite dimensional complex representations of (group algebras) finite groups, where the orthogonal complement can be defined in such a way that it is a submodule, and in this case indecomposable and irreducible coincide.

¹Note that with our definition of the direct sum this really only holds up to isomorphism, since M has elements m whereas $M \oplus 0$ has elements $(m, 0)$. However, we’re yet to define morphisms between modules, and once we do we’ll see that \oplus is the product in the category of modules, and as such is only defined up to isomorphism, so we may as well momentarily take the isomorphism that makes this equality true.

One of the main goals of representation theory is to classify all indecomposable modules of a given algebra. This then gives us an understanding of *all* modules over that algebra, since any nonsimple or decomposable module may be realised as a direct sum of these classified indecomposable modules.

2.4 Module Homomorphisms

Definition 2.4.1 — Module Homomorphism Let M and N be A -modules. An **A -module homomorphism** or **intertwiner** is a homomorphism of the underlying abelian groups $\varphi : M \rightarrow N$ which “commutes” with the action of A , by which we mean

$$\varphi(a \cdot m) = a \cdot \varphi(m) \quad (2.4.2)$$

for all $a \in A$ and $m \in M$.

An invertible A -module homomorphism is called an **isomorphism** of A -modules.

Homomorphisms of right A -modules may be defined similarly.

Notation 2.4.3 We write $\text{Hom}_A(M, N)$ for the set of A -module homomorphisms $M \rightarrow N$. Note that $\text{Hom}_A(M, N) \subseteq \text{Hom}_{\text{Ab}}(M, N)$ where $\text{Hom}_{\text{Ab}}(M, N)$ is the set of all homomorphisms $M \rightarrow N$ of the underlying abelian groups.

Note that in $\varphi(a \cdot m)$ a is acting on an element of M , and in $a \cdot \varphi(m)$ a is acting on an element of N , so these are in general different actions. Writing $a \cdot$ for the map $x \mapsto a \cdot x$ we can express the condition of commuting action as the commutativity of the diagram

$$\begin{array}{ccc} M & \xrightarrow{\varphi} & N \\ a \cdot \downarrow & & \downarrow a \cdot \\ M & \xrightarrow{\varphi} & N \end{array} \quad (2.4.4)$$

for all $a \in A$.

Lemma 2.4.5 Isomorphisms of A -modules are exactly bijective morphisms of A -modules.

Proof. Let $\varphi : M \rightarrow N$ be a bijective morphism of A -modules. Then the (set-theoretic) inverse, $\varphi^{-1} : N \rightarrow M$, exists. We claim that this is a morphism of A -modules. This follows by taking $n \in N$ to be the image of $m \in M$ under φ , giving

$$\varphi^{-1}(a \cdot n) = \varphi^{-1}(a \cdot \varphi(m)) = \varphi^{-1}(\varphi(a \cdot m)) = a \cdot m = a \cdot \varphi^{-1}(n). \quad (2.4.6)$$

Conversely, if $\varphi : M \rightarrow N$ is an isomorphism of A -modules it must necessarily be that φ^{-1} is the (set-theoretic) inverse of the underlying function

of φ , and so φ must be bijective. \square

If we instead talk of representations (V, ρ) and (W, σ) then a homomorphism of representations, $\varphi : V \rightarrow W$, must satisfy $\varphi(\rho(a)v) = \sigma(a)\varphi(v)$. Further, by linearity of ρ and σ and the fact that $\rho(1) = \text{id}_V$ and $\sigma(1) = \text{id}_W$ we have that for $\lambda \in \mathbb{k}$

$$\varphi(\lambda m) = \varphi(\rho(1)\lambda m) = \varphi(\rho(\lambda 1)m) = \sigma(\lambda 1)\varphi(m) = \lambda\sigma(1)\varphi(m) = \lambda\varphi(m). \quad (2.4.7)$$

This shows that φ must be a linear map $\varphi : V \rightarrow W$. In fact, we can *define* a homomorphism of representations to be a linear map $\varphi : M \rightarrow N$ satisfying $\varphi(\rho(a)m) = \sigma(a)\varphi(m)$. We will also write $\text{Hom}_A(V, W)$ for the set of representation morphisms $V \rightarrow W$. Note then that $\text{Hom}_A(V, W) \subseteq \text{Hom}_{\mathbb{k}\text{-Vect}}(V, W)$ where $\text{Hom}_{\mathbb{k}\text{-Vect}}(V, W)$ is the set of linear maps $V \rightarrow W$ of the underlying vector spaces. Using the notation Hom_A for both modules and representations is justified by the following remark.

Remark 2.4.8 There is a category, $A\text{-Mod}$ ($\text{Mod-}A$), with left (right) A -modules as objects and A -module homomorphisms as morphisms. Similarly, there is a category $\text{Rep}(A)$ of representations of A with objects being representations (V, ρ) and morphisms being homomorphisms of representations.

In [Section 2.2](#) we showed that we have a mapping $F : A\text{-Mod} \rightarrow \text{Rep}(A)$ constructing a representation from a module, and a mapping $G : \text{Rep}(A) \rightarrow A\text{-Mod}$ constructing a module from a representation. In the discussion above we extend this mapping to define a representation homomorphism from a module homomorphism. We can also ignore the requirement of linearity with respect to scalar multiplication in the definition of a representation homomorphism to recover a module homomorphism. Further, applying either of these constructions to the appropriate identity map just gives the identity, and both constructions preserve composition. These operations on homomorphisms are also inverses of each other. Thus, F and G are functors and we have $FG = \text{id}_{\text{Rep}(A)}$ and $GF = \text{id}_{A\text{-Mod}}$. Thus, $A\text{-Mod}$ and $\text{Rep}(A)$ are isomorphic as categories, justifying the fact that we will soon cease to distinguish between them.

Lemma 2.4.9 The category $A\text{-Mod}$ defined above is indeed a category.

Proof. First note that $\text{id}_M : M \rightarrow M$ is an A -module homomorphism for any A -module, M , since we have

$$\text{id}_M(a \cdot m) = a \cdot m = a \cdot \text{id}_M(m). \quad (2.4.10)$$

Now note that if $\varphi : M \rightarrow N$ and $\psi : N \rightarrow P$ are module homomorphisms then $\psi \circ \varphi : M \rightarrow P$ is a module homomorphism since

$$(\psi \circ \varphi)(a \cdot m) = \psi(\varphi(a \cdot m)) = \psi(a \cdot \varphi(m)) = a \cdot \psi(\varphi(m)) = a \cdot (\psi \circ \varphi)(m)$$

for all $a \in A$ and $m \in M$. Finally, composition is just composition of the underlying functions, which is associative. \square

2.5 Schur's Lemma

We can now give one of the first results of representation theory. It places a restriction on the types of morphisms we can have between modules when one or more of the modules is simple. We give the result as a proposition and a corollary, although for historical reasons it's called a lemma. The proposition is more general, and the corollary is a special case. Both are known as Schur's lemma, with context determining if we use the more general result or the special case.

Before we can prove this result however we need a couple of results about kernels and images of module morphisms.

Lemma 2.5.1 Let $\varphi : M \rightarrow N$ be a morphism of modules. Then $\ker \varphi$ is a submodule of M and $\operatorname{im} \varphi$ is a submodule of N .

Proof. STEP 1: $\ker \varphi$

We know that $\ker \varphi$ is a subgroup of M , so we only need to show that it is invariant under the action of A . Take $m \in \ker \varphi$, that is $m \in M$ is such that $\varphi(m) = 0$, and $a \in A$. Then

$$\varphi(a \cdot m) = a \cdot \varphi(m) = a \cdot 0. \quad (2.5.2)$$

For arbitrary $m' \in M$ we have

$$a \cdot 0 = a \cdot (m' - m') = (a \cdot m') - (a \cdot m') = 0 \quad (2.5.3)$$

so $a \cdot 0 = 0$ for any $a \in A$, and thus $\varphi(a \cdot m) = a \cdot 0 = 0$, so $a \cdot m \in \ker \varphi$.

STEP 2: $\operatorname{im} \varphi$

We know that $\operatorname{im} \varphi$ is a subgroup of N , so we only need to show that it is invariant under the action of A . Take $n \in \operatorname{im} \varphi$ and $a \in A$. There exists some $m \in M$ such that $n = \varphi(m)$. Then

$$a \cdot n = a \cdot \varphi(m) = \varphi(a \cdot m) \quad (2.5.4)$$

and $a \cdot m \in M$ so $a \cdot n \in \operatorname{im} \varphi$. □

Proposition 2.5.5 — Schur's Lemma Let \mathbb{k} be any (not necessarily algebraically closed) field, and let A be an algebra over \mathbb{k} . Let M and N be A -modules and let $\varphi : M \rightarrow N$ be a morphism of A -modules. Then

1. if M is simple either $\varphi = 0$ or φ is injective;
2. if N is simple either $\varphi = 0$ or φ is surjective.

Combined if M and N are simple then either $\varphi = 0$ or φ is an isomorphism.

Proof. STEP 1: M SIMPLE

Let M be simple, so its only submodules are 0 and M . We know that $\ker \varphi$ is a submodule of M , so there are two cases to consider:

- If $\ker \varphi = M$ then every element of M maps to 0, so $\varphi = 0$.
- If $\ker \varphi = 0$ then φ is injective^a.

STEP 2: N SIMPLE

Let N be simple, so its only submodules are 0 and N . We know that $\text{im } \varphi$ is a submodule of N , so there are two cases to consider:

- If $\text{im } \varphi = 0$ then every element of M maps to 0, so $\varphi = 0$.
- If $\text{im } \varphi = N$ then φ is surjective.

□

^aWe know that for group homomorphisms if the kernel is trivial then the map is injective, and injectivity is a set-theoretic property, so it still holds when we add the extra structure of the A -action

Corollary 2.5.6 — Schur's Lemma Let \mathbb{k} be an algebraically closed field, and let A be an algebra over \mathbb{k} . Let V be a finite dimensional representation of A . Then any representation homomorphism $\varphi : V \rightarrow V$ is a multiple of the identity. That is, $\varphi = \lambda \text{id}_V$ for $\lambda \in \mathbb{k}$. Note that $\lambda = 0$ subsumes the trivial case.

Proof. Let $\lambda \in \mathbb{k}$ be an eigenvalue of φ with corresponding eigenvector $v \in V$. Note that eigenvalues exist because

- V is finite dimensional so the determinant may be defined as a polynomial in the entries of some matrix representing φ in a fixed basis; and
- \mathbb{k} is algebraically closed, so this polynomial has roots.

Then by definition $\varphi(v) = \lambda v$ which we can rearrange to $(\varphi - \lambda \text{id}_V)v = 0$. Thus, $v \in \ker(\varphi - \lambda \text{id}_V)$, and since eigenvectors are, by definition, nonzero this means that $\ker(\varphi - \lambda \text{id}_V) \neq 0$, so $\varphi - \lambda \text{id}_V$ is not injective, so by Schur's lemma (Proposition 2.5.5) we must have that $\varphi - \lambda \text{id}_V = 0$. Thus, $\varphi = \lambda \text{id}_V$. □

Corollary 2.5.7 Let A be a commutative algebra over an algebraically closed field, \mathbb{k} . Then all nontrivial finite dimensional irreducible representations of A are one dimensional.

Proof. Let V be a finite dimensional irreducible representation of A . For $a \in A$ define a map $\varphi_a : V \rightarrow V$ by $v \mapsto \varphi_a(v) = a \cdot v$. This is an intertwiner: take $b \in A$ and $v \in V$, then we have

$$\varphi_a(b \cdot v) = a \cdot (b \cdot v) = (ab) \cdot v = (ba) \cdot v = b \cdot (a \cdot v) = b \cdot \varphi_a(v). \quad (2.5.8)$$

Note that this is only true because $ab = ba$.

By Schur's lemma (Corollary 2.5.6) there exists some $\lambda_a \in \mathbb{k}$ such that $\varphi_a = \lambda_a \text{id}_V$. Then $a \cdot v = \varphi_a(v) = \lambda_a v$, so every $a \in A$ acts as scalar multiplication. This means that any subspace is invariant, since every subspace is, by definition, invariant under scalar multiplication. Thus, the only way that a representation can have no nontrivial invariant subspaces is if it only has trivial subspaces, which is only true if it is one dimensional (zero dimensional being ruled out by the assumption that the representation is nontrivial). \square

Example 2.5.9 Consider $A = \mathbb{k}[x]$, which is a commutative algebra. We can determine all irreducible representations of A .

A representation, $\rho : \mathbb{k}[x] \rightarrow \text{End } V$, is fully determined by the value of $\rho(x)$, since given an arbitrary polynomial, $f(x) = \sum_{i=1}^n a_i x^i$, its action on $v \in V$ is determined through linearity by

$$f(x) \cdot v = \rho(f(x))v = \rho\left(\sum_{i=1}^n a_i x^i\right)v = \sum_{i=1}^n a_i \rho(x)^i v. \quad (2.5.10)$$

Further, by Corollary 2.5.7 we know that any irreducible representation of $\mathbb{k}[x]$ is one dimensional, so it must be that $\rho(v) = \lambda v$ for some $\lambda \in \mathbb{k}$.

Let V_λ denote the one-dimensional representation in which x acts as scalar multiplication by λ . We claim that $V_\lambda \cong V_\mu$ if and only if $\lambda = \mu$. Suppose that $\varphi : V_\lambda \rightarrow V_\mu$ is an isomorphism. Then $\varphi(x \cdot v) = \varphi(\lambda v) = \lambda \varphi(v)$ and $\varphi(x \cdot v) = x \cdot \varphi(v) = \mu \varphi(v)$. Thus, $\lambda = \mu$.

So, we have classified all irreducible representations of $\mathbb{k}[x]$, they are precisely the one dimensional vector spaces, V_λ for $\lambda \in \mathbb{k}$ in which $\rho(x) = \lambda \text{id}_{V_\lambda}$.

This result generalises to polynomials in an arbitrary number of variables, $\mathbb{k}[x_1, \dots, x_n]$. Then a representation is fully determined by the values of $\rho(x_1)$ through $\rho(x_n)$. Thus an irreducible representation is a one dimensional vector space, $V_{\lambda_1, \dots, \lambda_n}$ in which $\rho(x_i) = \lambda_i \text{id}_{V_{\lambda_1, \dots, \lambda_n}}$.

Go back to the case of $A = \mathbb{k}[x]$. For a nontrivial ($\lambda \neq 0$) finite dimensional irreducible representation, V_λ , instead of starting with the action of x we can perform a change of variables and work with $y = x/\lambda$. Then we get the representation V_1 . This means that all finite dimensional irreducible representations of $\mathbb{k}[x]$ are essentially the same, up to rescaling. This also means that they're pretty boring.

Indecomposable representations of $\mathbb{k}[x]$ are more interesting on the other hand. Let V be a finite dimensional representation. We can fix a basis and look at matrices. Suppose $B \in \text{End } V$, then since we work over an algebraically closed field we know that the Jordan normal form of B exists after a basis change, allowing us to write the matrix of B as

$$B = \begin{pmatrix} J_{\lambda_1, n_1} & & & \\ & J_{\lambda_2, n_2} & & \\ & & \ddots & \\ & & & J_{\lambda_k, n_k} \end{pmatrix} \quad (2.5.11)$$

where J_{λ_i, n_i} is the $n_i \times n_i$ Jordan block matrix

$$J_{\lambda_i, n_i} = \begin{pmatrix} \lambda_i & 1 & & & \\ & \lambda_i & 1 & & \\ & & \ddots & \ddots & \\ & & & \lambda_i & 1 \\ & & & & \lambda_i \end{pmatrix}. \quad (2.5.12)$$

This block diagonal decomposition of B gives us a corresponding direct sum decomposition of V . Each Jordan block cannot be diagonalised (with the exception of the 1×1 Jordan blocks which are trivially diagonal). Thus we cannot further decompose B and so we cannot further decompose V . The result is that

$$V = \bigoplus_{i=1}^k V_{\lambda_i, n_i} \quad (2.5.13)$$

where $V_{\lambda_i, n_i} = \mathbb{k}^{n_i}$ is an n_i -dimensional vector space upon which the action of B is given by J_{λ_i, n_i} . Then taking $B = \varphi(x)$ defines a representation of $\mathbb{k}[x]$ on V , and specifically we have the subrepresentations V_{λ_i, n_i} in which x acts as the Jordan block J_{λ_i, n_i} .

2.6 Ideals and Quotients

Definition 2.6.1 — Ideals Let A be an algebra. A subspace, $I \subseteq A$, such that $AI \subseteq I$ is called a **left ideal**. Similarly if $IA \subseteq I$ then we call I a **right ideal**. A **two-sided ideal** is simultaneously a left and right ideal.

Note that by AI we mean $AI = \{ai \mid a \in A, i \in I\}$, so the condition that I is a left ideal is that $ai \in I$ for all $a \in A$ and $i \in I$.

Example 2.6.2

- Any algebra, A , always has 0 and A as ideals. If these are the only ideals then we call A **simple**.
- Any left (right) ideal is a submodule of the left (right) regular representation. This is simply identifying that A is an A -module with the action being left (right) multiplication and as such the notion of an ideal coincides with that of a submodule. Note that the notion of a simple module coincides with the notion of a simple algebra under this identification.
- If $f: A \rightarrow B$ is an algebra morphism then $\ker f$ is a two-sided ideal. We know that $\ker f$ is a subspace of A , so just note that if $a \in \ker f$ then $f(a) = 0$ and we have

$$f(ba) = f(b)f(a) = f(b)0 = 0 \quad (2.6.3)$$

and

$$f(ab) = f(a)f(b) = 0f(a) = 0 \quad (2.6.4)$$

so ab and ba are in $\ker f$.

We will say “ideal” when we mean either a left ideal. Note that in the commutative case all left ideals are right ideals and hence two-sided ideals, so we don’t need to distinguish the three cases.

Notation 2.6.5 Let A be an algebra and $S \subseteq A$ a subset of A . Denote by $\langle S \rangle$ the two-sided ideal generated by S . That is,

$$\langle S \rangle = \text{span}\{asb \mid s \in S, \text{ and } a, b \in A\}. \quad (2.6.6)$$

For example, consider $\mathbb{k}[x]$. Then $\langle x \rangle$ consists of all polynomials that can be factorised as $xf(x)$ where $f(x)$ is an arbitrary polynomial, so $f(x) = \sum_{i=0}^n a_i x^i$. Thus, $xf(x) = \sum_{i=0}^n a_i x^{i+1}$, so $\langle x \rangle$ consists of all polynomials with zero constant term. More generally, $\langle x - a \rangle$ for $a \in \mathbb{k}$ consists of all polynomials which factorise as $(x - a)f(x)$ for an arbitrary polynomial $f(x)$, and thus this is the ideal consisting of all polynomials with a as a root.

The point of defining ideals is really in order to define quotients. In this way ideals are to algebras as normal subgroups are to groups.

Definition 2.6.7 — Quotient Let A be an algebra and $I \subseteq A$ an ideal. We define the **quotient** to be the algebra A/I whose elements are equivalence classes

$$[a] = a + I := \{a' \in A \mid a - a' \in I\}. \quad (2.6.8)$$

Addition and scalar multiplication are defined by

$$[a] + [b] = (a + I) + (b + I) = [a + b] = a + b + I \quad (2.6.9)$$

and

$$\lambda[a] = [\lambda a] \quad (2.6.10)$$

for $a, b \in A$ and $\lambda \in \mathbb{k}$.

Lemma 2.6.11 The quotient of an algebra by an ideal is again an algebra.

Proof. Let A be an algebra and $I \subseteq A$ an ideal. Note that the quotient of a vector space by any subspace is again a vector space, so we need only define a multiplication operation on this vector space. We do so by defining

$$[a][b] = (a + I)(b + I) := [ab] = ab + I. \quad (2.6.12)$$

We need to show that this is well-defined and satisfies the properties of

multiplication in an algebra.

STEP 1: WELL-DEFINED

Let $a, a' \in A$ be representatives of the same equivalence class, $[a] = [a']$. Then by definition $a - a' \in I$. For $b \in A$ we then have

$$[a][b] = [ab] = [a'b + (a - a')b] = [a'b] = [a'][b]. \quad (2.6.13)$$

Here we've used the fact that $a - a' \in I$ and I is an ideal so $(a - a')b \in I$, and we can add any element of I inside an equivalence class without leaving the equivalence class. Similarly, one can show that $[a][b] = [a][b']$ whenever $[b] = [b']$. Thus, this product is well-defined.

STEP 2: ALGEBRA

Linearity in the first argument follows from a direct calculation using the properties of quotient spaces:

$$\begin{aligned} [(a + \lambda a')b] &= [ab + \lambda a'b] = [ab] + \lambda[a'b] \\ &= [a][b] + \lambda[a'][b] = ([a] + \lambda[a'])[b] = [a + \lambda a'] [b] \end{aligned} \quad (2.6.14)$$

for $a, a', b \in A$ and $\lambda \in \mathbb{k}$. Linearity in the second argument follows similarly. Associativity follows from

$$[a]([b][c]) = [a][bc] = [a(bc)] = [(ab)c] = [ab][c] = ([a][b])[c]. \quad (2.6.15)$$

Unitality follows from

$$[1][a] = [1a] = [a], \quad \text{and} \quad [a][1] = [a1] = [a]. \quad (2.6.16)$$

□

2.6.1 Generators and Relations

One of the most common ways to define an algebra is as a quotient of another algebra by some ideal given in terms of generators. The most common starting place is the free algebra, $\mathbb{k}\langle x_1, \dots, x_m \rangle$. We can then take $f_1, \dots, f_n \in \mathbb{k}\langle x_1, \dots, x_m \rangle$, and form an ideal, $\langle f_1, \dots, f_n \rangle$. Then we may form the algebra

$$A = \mathbb{k}\langle x_1, \dots, x_m \rangle / \langle f_1, \dots, f_n \rangle. \quad (2.6.17)$$

Intuitively, elements of this are non-commutative polynomials in the x_i subject to the constraint that anywhere that we can manipulate the polynomial to be written with f_i we can set that f_i equal to zero.

For example, let $f_{i,j} = x_i x_j - x_j x_i$ for $i, j = 1, \dots, m$. Consider the algebra $A = \mathbb{k}\langle x_1, \dots, x_m \rangle / \langle f_{i,j} \rangle$ consists of non-commutative polynomials in x_i subject to the condition that $x_i x_j - x_j x_i = 0$, which is to say $x_i x_j = x_j x_i$, which is exactly the condition that the x_i do commute with each other.

Another example is $A = \mathbb{k}\langle x_1, \dots, x_n \rangle / \langle x_i^2 - e, x_i x_{i+1} x_i - x_{i+1} x_i x_{i+1} \rangle$. This sets $x_i^2 = e$ and $x_i x_{i+1} x_i = x_{i+1} x_i x_{i+1}$ (called the **braid relation**). These are exactly the relations defining the symmetric group, S_n , when we interpret x_i as the transposition $(i \ i + 1)$. We're also taking linear combinations of these x_i , so $A = \mathbb{k}S_n$.

2.6.2 Quotient Modules

Definition 2.6.18 — Quotient Module Let M be an A -module and N a submodule of M . We define the **quotient module**, M/N , to be the module consisting of equivalence classes

$$[m] = m + N := \{m' \in M \mid m - m' \in N\}. \quad (2.6.19)$$

Addition in this module is defined by

$$[m] + [m'] = [m + m'] \quad (2.6.20)$$

for $m, m' \in M$ and the action of A is given by

$$a \cdot [m] = [a \cdot m] \quad (2.6.21)$$

for $a \in A$ and $m \in M$.

Lemma 2.6.22 The quotient of a module by a submodule is again a module.

Proof. Let M be an A -module with $N \subseteq M$ a submodule. Then N is a subgroup of an abelian group, and so is automatically a normal subgroup. Then we know that M/N is an abelian group also.

Suppose that $[m] = [m']$, that is m and m' are representatives of the same equivalence class. Then $m' - m \in N$. We then have

$$\begin{aligned} a \cdot [m] &= a \cdot [m' + (m - m')] = [a \cdot (m' + (m - m'))] \\ &= [a \cdot m' + a \cdot (m - m')] = [a \cdot m'] = a \cdot [m']. \end{aligned} \quad (2.6.23)$$

Here we've used the fact that $m' - m \in N$ and N is a submodule so $a \cdot (m' - m) \in N$ as well. So, the action of $a \in A$ on $[m] = [m']$ is well-defined.

It remains to show that the action of A on M/N makes it an A -module:

$$\text{M1 } (ab) \cdot [m] = [(ab) \cdot m] = [a \cdot (b \cdot m)] = a \cdot [b \cdot m] = a \cdot (b \cdot [m]);$$

$$\text{M2 } 1 \cdot [m] = [1 \cdot m] = [m];$$

$$\text{M3 } a \cdot ([m] + [n]) = a \cdot [m + n] = [a \cdot (m + n)] = [a \cdot m + a \cdot n] = [a \cdot m] + [a \cdot n] = a \cdot [m] + a \cdot [n];$$

$$\text{M4 } (a + b) \cdot [m] = [(a + b) \cdot m] = [a \cdot m + b \cdot m] = [a \cdot m] + [b \cdot m] = a \cdot [m] + b \cdot [m]$$

for all $a, b \in A$ and $m, n \in M$. □

Remark 2.6.24 Consider the left regular representation of A . As we have mentioned ideals of A are precisely submodules of the regular representation. It follows that A/I is a left A -module precisely when I is a left ideal.

Three

Tensor Products

3.1 Tensor Product of Modules

We first define the tensor product of R -modules (R a ring). This definition can also be applied to A -modules (A an algebra) without modification.

Definition 3.1.1 — Tensor Product Let R be a ring, M a right R -module, and N a left R -module. Then the **tensor product**, $M \otimes_R N$, is the abelian group

$$\frac{F(\{m \otimes n \mid m \in M, n \in N\})}{I} \quad (3.1.2)$$

where $F(X)$ denotes the free abelian group on the set X and I is the normal subgroup generated from all elements of the form

- $(m + m') \otimes n - m \otimes n - m' \otimes n$;
- $m \otimes (n + n') - m \otimes n - m \otimes n'$;
- $(m \cdot r) \otimes n - m \otimes (r \cdot n)$

with $m, m' \in M, n, n' \in N$ and $r \in R$.



The tensor product does not, in general, have the structure of an R -module. It is just an abelian group. In a sense the R -actions of M and N are “used up” in the construction and don’t “survive” to produce a sensible notion of an R -action on $M \otimes_R N$.

Notation 3.1.3 When R is clear from context we will write $M \otimes N$ instead of $M \otimes_R N$. Conversely, if needed we’ll write $m \otimes_R n$ for elements of $M \otimes_R N$ if there are multiple ways to define the tensor product.

Intuitively, $M \otimes_R N$ consists of sums of elements which we write as¹ $m \otimes n$ with $m \in M$ and $n \in N$. So, one element of $M \otimes_R N$ might be

$$m_1 \otimes n_1 + m_2 \otimes n_2 + m_3 \otimes n_3 \quad (3.1.4)$$

with $m_i \in M$ and $n_i \in N$. Note that there are no factors of R here, this is purely an operation in the free group. The quotient imposes that in $M \otimes_R N$ we have the

¹We should write $[m \otimes n]$ or something similar, since what we actually have is the equivalence class of $m \otimes n$ in $F(\{m \otimes n\})/I$.

relations

$$(m + m') \otimes n = m \otimes n + m' \otimes n; \quad (3.1.5)$$

$$m \otimes (n + n') = m \otimes n + m \otimes n'; \quad (3.1.6)$$

$$(m \cdot r) \otimes n = m \otimes (r \cdot n). \quad (3.1.7)$$

As we mentioned the tensor product of a right and left R -module is not, in general, an R -module in any consistent way. In order for the tensor product to be a module we need to have some extra module structure present in one of the two modules which then remains after the tensor product is formed. Of course, this extra structure must be compatible with the existing structure, and it turns out that the following is exactly the right definition for this purpose.

Definition 3.1.8 — Bimodule Let A and B be associative unital \mathbb{k} -algebras. An (A, B) -bimodule is an abelian group, M , which is both a left A -module and a right B module in such a way that

$$(a \cdot m) \cdot b = a \cdot (m \cdot b) \quad (3.1.9)$$

for all $a \in A$, $b \in B$, and $m \in M$.

Example 3.1.10 Let V be a \mathbb{k} -vector space and a left A -module. Then V is an (A, \mathbb{k}) -bimodule where $a \cdot v$ is just the action of A on V as an A -module and $v \cdot \lambda = \lambda v$ is just scalar multiplication by elements of \mathbb{k} . That this is a bimodule follows because

$$a \cdot (v \cdot \lambda) = a \cdot (\lambda v) = \lambda(a \cdot v) = (a \cdot v) \cdot \lambda \quad (3.1.11)$$

having used the fact that the action of a on v is \mathbb{k} -linear.

In fact, we can define a bimodule first (just combining the definitions of a left and right module), then a left A -module is an (A, \mathbb{k}) -bimodule, and a right A -module is a (\mathbb{k}, A) -bimodule.

Lemma 3.1.12 Let M be an (A, B) -bimodule, and N a left B -module. Then $M \otimes_B N$ is a left A -module with $a \cdot (m \otimes n) := (a \cdot m) \otimes n$.

Proof. First note that as an (A, B) -bimodule M is, in particular, a right B -module. Thus, the tensor product $M \otimes_B N$ is defined as the quotient of a free abelian group by an ideal, and so is again an abelian group. It remains only to show that this abelian group equipped with the action of A on the first factor is an A -module.

To do so take an arbitrary element of $M \otimes_B N$, which is of the form $\sum_{i \in I} m_i \otimes n_i$ where I is some finite indexing set, $m_i \in M$ and $n_i \in N$. We are free to define the action of A on this element to be

$$a \cdot \left(\sum_{i \in I} m_i \otimes n_i \right) := \sum_{i \in I} (a \cdot m_i) \otimes n_i. \quad (3.1.13)$$

Then when I is a singleton this reduces to $a \cdot (m \otimes n) = (a \cdot m) \otimes n$ as

required.

We can now prove that this makes $M \otimes_B N$ a left A -module:

$$\begin{aligned} \text{M1 } (ab) \cdot \sum_i m_i \otimes n_i &= \sum_i ((ab) \cdot m_i) \otimes n_i = \sum_i (a \cdot (b \cdot m_i)) \otimes n_i = \\ &= a \cdot \sum_i (b \cdot m_i) \otimes n_i = a \cdot (b \cdot \sum_i m_i \otimes n_i); \end{aligned}$$

$$\text{M2 } 1 \cdot \sum_i m_i \otimes n_i = \sum_i (1 \cdot m_i) \otimes n_i = \sum_i m_i \cdot n_i;$$

$$\begin{aligned} \text{M3 } a \cdot \left(\sum_{i \in I} m_i \otimes n_i + \sum_{j \in J} m_j \otimes n_j \right) &= a \cdot \left(\sum_{i \in I \sqcup J} m_i \otimes n_i \right) = \sum_{i \in I \sqcup J} (a \cdot m_i) \otimes n_i \\ &= \sum_{i \in I} (a \cdot m_i) \otimes n_i + \sum_{j \in J} (a \cdot m_j) \otimes n_j; \end{aligned}$$

$$\begin{aligned} \text{M4 } (a+b) \cdot \sum_i m_i \otimes n_i &= \sum_i ((a+b) \cdot m_i) \otimes n_i = \sum_i (a \cdot m_i + b \cdot m_i) \otimes n_i = \\ &= \sum_i (a \cdot m_i) \otimes n_i + \sum_i (b \cdot m_i) \otimes n_i = a \cdot \sum_i m_i \otimes n_i + b \cdot \sum_i m_i \otimes n_i. \end{aligned}$$

□

Similarly, if M is a right A -module and N is an (A, B) -bimodule then $M \otimes_A N$ is a right B -module with the action given by $(m \otimes n) \cdot b = m \otimes (n \cdot b)$.

Example 3.1.14 Any \mathbb{k} -vector space, V , is a (\mathbb{k}, \mathbb{k}) -bimodule, defining $\lambda \cdot v = \lambda v = v \cdot \lambda$ for $\lambda \in \mathbb{k}$ and $v \in V$. If U is some other vector space then we can form the \mathbb{k} -module $V \otimes_{\mathbb{k}} U$, which is of course just the usual tensor product of vector spaces.

In fact, this works for any commutative algebra, A , we can take any A -module as an (A, A) -bimodule, so if M and N are A -modules then $M \otimes_A N$ is an A -module.

3.1.1 Universal Property

The tensor product may also be defined via a universal property.

Lemma 3.1.15 Let M be a right A -module, and let N be a left A -module. Then for any abelian group, G , and any group homomorphism $f : M \times N \rightarrow G$ satisfying ... there is a unique group homomorphism $\bar{f} : M \otimes_A N \rightarrow G$ such that $\bar{f}(m \otimes n) = f(m, n)$ for all $m \in M$ and $n \in N$. That is, the diagram

$$\begin{array}{ccc} M \times N & \xrightarrow{- \otimes -} & M \otimes_A N \\ & \searrow f & \downarrow \exists! \bar{f} \\ & & G \end{array} \quad (3.1.16)$$

commutes.

Proof. To make this diagram commute we can define $\bar{f}(m \otimes n) = f(m, n)$. The fact that \bar{f} is a group homomorphism means that this uniquely defines

the value of \bar{f} on any element of $M \otimes_A N$ by

$$\bar{f}\left(\sum_i m_i \otimes n_i\right) = \sum_i f(m_i, n_i). \quad (3.1.17)$$

Note that $\text{Hom}_A(M, N)$ inherits the module structure of N via pointwise operations. Let M be an (A, B) -bimodule, N a (B, C) -bimodule, and P an (A, C) -bimodule for three algebras, A , B , and C . Then we can form the tensor product $M \otimes_B N$, which is an A -module, and we can consider the hom-set $\text{Hom}_A(M \otimes_B N, P)$, of left A -module homomorphisms, this is itself an A -module, and in fact is an (A, A) -bimodule. We can also form the hom-set $\text{Hom}_C(N, P)$ of right C -module homomorphisms, which is an left A -module under pointwise action using the A -module structure of P . Then we can take the hom-set $\text{Hom}_B(M, \text{Hom}_C(N, P))$, which is an A -module under pointwise the action. Then it turns out that we actually have an isomorphism

$$\text{Hom}_A(M \otimes_B N, P) \xrightarrow{\cong} \text{Hom}_B(M, \text{Hom}_C(N, P)) \quad (3.1.18)$$

given by sending f to g defined by $g(m)(n) = f(m \otimes n)$. This isomorphism is natural in all objects, and thus this is an adjunction.

3.2 Tensor Algebra

Definition 3.2.1 — Tensor Algebra Let V be a vector space over \mathbb{k} . Then the **tensor algebra**, TV , is defined to be

$$\bigoplus_{n=0}^{\infty} V^{\otimes n} = \mathbb{k} \oplus V \oplus (V \otimes V) \oplus (V \otimes V \otimes V) \oplus \cdots. \quad (3.2.2)$$

Multiplication is defined by $ab = a \otimes b \in V^{\otimes(n+m)}$ for $a \in V^{\otimes n}$ and $b \in V^{\otimes m}$, and extended linearly.

Lemma 3.2.3 Let V be an n -dimensional vector space over \mathbb{k} . Then TV is isomorphic to $\mathbb{k}\langle x_1, \dots, x_n \rangle$, the free algebra on n indeterminates.

Proof. Pick a basis for V . Identify this basis with the x_i . Elements of TV are linear combinations of tensor products of these basis elements, so we can identify them with polynomials in non-commuting variables. For example, given the basis $\{e_i\}$ for V we have that $e_1 \otimes e_2 \otimes e_1$ maps to $x_1 x_2 x_1$, and $e_1 \otimes e_2 + e_1 \otimes e_3 \otimes e_2$ maps to $x_1 x_2 + x_1 x_3 x_2$. \square

The nice thing about the tensor algebra is that it gives us a basis free way to work with the free algebra, that is a way that is independent of the choice of generators. As it is there is no commutativity imposed on the product in TV , we can impose some commutativity condition by taking quotients.

Definition 3.2.4 — Quotients of the Tensor Algebra Let V be a vector space over \mathbb{k} . We define following quotients:

- $SV := TV/\langle v \otimes w - w \otimes v \rangle$, the **symmetric algebra**; and
- $\Lambda V := TV/\langle v \otimes w + w \otimes v \rangle$, the **exterior algebra**.

If $\mathfrak{g} = V$ is a Lie algebra then we may define the quotient $\mathcal{U}(\mathfrak{g}) := TV/\langle v \otimes w - w \otimes v - [v, w] \rangle$, the **universal enveloping algebra**.

The idea is that for SV we impose that² $v \otimes w = w \otimes v$, which makes SV isomorphic to $\mathbb{k}[x_1, \dots, x_n]$ for $n = \dim V$. For ΛV we impose that $v \otimes w = -w \otimes v$ (usually the product here is written as $v \wedge w$). Finally, for $\mathcal{U}(\mathfrak{g})$ we impose that the bracket, $[v, w]$ is exactly the commutator $v \otimes w - w \otimes v$. This last case is nice because it allows us to treat the abstract bracket as if it were a commutator.

²identifying elements with their equivalence class

Note that the tensor algebra, as well as the quotients SV and ΛV , are graded algebras, meaning that they have decompositions as direct sums:

$$SV = \bigoplus_{n=0}^{\infty} S^n V, \quad \text{and} \quad \Lambda V = \bigoplus_{n=0}^{\infty} \Lambda^n V. \quad (3.2.5)$$

Here $S^n V$ ($\Lambda^n V$) is the n th (anti)symmetric tensor power of V , that is, it's $V^{\otimes n}$ modulo the relation that factors (anti)commute. Note that $S^n V$ is isomorphic to the subalgebra of $\mathbb{k}[x_1, \dots, x_n]$ consisting of homogeneous polynomials of degree n .

Four

Jacobson's Density Theorem

4.1 Semisimple Representations

Recall that a module is semisimple if it is a direct sum of simple modules, and a simple module is one with no nontrivial submodules.

Example 4.1.1 Let V be an n -dimensional simple A -module. Then $\text{End } V$ is an A -module as well, with A acting by left matrix multiplication (after fixing some basis so that elements of $\text{End } V$ can be identified with matrices and then identifying elements of A acting on $\text{End } V$ with the corresponding linear operator on V). With this construction $\text{End } V$ is semisimple, in particular

$$\text{End } V \cong \underbrace{V \oplus \cdots \oplus V}_{n \text{ terms}} =: nV. \quad (4.1.2)$$

This isomorphism is given by fixing some basis, $\{v_1, \dots, v_n\} \subseteq V$, and then defining a linear map $\text{End } V \rightarrow nV$ by $\varphi \mapsto (\varphi(v_1), \dots, \varphi(v_n))$. Viewing v_i as column matrices $\varphi(v_i)$ is simply the i th column of the matrix corresponding to φ in this basis.

In this example $\text{End } V$ ends up being a direct sum of a single simple module. In the general semisimple case any simple module can appear in the decomposition. If we restrict ourselves to finite dimensions then we can get a pretty good handle on which simple modules appear in such a decomposition. In particular, any finite-dimensional semisimple module, V , may be decomposed as

$$V = \bigoplus_{i \in I} m_i V_i \quad (4.1.3)$$

with $m_i \in \mathbb{Z}_{\geq 0}$ and V_i running over all finite dimensional simple modules. We call m_i the **multiplicity** of V_i in V . Note that since this decomposition is unique up to the order of the terms.

Lemma 4.1.4 Let V be a finite dimensional semisimple A -module, with decomposition

$$V = \bigoplus_{i \in I} m_i V_i \quad (4.1.5)$$

with $m_i \in \mathbb{Z}_{\geq 0}$ and V_i simple. Then the multiplicity, m_i , is given by

$$m_i = \dim(\text{Hom}_A(V_i, V)). \quad (4.1.6)$$

Proof. We make use of the fact that^a

$$\text{Hom}_A(V_i, V' \oplus V'') \cong \text{Hom}_A(V_i, V') \oplus \text{Hom}_A(V_i, V''). \quad (4.1.7)$$

This extends to all finite direct sums.

Note that $\text{Hom}_A(V_i, V)$ is an (A, \mathbb{k}) -bimodule with the left action $(a \cdot \varphi)(v) = \varphi(a \cdot v)$ and right action $(\varphi \cdot \lambda)(v) = \lambda \varphi(v)$. Further, V_i is a right \mathbb{k} -module with the action $v \cdot \lambda = \lambda v = (\lambda 1_A) \cdot v$. Thus, $\text{Hom}_A(V_i, V) \otimes_{\mathbb{k}} V_i$ is a left A -module.

We can define a map

$$\begin{aligned} \psi : \bigoplus_{i \in I} \text{Hom}_A(V_i, V) \otimes_{\mathbb{k}} V_i &\rightarrow V \\ \bigoplus_{i \in I} \varphi_i \otimes v_i &\mapsto \sum_i \varphi_i(v_i). \end{aligned} \quad (4.1.8)$$

This is an A -module isomorphism:

$$\psi(a \cdot \bigoplus_{i \in I} \varphi_i \otimes v_i) = \psi(\bigoplus_{i \in I} \varphi_i \otimes (a \cdot v_i)) \quad (4.1.9)$$

$$= \sum_{i \in I} \varphi_i(a \cdot v_i) \quad (4.1.10)$$

$$= \sum_{i \in I} a \cdot \varphi_i(v_i) \quad (4.1.11)$$

$$= a \cdot \sum_{i \in I} \varphi_i(v_i) \quad (4.1.12)$$

$$= a \cdot \psi(\bigoplus_{i \in I} \varphi_i \otimes v_i). \quad (4.1.13)$$

Linearity is clear from the definition. It remains only to show that this map is invertible. By linearity it is sufficient to show that the map

$$\text{Hom}(V_i, V) \otimes V_i \rightarrow V \quad (4.1.14)$$

$$\varphi_i \otimes v_i \mapsto \varphi_i(v_i) \quad (4.1.15)$$

is an isomorphism. Since V_i is simple Schur's lemma tells us that this map is either zero or surjective. It is clearly not zero, since we can simply choose some vector v_i and some nonzero map φ_i on which $\varphi_i(v_i) \neq 0$. Thus, this map is surjective. A surjective linear map between finite dimensional modules is an isomorphism. Hence, the map in Equation (4.1.8) is an isomorphism.

We then have

$$\dim V = \dim\left(\bigoplus_{i \in I} \text{Hom}_A(V_i, V)\right) \quad (4.1.16)$$

$$= \sum_{i \in I} \dim(\text{Hom}_A(V_i, V)) \dim(V_i) \quad (4.1.17)$$

and

$$\dim V = \dim\left(\bigoplus_{i \in I} m_i V_i\right) \quad (4.1.18)$$

$$= \sum_{i \in I} m_i \dim(V_i). \quad (4.1.19)$$

Since these are finite sums and this must hold for arbitrary semisimple modules V , including the case where $V = V_i$ is actually simple, we must have that

$$m_i = \dim(\text{Hom}_A(V_i)).$$

□

^a $\text{Hom}(V_i, -)$ is right adjoint (to $- \otimes_A V_i$) and as such preserves colimits

The decomposition into simple submodules also puts restrictions on the non-simple submodules that we can have. First, every submodules of a semisimple module must itself be semisimple, meaning it has its own decomposition into simple modules. Further, the simple modules that can appear in the decomposition of the submodule are only the ones that appear in the decomposition of the module. Finally, the multiplicity with which these simple modules appear in the submodule must be at most the multiplicity with which they appear in the original module. That is, the only way to form a submodule of a semisimple module is to take some subset of the simple modules that appear in the decomposition and take their direct sum.

Proposition 4.1.20 Let V be a semisimple finite-dimensional A -module with decomposition

$$V = \bigoplus_{i=1}^m n_i V_i \quad (4.1.21)$$

with the V_i pairwise-nonisomorphic simple A -modules. Let $W \subseteq V$ be a submodule. Then

$$W = \sum_{i=1}^m r_i V_i \quad (4.1.22)$$

with $0 \leq r_i \leq n_i$ for all i , and the inclusion $\varphi : W \hookrightarrow V$ decomposes as

$$\varphi = \bigoplus_{i=1}^m \varphi_i \quad (4.1.23)$$

where $\varphi_i : r_i V_i \rightarrow n_i V_i$ are maps given by $\varphi_i(v_1, \dots, v_{r_i}) = (v_1, \dots, v_{r_i}) \cdot X_i$ where $X_i \in \text{Mat}_{r_i \times n_i}(\mathbb{k})$ acts on the row vector by right matrix multiplication and has rank r_i .

Proof. The proof is by induction on $n = \sum_{i=1}^m n_i$. For the base case we just have that V is simple, and so its only submodules are the zero module (the empty direct sum) or V itself, in which case the statement clearly holds. Now suppose that this is the case when $\sum_i n_i = n-1$. Fix some submodule, $W \subseteq V$. If $W = 0$ then we're done, so suppose $W \neq 0$. Fix some simple submodule, $P \subseteq W$. Such a P exists as a consequence of [Lemma 4.1.29](#). By Schur's lemma P must be isomorphic to V_i for some i , and the inclusion

$\varphi|_P : P \rightarrow V$ factors through $n_i V_i$ by

$$P \xrightarrow{\cong} V_i \hookrightarrow n_i V_i \hookrightarrow V. \quad (4.1.24)$$

Identifying P with V_i this map is given by

$$v \mapsto (vq_1, \dots, vq_{n_i}) \quad (4.1.25)$$

with $q_i \in \mathbb{k}$ not all zero.

The group $G_i = \text{GL}_{n_i}(\mathbb{k})$ acts on $n_i V_i$ by right matrix multiplication. We can also act trivially on $n_j V_j$ for $j \neq i$. Then G_i acts on V . This gives an action of G_i on the set of submodules of V , and this action preserves the property that we're trying to establish, that under the action of $g_i \in G_i$ the matrix X_i goes to $X_i g_i$ while the matrices X_j ($j \neq i$) are left unchanged. Taking $g_i \in G_i$ such that $(1, \dots, q_{n_i})g_i = (1, 0, \dots, 0)$, which is always possible as g_i is invertible, we have that Wg_i contains the first summand, V_i , of $n_i V_i$. Thus, $Wg_i \cong V_i \oplus W'$ where

$$W' \subseteq n_1 V_1 \oplus \dots \oplus (n_i - 1)V_i \oplus \dots \oplus n_m V_m \quad (4.1.26)$$

is the kernel of the projection of Wg_i onto the first summand V_i . The inductive hypothesis then holds for this subspace, and so it has a decomposition

$$W' \cong \bigoplus_{j=1}^m r'_j V_j \quad (4.1.27)$$

with $0 \leq r'_i \leq n_i - 1$ and $0 \leq r_j \leq n_j$ for $j \neq i$, and so taking

$$W \cong V_i \oplus W' \cong \bigoplus_{j=1}^m r_j V_j \quad (4.1.28)$$

with $r_i = r'_i + 1$ and $r_j = r'_j$ we get the desired result. \square

Lemma 4.1.29 Any nonzero finite dimensional A -module contains a simple submodule.

Proof. The proof is by induction on dimension. Let V be a finite dimensional nonzero A -module. We start with $\dim V = 1$. Then V is itself simple, and we are done. Suppose then that all A -modules of dimension at most k contain a simple submodule. Consider the case when $\dim V = k+1$. If V is simple we are done. If V is not simple then it contains a proper submodule, W . Since W is a *proper* submodule it has dimension less than $k+1$, and thus the induction hypothesis holds. Thus, W has a simple submodule, which is then also a simple submodule of V . Then, by induction, the statement holds for all finite dimensional A -modules. \square

Remark 4.1.30 We assumed that \mathbb{k} was algebraically closed in the use of Schur's lemma above. However, this is not required for a modified result to hold. If we replace $\text{Mat}_{r_i \times n_i}(\mathbb{k})$ with $\text{Mat}_{r_i \times n_i}(D_i)$ where $D_i = \text{End}_A(V_i)$ then the result holds for any field \mathbb{k} . The D_i are division algebras (algebras in which division by any nonzero element is defined). When \mathbb{k} is algebraically closed Schur's lemma applies and tells us that the maps $V_i \rightarrow V_i$ are just scalar multiplication, allowing us to identify D_i with \mathbb{k} to get the result as stated above.

Corollary 4.1.31 Let V be a finite dimensional simple A -module. Given two subsets $\{x_1, \dots, x_n\}, \{y_1, \dots, y_n\} \subseteq V$ with the first being linearly independent there exists some $a \in A$ such that $a \cdot x_i = y_i$.

Proof. The proof is by contradiction, so suppose that this is not the case. Then $W = \{(a \cdot x_1, \dots, a \cdot x_n) \mid a \in A\}$ must be a proper submodule of nV , that is there is some element of V we can pick for one of the y_i such that we cannot reach (y_1, \dots, y_n) by the action of a . Then since V is simple we know that $W = rV$ for some $r < n$, a strict inequality since we have a *proper* submodule. By Proposition 4.1.20 we know that there is some $X \in \text{Mat}_{r \times n}(\mathbb{k})$ and some $u_1, \dots, u_r \in V$ such that

$$(u_1, \dots, u_r) \cdot X = (x_1, \dots, x_n). \quad (4.1.32)$$

To achieve this result we've just considered the $a = 1$ case to get $(x_1, \dots, x_n) \in W = rV$. Since $r < n$ we know that there is some $(z_1, \dots, z_n) \in \mathbb{k}^n \setminus \{0\}$ such that $X \cdot (z_1, \dots, z_n)^T = 0$, because X only has rank r . Thus, we can consider

$$0 = (u_1, \dots, u_r) \cdot X \cdot (z_1, \dots, z_n)^T \quad (4.1.33)$$

$$= (x_1, \dots, x_n) \cdot (z_1, \dots, z_n)^T \quad (4.1.34)$$

$$= \sum_{i=1}^n z_i x_i. \quad (4.1.35)$$

Since the x_i are linearly independent this means that $z_i = 0$, a contradiction. \square

4.2 Density Theorem

We're now ready to start working towards a result known as the density theorem. This result says that a certain class of algebras are basically just direct sums of matrix algebras. We have to prove some technical results first though.

Theorem 4.2.1. Let V be a finite dimensional A -module.

1. If V is simple then the associated algebra morphism $r : A \rightarrow \text{End } V$ is surjective.

2. If $V = \bigoplus_{i=1}^m V_i$ with the V_i pairwise nonisomorphic finite dimensional simple A -modules then

$$r = \bigoplus_{i=1}^m r_i : A \rightarrow \bigoplus_{i=1}^m \text{End } V_i \quad (4.2.2)$$

is surjective.

Proof. 1. Fix some basis, $\{v_1, \dots, v_n\} \subseteq V$, and let $w_i = \varphi(v_i)$ for some $\varphi \in \text{End } V$. Then by [Corollary 4.1.31](#) there exists some $a \in A$ such that $a \cdot v_i = w_i$, and thus $r(a) = \varphi$, so r is surjective.

2. Let B_i be the image of A in $\text{End } V_i$. Notice that $\text{End } V_i \cong d_i V_i$ where $d_i = \dim V_i$. Let B be the image of A in $\bigoplus_i \text{End } V_i$. Then $B \cong \bigoplus_i B_i \cong \bigoplus_i d_i V_i$, and the first part tells us that $B_i = \text{End } V_i$ by surjectivity of each representation map, and thus $B \cong \bigoplus \text{End } V_i$, so r is surjective. \square

The next result considers what happens when we have an algebra that is a direct sum of matrix algebras. Before the proof however we need the following definition.

Definition 4.2.3 — Dual Module Let V be a left A -module. Then the **dual module** is $V^* = \text{Hom}_{\mathbb{k}}(V, \mathbb{k})$ with the action defined by $(f \cdot a)(v) = f(a \cdot v)$ for all $f \in V^*$, $a \in A$, and $v \in V$.

Theorem 4.2.4. Let \mathbb{k} be a field which is not necessarily algebraically closed. Let A be the \mathbb{k} -algebra given by

$$A = \bigoplus_{i=1}^r \text{Mat}_{d_i}(\mathbb{k}) \quad (4.2.5)$$

for some $d_i \in \mathbb{N}$. Then

1. the simple A -modules are \mathbb{k}^{d_i} with (X_1, \dots, X_r) acting by matrix multiplication by X_i ; and
2. any finite dimensional A -module is semisimple.

Proof. 1. Let $v, w \in \mathbb{k}^{d_i}$ be such that $v \neq 0$. Then there exists some linear map sending v to w , and hence some matrix $X \in \text{Mat}_{d_i}(\mathbb{k})$ such that $Xv = w$. Thus, $V_i = \mathbb{k}^{d_i}$ must be simple since any nonzero subspace containing v and not w cannot be a submodule.

2. Let W be a finite dimensional left A -module. Consider its dual, W^* , which we can think of as a left A^{op} -module. The algebra A^{op} is given

by

$$A^{\text{op}} = \bigoplus_i \text{Mat}_{d_i}(\mathbb{k})^T \cong \bigoplus_i \text{Mat}_{d_i}(\mathbb{k}) \quad (4.2.6)$$

and we identify $a \in A$ with $a^T \in A^{\text{op}}$ where $(X_1, \dots, X_r)^T = (X_1^T, \dots, X_r^T)$. Really nothing is going on here since we're considering square matrices so taking the transpose changes individual elements but doesn't change the set of all matrices under consideration.

What this lets us do is interpret W^* as an A -module with $a \cdot f = f \cdot a^T$. We can fix a basis $\{f_1, \dots, f_n\} \subseteq W^*$, and then define a surjection

$$\varphi : nA \twoheadrightarrow W^* \quad (4.2.7)$$

$$a_1 \oplus \dots \oplus a_n \mapsto a_1 \cdot f_1 + \dots + a_n \cdot f_n. \quad (4.2.8)$$

This is a surjection by [Theorem 4.2.1](#). We can consider the dual map, $\varphi^* : W \hookrightarrow (nA)^* \cong nA$, which will be an injection. Further, $W \cong \text{im } \varphi^* \subseteq nA$ is a submodule of the semisimple module nA (where $a \cdot (b_1 \oplus \dots \oplus b_n) = ab_1 \oplus \dots \oplus ab_n$) and we can apply [Proposition 4.1.20](#) to conclude that W is semisimple. □

What we have just shown is that matrix algebras, and their direct sums, have particularly nice properties. We understand their simple modules well, they're just \mathbb{k}^d with d appearing as the number of rows of some matrix, and all finite dimensional modules are semisimple, so all are just some direct sum $\bigoplus_i \mathbb{k}^{d_i}$. The logical next question is when is a given algebra, A , isomorphic to some direct sum of matrix algebras? It turns out that there's a simple subspace we can consider that vanishes only when A is a direct sum of matrix algebras.

Definition 4.2.9 — Radical Let A be an algebra. We call

$$\text{Rad } A = \{a \in A \mid a \text{ acts as zero on any simple } A\text{-module}\} \subseteq A \quad (4.2.10)$$

the **radical** of A .

Definition 4.2.11 — Nilpotent Ideal Let A be an algebra. We call $a \in A$ a **nilpotent element** if there exists some $k \in \mathbb{N}$ such that $a^k = 0$. A **nilpotent ideal** is an ideal in which all elements are nilpotent.

Proposition 4.2.12

1. $\text{Rad } A$ is a two-sided ideal.
2. If A is finite dimensional then any nilpotent two-sided ideal is contained in $\text{Rad } A$.

3. $\text{Rad } A$ is the largest two-sided nilpotent ideal.

Proof. 1. We first show that $\text{Rad } A$ is a subspace. Let V be a simple A -module. Then if $a, b \in \text{Rad } A$ we have

$$(a + b) \cdot v = a \cdot v + b \cdot v = 0 + 0 = 0 \quad (4.2.13)$$

for all $v \in V$, and thus $\text{Rad } A$ is closed under addition. If $\lambda \in \mathbb{k}$ we also have

$$(\lambda a) \cdot v = \lambda(a \cdot v) = \lambda 0 = 0, \quad (4.2.14)$$

and so $\text{Rad } A$ is closed under scalar multiplication. Thus, $\text{Rad } A$ is a subspace of A .

Let $a \in \text{Rad } A$ and $b \in A$. Then we know that if V is a simple A -module $a \cdot v = 0$ for all $v \in V$. We therefore have

$$(ab) \cdot v = a \cdot (b \cdot v) = 0, \quad \text{and} \quad (ba) \cdot v = b \cdot (a \cdot v) = b \cdot 0 = 0 \quad (4.2.15)$$

since $b \cdot v \in V$ so a acts on it by zero, and b acts linearly so it sends 0 to 0. Thus, $ab, ba \in \text{Rad } A$, so $\text{Rad } A$ is a two-sided ideal.

2. Let V be a simple A -module and I a nilpotent ideal. Fix some nonzero $v \in V$. Then $I \cdot v \subseteq V$ is a submodule. By simplicity of V there are two possibilities

- $I \cdot v = V$, and since $v \in V$ there must be some $x \in I$ such that $x \cdot v = v$, but then we cannot have that $x^k = 0$ for any $k \in \mathbb{N}$ as we must have $x^k \cdot v = v$, so we can't have $I \cdot v = V$ if I is nilpotent;
- $I \cdot v = 0$, in which case every element of I acts as zero on any element of V , and so $I \subseteq \text{Rad } A$.

3. Let

$$0 = A_0 \subseteq A_1 \subseteq A_2 \subseteq \cdots \subseteq A_n = A \quad (4.2.16)$$

be a filtration of the regular representation of A such that A_{i+1}/A_i is simple. Such a filtration exists by [Lemma 4.2.19](#).

Let $x \in \text{Rad } A$, then x acts on the simple A -module A_{i+1}/A_i by zero, and so x must map any element of A_{i+1} to some element of A_i , since that will then be sent to zero in the quotient. Thus x^n acts as zero on all of $A_n = A$, and so $\text{Rad } A$ is nilpotent. By the previous part we also know that $\text{Rad } A$ contains any nilpotent two-sided ideal, and so $\text{Rad } A$ is the largest two-sided nilpotent ideal (ordered by inclusion). \square

Definition 4.2.17 — Filtration Let V be an A -module. A finite **filtration** of

V is a sequence of submodules

$$0 = V_0 \subseteq V_1 \subseteq \cdots \subseteq V_n = V. \quad (4.2.18)$$

Lemma 4.2.19 Let V be a finite dimensional A -module. Then there is a filtration

$$0 = V_0 \subseteq V_1 \subseteq \cdots \subseteq V_n = V \quad (4.2.20)$$

for which V_{i+1}/V_i is a simple A -module for all i .

Proof. We induct on $\dim V$. If $\dim V = 0$ then we have the filtration $0 = V_0 = V$ and we are done. Suppose the result holds for all dimensions less than $\dim V$. If V is simple then we have the filtration $0 = V_0 \subseteq V_1 = V$ and $V/0 \cong V$ is simple, so we're done. Suppose then that V is not simple, and pick some nontrivial submodule $V_1 \subsetneq V$. Take the module $U = V/V_1$. Since $V_1 \neq 0$ we know that $\dim(V/V_1) < \dim V$, and so by the induction hypothesis there is a filtration

$$0 = U_0 \subseteq U_1 \subseteq \cdots \subseteq U_{n-1} = U \quad (4.2.21)$$

such that U_{i+1}/U_i is simple. Let $\pi : V \twoheadrightarrow V/V_1$ be the canonical projection. For $i \geq 2$ define $V_i = \pi^{-1}(U_i)$ to be the preimage of U_i under this projection. Then we have the filtration

$$0 = V_0 \subseteq V_1 \subseteq \cdots \subseteq V_n = V. \quad (4.2.22)$$

Note that here we've used the fact that the preimage under a module morphism of a submodule of the codomain is a submodule of the domain, which can be seen as follows: take $v \in V_i$ and we have some $u \in U_i$ such that $\pi(v) = u$, then

$$a \cdot v = a \cdot \pi^{-1}(u) = \pi^{-1}(a \cdot u) \in V_i \quad (4.2.23)$$

which shows that $a \cdot v \in V_i$ also, so V_i is closed under the action of A , and the preimage of a subspace is again a subspace.

All we have to do now is show that the given filtration has the desired property. To see that this is indeed the case consider $V_{i+1}/V_i = \pi^{-1}(U_{i+1})/\pi^{-1}(U_i) \cong \pi^{-1}(U_{i+1}/U_i)$ which shows that V_{i+1}/V_i is the preimage of a simple module, and must therefore be simple itself, if it wasn't then the image of any nontrivial submodule of V_{i+1}/V_i would provide a nontrivial submodule of U_{i+1}/U_i . \square

The following result gives us a handle on the number of simple A -modules in the finite dimensional case. It also shows that given any algebra we can always quotient by the radical to get something isomorphic to a direct sum of endomorphism spaces, which is isomorphic to a direct sum of matrix algebras. In this way

the radical consists of the elements which obstruct our attempt to understand A as being formed from matrix algebras.

Notation 4.2.24 We write $\text{Irr}(A)$ for the set of isomorphism classes of simple A -modules. We further assume that each isomorphism class has some canonical choice of representative, which we'll call V_i , so we can take $\text{Irr}(A) = \{V_i\}$. We assume that sums over the index i in V_i run over all simple A -modules.

Theorem 4.2.25. Any finite dimensional algebra, A , has only finitely many simple A -modules, V_i , (up to isomorphism) and

$$\sum_i (\dim V_i)^2 \leq \dim A. \quad (4.2.26)$$

Further,

$$A/\text{Rad } A \cong \bigoplus_i \text{End } V_i. \quad (4.2.27)$$

Proof. Let V be a simple A -module and take some $v \in V$ with $v \neq 0$. Then $A \cdot v \neq 0$ since $1 \in A$ so $v \in A \cdot v$. Thus, by simplicity we must have that $A \cdot v = V$. Further, V is finite dimensional since A is finite dimensional, and if we could construct infinitely many linearly independent elements by acting on v with elements of A those infinitely many elements of A would be linearly independent in A , a contradiction.

Now let $\{V_i\} = \text{Irr}(A)$ be the set of simple A -modules. Then by [Theorem 4.2.1](#) we have a surjection

$$\bigoplus_i \rho_i : A \twoheadrightarrow \bigoplus_i \text{End } V_i. \quad (4.2.28)$$

Thus, we have

$$\dim \left(\bigoplus_i \text{End } V_i \right) = \sum_i \dim(\text{End } V_i) \quad (4.2.29)$$

$$= \sum_i (\dim V_i)^2 \quad (4.2.30)$$

where we've used the fact that the dimension of a direct sum is the sum of the dimensions, and $\text{End } V$ has dimension $(\dim V)^2$, which can be seen by fixing a basis for V and considering elements of $\text{End } V$ as $(\dim V) \times (\dim V)$ matrices. Finally, since the above map is a surjection the dimension is bounded by $\dim A$, and thus we have

$$\sum_i (\dim V_i)^2 \leq \dim A \quad (4.2.31)$$

as claimed.

We have that

$$\ker \left(\bigoplus_i \rho_i \right) = \text{Rad } A \quad (4.2.32)$$

since by definition elements of this kernel are sent to the zero map when they act on each simple module, V_i , and this is exactly the definition of said elements being in $\text{Rad } A$. Thus, by the first isomorphism theorem we have that

$$A / \ker \left(\bigoplus_i \rho_i \right) = A / \text{Rad } A \cong \bigoplus_i \text{End } V_i. \quad \square$$

We now give a definition of a semisimple algebra. Note that several equivalent definitions are in use, and some of these are covered in [Proposition 4.2.34](#).

Definition 4.2.33 — Semisimple Algebra A finite dimensional algebra, A , is **semisimple** if $\text{Rad } A = 0$.

Proposition 4.2.34 Let A be a finite dimensional algebra, then the following are equivalent:

- (I) A is semisimple, that is $\text{Rad } A = 0$;
- (II) $\dim A = \sum_i (\dim V_i)^2$ where V_i runs over all simple A -modules;
- (III) $A \cong \bigoplus_i \text{Mat}_{d_i}(\mathbb{k})$ for some $d_i \in \mathbb{N}$;
- (IV) Any finite dimensional A -module is semisimple. In particular, the regular representation is semisimple.

Proof. STEP 1: (I) \implies (II)
We have that

$$A / \text{Rad } A \cong \bigoplus_i \text{End } V_i \quad (4.2.35)$$

and taking dimensions we have

$$\dim(A / \text{Rad } A) = \sum_i (\dim V_i)^2. \quad (4.2.36)$$

If A is semisimple then $\text{Rad } A = 0$ and this reduces to the equality

$$\dim A = \sum_i (\dim V_i)^2. \quad (4.2.37)$$

STEP 2: (I) \implies (III)

By [Theorem 4.2.25](#) we know that

$$A / \text{Rad } A \cong \bigoplus_i \text{End } V_i \quad (4.2.38)$$

and if A is semisimple then $\text{Rad } A = 0$ so this reduces to

$$A \cong \bigoplus_i \text{End } V_i. \quad (4.2.39)$$

Fixing some basis for V_i we may identify elements of $\text{End } V_i$ with matrices in $\text{Mat}_{d_i}(\mathbb{k})$ where $d_i = \dim V_i$. Thus, we have

$$A \cong \bigoplus_i \text{Mat}_{d_i}(\mathbb{k}). \quad (4.2.40)$$

STEP 3: (III) \implies (IV)

By the second part of [Theorem 4.2.4](#) we have that any finite dimensional A -module is semisimple.

STEP 4: (IV) \implies (I)

Consider the regular representation of A which decomposes as

$$A \cong \bigoplus_i n_i V_i \quad (4.2.41)$$

with V_i simple and $n_i \in \mathbb{Z}_{\geq 0}$. Take some $x \in \text{Rad } A$, then by definition x acts as zero on each V_i submodule, and so acts as zero on all of A , in particular $x \cdot 1 = 0$. In the regular representation the action of x is just multiplication, so $x \cdot 1 = x1 = x$, thus we must have $x = 0$, and hence $\text{Rad } A = 0$. \square

One question that we may ask is how many simple A -modules are there (up to isomorphism)? Of course, if we can find the decomposition $A \cong \bigoplus_i \text{End } V_i$ then we have answered the question, but we can often answer the question much faster with the following result definition and result.

Definition 4.2.42 — Centre Let A be an algebra. The **centre** of A , denoted $Z(A)$, is the subalgebra

$$Z(A) := \{a \in A \mid ab = ba \forall b \in A\}. \quad (4.2.43)$$

That is, the centre is the subspace consisting of all elements of A that commute with all other elements of A . This is clearly a subspace since if $a, a' \in Z(A)$ then $(a + \lambda a')b = ab + \lambda a'b = ba + \lambda ba' = b(a + \lambda a')$ for all $b \in A$ and $\lambda \in \mathbb{k}$. This is in fact a subalgebra since if $a, a' \in Z(A)$ then $aa'b = aba' = aa'b$ so $aa' \in Z(A)$.

Lemma 4.2.44 Let A be a finite dimensional semisimple algebra. Then

$$|\text{Irr}(A)| = \dim Z(A). \quad (4.2.45)$$

Proof. First note that if A_1 and A_2 are algebras then

$$Z(A_1 \oplus A_2) = Z(A_1) \oplus Z(A_2), \quad (4.2.46)$$

since if $(a_1, a_2) \in Z(A_1 \oplus A_2)$ then we have

$$(a_1, a_2)(b_1, b_2) = (b_1, b_2)(a_1, a_2) \quad (4.2.47)$$

for all $b_1, b_2 \in A_1 \oplus A_2$, and evaluating the left hand side gives $(a_1 b_1, a_2 b_2)$

and the right hand side gives $(b_1 a_1, b_2 a_2)$, so this equality holds if and only if $a_i b_i = b_i a_i$ for all $b_i \in A_i$, in other words, if $a_i \in Z(A_i)$ and thus if and only if $(a_1, a_2) \in Z(A_1) \oplus Z(A_2)$.

Since A is semisimple we know that $\text{Rad } A = 0$, and thus

$$A / \text{Rad } A = A / 0 \cong A \cong \bigoplus_i \text{End } V_i \quad (4.2.48)$$

by [Theorem 4.2.25](#). Thus, we have

$$Z(A) = \bigoplus_i Z(\text{End}(V_i)). \quad (4.2.49)$$

Further, since V_i is a simple module we know by Schur's lemma ([Proposition 2.5.5](#)) that if an element commutes with all other elements then said element is just scalar multiplication, and further any multiplication by a scalar gives such a map, so

$$Z(\text{End } V_i) \cong \mathbb{k}. \quad (4.2.50)$$

Combining these two results we have

$$Z(A) \cong \bigoplus_i \mathbb{k} = |\text{Irr } A| \mathbb{k} \quad (4.2.51)$$

and so

$$\dim Z(A) = |\text{Irr } A| \quad (4.2.52)$$

where we've used the fact that the sum is indexed by simple A -modules, so has exactly as many terms as there are simple A -modules, and of course, $\dim \mathbb{k} = 1$. \square

Note that if A is not semisimple then this result no longer holds, since $A / \text{Rad } A \not\cong A$. However, given a simple A -module, V , we know that all elements of $\text{Rad } A$ act on V by zero, and thus there is a corresponding $(A / \text{Rad } A)$ -module V' , which has the same underlying space, but now elements of $A / \text{Rad } A$ act by $[a] \cdot v = a \cdot v$ for any representative a of this equivalence class. This gives a well-defined action precisely because elements of $\text{Rad } A$ act by zero, so if a' is some other representative then $a - a' \in \text{Rad } A$ and thus $0 = (a - a') \cdot v = a \cdot v - a' \cdot v$ and thus $a \cdot v = a' \cdot v$ as required.

In fact, more generally if I is an ideal of A and V is an A -module on which all elements of I act as zero then A/I acts on V by $[a] \cdot v = a \cdot v$. This can be quite useful when we define algebras via a quotient, first construct an A -module, V , then show that the ideal $I \subseteq A$ acts as zero on V , then we automatically get an (A/I) -module structure for V .

Five

Character Theory

In this chapter we study character theory. The general idea being that for finite dimensional representations we can identify elements of A with linear maps $V \rightarrow V$ which we can identify with matrices. We can then take the trace of these matrices, which is a nice thing to do because the trace is basis independent, despite the identification of elements and matrices requiring us to pick a basis. We can then learn a surprising amount just looking at these traces, which we call characters.

5.1 Definitions

Definition 5.1.1 — Character Let A be an algebra and V a finite dimensional A -module with the corresponding algebra homomorphism $\rho : A \rightarrow \text{End } V$. Then the **character** of V is the map

$$\chi_V : A \rightarrow \mathbb{k} \quad (5.1.2)$$

$$a \mapsto \chi_V(a) = \text{tr}_V \rho(a) \quad (5.1.3)$$

Note that we write tr_V to denote the trace of matrices corresponding to elements of $\text{End } V$ after fixing some basis. We do this because later we'll want to take characters over different modules, and it's helpful to be able to distinguish which space the matrices we're taking the trace of act on. When there's no chance of confusion we'll drop the subscript V .

Definition 5.1.4 Let A be an algebra with subalgebras $B, C \subseteq A$. Then we denote by $[B, C]$ the subspace

$$[B, C] = \text{span}\{[b, c] \mid b \in B \text{ and } c \in C\} \quad (5.1.5)$$

where $[b, c] = bc - cb$.

Note that for any A -module, V , with corresponding character χ_V , we have

$[A, A] \subseteq \ker \chi_V$, since

$$\chi_V([a, b]) = \text{tr}(\rho([a, b])) \quad (5.1.6)$$

$$= \text{tr}(\rho(a)\rho(b) - \rho(b)\rho(a)) \quad (5.1.7)$$

$$= \text{tr}(\rho(a)\rho(b)) - \text{tr}(\rho(b)\rho(a)) \quad (5.1.8)$$

$$= \text{tr}(\rho(a)\rho(b)) - \text{tr}(\rho(a)\rho(b)) \quad (5.1.9)$$

$$= 0, \quad (5.1.10)$$

having used the cyclic property of the trace. Thus $[a, b] \in \ker \chi_V$ for all $a, b \in A$, and since the kernel is a subspace any linear combination of commutators will also vanish under χ_V , showing that $[A, A] \subseteq \ker \chi_V$.

This tells us that the character also gives a well-defined map

$$\tilde{\chi}_V : A/[A, A] \rightarrow \mathbb{k} \quad (5.1.11)$$

defined by

$$\tilde{\chi}_V([a]) = \chi_V(a) = \text{tr}_V(\rho(a)). \quad (5.1.12)$$

In fact, it will prove more useful to define the character to be such a map. This allows us to view the character as an element of the dual space

$$\tilde{\chi}_V \in (A/[A, A])^* = \text{hom}_{\mathbb{k}}(A/[A, A], \mathbb{k}). \quad (5.1.13)$$

We will do this, and do not distinguish between χ_V and $\tilde{\chi}_V$ in the notation.

This is a useful thing to do because now the characters live in a vector space, and that lets us do linear-algebra-things to them, like look for a basis of this space.

Theorem 5.1.14. Let A be a finite dimensional algebra. The characters of distinct finite-dimensional simple A -modules are linearly independent in $(A/[A, A])^*$. Further, if A is finite dimensional and semisimple then the characters of simple A -modules provide a basis for $(A/[A, A])^*$.

Proof. STEP 1: LINEAR INDEPENDENCE

Let that A be a finite dimensional (not necessarily semisimple) algebra. Then there is a finite number, n , of simple A -modules, V_i for $i = 1, \dots, n$, with corresponding algebra homomorphisms $\rho_i : A \rightarrow \text{End } V_i$. Then by the density theorem we have a surjection

$$\rho_1 \oplus \dots \oplus \rho_n : A \twoheadrightarrow \text{End } V_1 \oplus \dots \oplus \text{End } V_n. \quad (5.1.15)$$

Suppose that

$$\sum_i \lambda_i \chi_{V_i} = 0 \quad (5.1.16)$$

with $\lambda_i \in \mathbb{k}$. If $a \in A$ we must therefore have

$$\sum_i \lambda_i \chi_{V_i}(a) = 0. \quad (5.1.17)$$

Now take some arbitrary $M \in \text{End } V_1 \oplus \cdots \oplus \text{End } V_n$, which we view as a matrix by fixing some basis, which fixes a basis for each V_i . We can then identify that $M = M_1 \oplus \cdots \oplus M_n$, where each $M_i \in \text{End } V_i$ is viewed as a matrix through the corresponding fixed basis. We can then consider the sum

$$\sum_i \lambda_i \text{tr}_{V_i} M_i \quad (5.1.18)$$

where the λ_i are the same coefficients as before. By surjectivity of $\rho_1 \oplus \cdots \oplus \rho_n$ we know that there is some $a \in A$ such that $M = (\rho_1 \oplus \cdots \oplus \rho_n)(a)$, and thus $M_i = \rho_i(a)$. This then gives that the sum above is

$$\sum_i \lambda_i \text{tr}_{V_i}(\rho_i(a)) = \sum_i \lambda_i \chi_{V_i}(a) = 0. \quad (5.1.19)$$

Now, we are free to choose M , and hence M_i , such that $\text{tr}_{V_i} M_i$ takes on any value in \mathbb{k} , which means that the only way this equation can hold for an arbitrary choice of M is if $\lambda_i = 0$ for all $i = 1, \dots, n$. Thus, the χ_{V_i} are linearly independent.

STEP 2: BASIS

Now suppose that A is a finite dimensional semisimple algebra. We have shown that the characters, χ_{V_i} , corresponding to simple A -modules, are linearly independent elements of $(A/[A, A])^*$. We now show that they are also a spanning set of $(A/[A, A])^*$.

Since A is semisimple we have that

$$A \cong \bigoplus_{i=1}^n \text{Mat}_{d_i}(\mathbb{k}) \quad (5.1.20)$$

where $d_i = \dim V_i$. We have the following well known fact about derived subalgebras of Lie algebras ([Lemma 5.1.29](#)):

$$[\text{Mat}_d(\mathbb{k}), \text{Mat}_d(\mathbb{k})] = [\mathfrak{gl}_{d_i}(\mathbb{k}), \mathfrak{gl}_{d_i}(\mathbb{k})] = (\mathfrak{gl}_{d_i}(\mathbb{k}))' = \mathfrak{sl}_d(\mathbb{k}). \quad (5.1.21)$$

The Lie algebra $\mathfrak{sl}_d(\mathbb{k})$ consists precisely of the $d \times d$ matrices over \mathbb{k} with zero trace. Further, for algebra B and C , we have

$$[B \oplus C, B \oplus C] = [B, B] \oplus [C, C], \quad (5.1.22)$$

which follows immediately by linearity. Thus, we have

$$[A, A] \cong \bigoplus_{i=1}^n \mathfrak{sl}_{d_i}(\mathbb{k}). \quad (5.1.23)$$

It then follows that

$$A/[A, A] \cong \left(\bigoplus_{i=1}^n \text{Mat}_{d_i}(\mathbb{k}) \right) / \left(\bigoplus_{i=1}^n \mathfrak{sl}_{d_i}(\mathbb{k}) \right) \quad (5.1.24)$$

$$= \left(\bigoplus_{i=1}^n \mathfrak{gl}_{d_i}(\mathbb{k}) \right) / \left(\bigoplus_{i=1}^n \mathfrak{sl}_{d_i}(\mathbb{k}) \right) \quad (5.1.25)$$

$$\cong \bigoplus_{i=1}^n \mathfrak{gl}_{d_i}(\mathbb{k}) / \mathfrak{sl}_{d_i}(\mathbb{k}) \quad (5.1.26)$$

$$\cong \bigoplus_{i=1}^n \mathbb{k} \quad (5.1.27)$$

$$= \mathbb{k}^n. \quad (5.1.28)$$

This shows that we have n -linearly independent elements, χ_{V_i} , and $\dim(A/[A, A]) = n$, so these linearly independent elements are actually a basis. \square

Lemma 5.1.29 The derived subalgebra of $\mathfrak{gl}_n(\mathbb{k})$ is $\mathfrak{sl}_n(\mathbb{k})$.

Proof. First note that $\mathfrak{gl}_n(\mathbb{k}) = \text{Mat}_n(\mathbb{k})$ is the (Lie algebra) of $n \times n$ matrices with entries in \mathbb{k} . The elementary matrices, E_{ij} , form a basis of $\mathfrak{gl}_n(\mathbb{k})$. Note that E_{ij} , for $i, j = 1, \dots, n$, are matrices which are zero everywhere except in row i and column j , where they have a 1. So, it is sufficient to show that the commutator of any two elementary matrices is in $\mathfrak{sl}_n(\mathbb{k})$, and then any linear span of such commutators will be in $\mathfrak{sl}_n(\mathbb{k})$. To do this first note that

$$E_{ij}E_{kl} = \delta_{jk}E_{il}. \quad (5.1.30)$$

Then we have

$$[E_{ij}, E_{kl}] = E_{ij}E_{kl} - E_{kl}E_{ij} \quad (5.1.31)$$

$$= \delta_{jk}E_{il} - \delta_{li}E_{kj}. \quad (5.1.32)$$

Now we consider cases:

1. if $i \neq l$ and $j \neq k$ we get 0;
2. if $l \neq i$ and $j = k$ we get E_{il} ;
3. if $l = i$ and $j \neq k$ we get $-E_{kj}$;
4. if $i = l$ and $j = k$ we get $E_{ii} - E_{jj}$.

We see that in each case the matrix we get is traceless, specifically in the last case if $i \neq j$ then the diagonal contains a 1 and a -1 , and if $i = j$ then we have zero, and the second and third case have zero on the diagonal since $i \neq l$ and $k \neq j$ in these two cases. Thus, each matrix we get from $[E_{ij}, E_{kl}]$ is an element of $\mathfrak{sl}_n(\mathbb{k})$. \square

Lemma 5.1.33 Characters are invariant under isomorphism.

Proof. Let V and W be isomorphic finite dimensional A -modules. Then V and W are related by an isomorphism, $V \rightarrow W$, but fixing bases for both we can view this isomorphism as a basis change, and the character is independent of basis choice. \square

Lemma 5.1.34 Let V be a finite dimensional A -module, and let $W \subseteq V$ be a submodule. Then

$$\chi_V = \chi_W + \chi_{V/W}. \quad (5.1.35)$$

Proof. Fix a basis for W and extend this to a basis of V . This can be done since $V = W \oplus V/W$ as vector spaces. Then any linear map $\varphi: V \rightarrow V$ such that $\varphi(W) \subseteq W$ decomposes into a linear map $W \rightarrow W$ and a linear map $V/W \rightarrow V/W$. Since W is a submodule $\rho(a)$ is exactly such a linear map for all $a \in A$, and thus

$$\mathrm{tr}_V \rho(a) = \mathrm{tr}_W \rho(a) + \mathrm{tr}_{V/W} \rho(a), \quad (5.1.36)$$

and so

$$\chi_V = \chi_W + \chi_{V/W}. \quad \square$$

5.2 Jordan–Hölder and Krull–Schmidt Theorems

We can now prove two standard results about filtrations using character theory.

Theorem 5.2.1 — Jordan–Hölder. Let V be a finite dimensional A -module with filtrations

$$0 = V_0 \subseteq V_1 \subseteq \cdots \subseteq V_n = V \quad (5.2.2)$$

and

$$0 = V'_0 \subseteq V'_1 \subseteq \cdots \subseteq V'_m = V \quad (5.2.3)$$

such that $W_i = V_i/V_{i-1}$ and $W'_i = V'_i/V'_{i-1}$ are simple. Then

1. $n = m$; and
2. There exists some $\sigma \in S_n$ such that $W_i \cong W'_{\sigma(i)}$, that is, the two series give rise to the same simple A -modules (up to isomorphism), but possibly in different orders.

Proof.



This proof holds only in characteristic 0. The result does hold in general though, and can be proven in positive characteristic by induction on the dimension of V . The problem in characteristic p is that the coefficients only end up being determined mod p .

Consider the character χ_V . Using the first series and [Lemma 5.1.34](#) we know that

$$\chi_V = \bigoplus_{i=1}^n \chi_{W_i}, \quad (5.2.4)$$

and using the second series we know that

$$\chi_V = \bigoplus_{i=1}^m \chi_{W'_i}. \quad (5.2.5)$$

Since the characters of the simple A -modules form a basis of $(A/[A, A])^*$ any decomposition such as the above must be unique, and thus we have $n = m$ and there is some permutation, $\sigma \in S_n$ such that $\chi_{W_i} = \chi_{W'_{\sigma(i)}}$, and thus $W_i \cong W'_{\sigma(i)}$. \square

Definition 5.2.6 — Jordan–Hölder Series Given a finite dimensional A -module, V , admitting a filtration

$$0 = V_0 \subseteq V_1 \subseteq \cdots \subseteq V_n = V \quad (5.2.7)$$

such that V_i/V_{i-1} are simple we call n the **length** of V , and the set of simple modules $\{V_i/V_{i-1}\}$ is called the **Jordan–Hölder series** of V .

Note that by the Jordan–Hölder theorem the length and Jordan–Hölder series are well-defined, being independent of the choice of filtration, so long as the quotient of successive modules is simple.

The following result holds for finite length modules. Note that finite length is a strictly weaker condition than finite dimension, since finite dimension guarantees the existence of

Theorem 5.2.8 — Krull–Schmidt. Every finite length A -module, V , is a direct sum of indecomposable modules. Further, this decomposition is unique up to isomorphism and permutation of the summands.

Proof. STEP 1: EXISTENCE

Let V be a finite length A -module. We may suppose that $V = V_1 \oplus V_2$ with V_i A -modules, and without loss of generality we assume that V_1 cannot be written as a sum of indecomposables. Then we must be able to decompose

V_1 again. Continuing on we see that this gives rise to an infinite length filtration, contradicting the assumption that V has finite length.

STEP 2: UNIQUENESS

We make use of [Lemma 5.2.14](#). Using this result take two decompositions into indecomposables

$$V = V_1 \oplus \cdots \oplus V_m = V'_1 \oplus \cdots \oplus V'_m. \quad (5.2.9)$$

We will prove that $V_k \cong V'_k$ for some k . Let

$$i_k : V_k \hookrightarrow V, \quad \text{and} \quad i'_k : V'_k \hookrightarrow V \quad (5.2.10)$$

be the natural inclusions, and

$$p_k : V \twoheadrightarrow V_k, \quad \text{and} \quad p'_k : V \twoheadrightarrow V'_k \quad (5.2.11)$$

be the natural projections. Then we have the map

$$\theta_k : p_1 \circ i'_k \circ p'_k \circ i_1 : V_1 \rightarrow V_1, \quad (5.2.12)$$

which is a composite of module morphisms, so is itself a module morphism. We also have that $\sum_k \theta_k = \text{id}_V$, since summing over all k the image of $i'_k \circ p'_k$ in the middle runs over all of V . We know that id_V is not nilpotent, so by the contrapositive of [Lemma 5.2.14](#) we know that at least one of the θ_k s must be an isomorphism. Without loss of generality we assume that θ_1 is an isomorphism. Then we have that

$$V_1 = \text{im}(p'_1 \circ i_1) \oplus \ker(p_1 \circ i'_1), \quad (5.2.13)$$

but V_1 is indecomposable, so $p'_1 \circ i_1 : V_1 \rightarrow V'_1$ must be an isomorphism. We may then consider $V_2 \oplus \cdots \oplus V_m \cong V'_2 \oplus \cdots \oplus V'_m$, and by the same logic we may take $V_2 \cong V'_2$. Repeating this eventually terminates after m applications. \square

Lemma 5.2.14 Let W be a finite dimensional indecomposable A -module. Then

1. any module morphism $\theta : W \rightarrow W$ is either an isomorphism or nilpotent;
2. if $\theta_i : W \rightarrow W$ for $i = 1, \dots, n$ is a set of nilpotent module morphisms then $\theta = \sum_i \theta_i$ is also a nilpotent module morphism.

Proof. We work over an algebraically closed field, thus W splits into a sum of generalised eigenspaces. These are submodules of W . Thus, θ can have only one eigenvalue, call it λ . If $\lambda = 0$ then θ is nilpotent, and if $\lambda \neq 0$ then θ is an isomorphism.

We prove that the sum of nilpotents is nilpotent by induction on n . For the

base case, $n = 1$, we clearly have that $\theta = \theta_1$ is nilpotent. Suppose then that the hypothesis holds up to n summands, and that at n summands θ is not nilpotent. Then θ must be an isomorphism, and thus its inverse exists, and we have $\text{id}_W = \theta\theta^{-1} = \theta^{-1} \sum_{i=1}^n \theta_i = \sum_{i=1}^n \theta^{-1}\theta_i$. Since the morphisms $\theta^{-1}\theta_i$ are not isomorphisms they are nilpotent, and thus $\text{id}_W - \theta^{-1}\theta_n = \theta^{-1}\theta_1 + \dots + \theta^{-1}\theta_{n-1}$ is an isomorphism, but it's also a sum of $n-1$ nilpotents, so it should be nilpotent, a contradiction. Thus by induction any such sum of nilpotents is itself nilpotent. \square

5.3 Tensor Products

Let A and B be \mathbb{k} -algebras. Then $A \otimes_{\mathbb{k}} B$ is also a \mathbb{k} -algebra when equipped with the product

$$(a \otimes b)(a' \otimes b') = aa' \otimes bb' \quad (5.3.1)$$

for $a, a' \in A$ and $b, b' \in B$.

Theorem 5.3.2. Let A and B be \mathbb{k} -algebras. Let V be a simple finite dimensional A -module, and W a simple finite dimensional B -module. Then $V \otimes_{\mathbb{k}} W$ is a simple $(A \otimes_{\mathbb{k}} B)$ -module. Further, any finite dimensional simple $(A \otimes_{\mathbb{k}} B)$ -module is of this form with V and W unique.

Proof. By the density theorem we have surjections $A \twoheadrightarrow \text{End } V$ and $B \twoheadrightarrow \text{End } W$. Thus, we have a surjection

$$A \otimes B \twoheadrightarrow \text{End } V \otimes \text{End } W \cong \text{End}(V \otimes W). \quad (5.3.3)$$

Thus, $V \otimes W$ must be simple, as any submodules would only arise as submodules of V and W .

Now suppose that U is a simple $(A \otimes B)$ -module, and let A' and B' denote the images of A and B in $\text{End } U$. Then A' and B' are finite dimensional, and we can assume without loss of generality that A and B are also finite dimensional. By [Claim 5.3.6](#) we have that

$$\text{Rad}(A \otimes B) = \text{Rad}(A) \otimes B + A \otimes \text{Rad}(B) \quad (5.3.4)$$

and thus, we have

$$(A \otimes B) / \text{Rad}(A \otimes B) = A / \text{Rad}(A) \otimes B / \text{Rad}(B). \quad (5.3.5)$$

Since all of the algebras in question are matrix algebras the assertion follows. \square

Claim 5.3.6 For \mathbb{k} -algebras A and B we have

$$\text{Rad}(A \otimes B) = \text{Rad}(A) \otimes B + A \otimes \text{Rad}(B). \quad (5.3.7)$$

Proof. Consider the simple module $V \otimes W$, where V is a simple A -module and W is a simple B -module. We know that if $a \otimes b \in \text{Rad}(A \otimes B)$ then $a \otimes b$ acts as zero on $V \otimes W$. We also know that if $v \otimes w \in V \otimes W$ then $a \otimes b$ acts as

$$(a \otimes b) \cdot (v \otimes w) = (a \cdot v) \otimes (b \cdot w). \quad (5.3.8)$$

If this is to vanish then it must be that either $a \cdot v = 0$ or $b \cdot w = 0$. Thus, $a \in \text{Rad } A$ or $b \in \text{Rad } B$, and so $a \otimes b \in \text{Rad } A \otimes B + A \otimes \text{Rad } B$. Conversely, clearly any element of this set acts trivially on $V \otimes W$, and thus we have containment the other way. \square

Six

Representation Theory of Finite Groups

Throughout this chapter G will be a finite group.

In this chapter we will look at representations of finite groups. We have already developed much of the required theory because group representations, $\rho : G \rightarrow \text{GL}(V)$, are in one-to-one correspondence with $\mathbb{k}G$ -modules. Note that we write G -module and $\text{Hom}_G(V, W)$ for $\mathbb{k}G$ -module and $\text{Hom}_{\mathbb{k}G}(V, W)$.

6.1 Maschke's Theorem

Theorem 6.1.1 — Maschke. Let $\text{char } \mathbb{k}$ be coprime to $|G|$. Then

1. $\mathbb{k}G$ is semisimple;
2. $\mathbb{k}G \cong \bigoplus_i \text{End } V_i$ with the isomorphism given on the basis by $g \mapsto \bigoplus_i \rho_i(g)$ where $\rho_i : G \rightarrow \text{GL}(V_i)$ are the irreducible representations of G .

Proof. We know that semisimplicity of $\mathbb{k}G$ implies that $\mathbb{k}G$ decomposes as in the second point (Proposition 4.2.34), so we need only show that $\mathbb{k}G$ is semisimple.

To prove that $\mathbb{k}G$ is semisimple it is sufficient to prove that given a G -module, V , and a G -submodule $W \subseteq V$ there is some G -submodule, W' such that $V = W \oplus W'$. This will show that any finite-dimensional $\mathbb{k}G$ -module is semisimple, and hence that $\mathbb{k}G$ is semisimple by Proposition 4.2.34.

Given a G -module, V , and a G -submodule, W , we always have as vector spaces some $\bar{W} \subseteq V$ such that $V = W \oplus \bar{W}$. We will construct from \bar{W} a G -submodule W' such that $V = W \oplus W'$.

Let $p : V \rightarrow W$ be projection onto the subspace W . That is, $p|_W = \text{id}_W$ and $p|_{\bar{W}} = 0$. We may define

$$P = \frac{1}{|G|} \sum_{g \in G} \rho(g) p \rho(g)^{-1} \quad (6.1.2)$$

where $\rho : G \rightarrow \text{GL}(V)$ is our representation map. Now consider $W' = \ker P$. We claim that W' is a submodule and $V = W \oplus W'$.

To verify these we need to show that $G \cdot W' \subseteq W'$ and that P is projection onto W . Suppose that $w \in W'$, that is $Pw = 0$. Then for $h \in G$ we have

$$P(h \cdot w) = P\rho(h)w \quad (6.1.3)$$

$$= \frac{1}{|G|} \sum_{g \in G} \rho(g)p\rho(g)^{-1}\rho(h)w \quad (6.1.4)$$

$$= \frac{1}{|G|} \sum_{g \in G} \rho(g)p\rho(g^{-1}h)w \quad (6.1.5)$$

$$= \frac{1}{|G|} \sum_{g' \in G} \rho(hg')p\rho(g'^{-1})w \quad (6.1.6)$$

$$= \rho(h) \frac{1}{|G|} \sum_{g' \in G} \rho(g')p\rho(g'^{-1})w \quad (6.1.7)$$

$$= \rho(h)Pw \quad (6.1.8)$$

$$= 0 \quad (6.1.9)$$

where we've reparametrised the sum using $g'^{-1} = g^{-1}h$, so $g' = h^{-1}g$ and $g = hg'$. This is a common trick when dealing with sums over group elements like this one. We have successfully shown that $h \cdot w \in \ker P$ if $w \in \ker P$, and thus $h \cdot w \in W'$.

We can now verify that P is a projection onto W . For this we have to show that $P|_W = \text{id}_W$, and $P(V) \subseteq W$, which combined imply that $P^2 = P$. For the first if $w \in W$ consider

$$Pw = \frac{1}{|G|} \sum_{g \in G} \rho(g)p\rho(g)^{-1}w. \quad (6.1.10)$$

Since W is a submodule we know that $\rho(g)^{-1}w \in W$, then since p is a projection onto W we know that $p\rho(g)^{-1}w = \rho(g)^{-1}w$, and thus $\rho(g)p\rho(g)^{-1}w = \rho(g)\rho(g)^{-1}w = w$. So, the sum reduces to

$$Pw = \frac{1}{|G|} \sum_{g \in G} w = \frac{|G|}{|G|} w = w. \quad (6.1.11)$$

Thus, $P|_W = \text{id}_W$ as claimed. Now we can show that $P(V) \subseteq W$. For $v \in V$ consider

$$Pv = \frac{1}{|G|} \sum_{g \in G} \rho(g)p\rho(g)^{-1}v. \quad (6.1.12)$$

By definition V is closed under the action of g , so $\rho(g)^{-1}v \in V$, then by definition $p\rho(g)^{-1}v \in W$, and since W is a submodule $\rho(g)p\rho(g)^{-1}v \in W$ for all $g \in G$. Submodules are closed under taking linear combinations, so $Pv \in W$. Thus, P is a projection onto W , and so we have the decomposition of vector spaces $V = W \oplus W'$, and we've already shown that W' is actually a submodule, so this is a decomposition of G -modules. \square

Corollary 6.1.13 We have

$$\mathbb{k}G \cong \bigoplus_i (\dim V_i) V_i \quad (6.1.14)$$

and

$$|G| = \sum_i (\dim V_i)^2. \quad (6.1.15)$$

Proof. This is simply Maschke's theorem applied to the regular representation, which is just G acting on itself by multiplication, where we've used $|G| = \dim \mathbb{k}G$. \square

The converse of Maschke's theorem holds also.

Proposition 6.1.16 If $\mathbb{k}G$ is semisimple then $\text{char } \mathbb{k}$ and $|G|$ are coprime.

Proof. By Maschke's theorem we can write

$$\mathbb{k}G \cong \bigoplus_{i=1}^r \text{End } V_i \quad (6.1.17)$$

where the V_i are simple G -modules and $V_1 = \mathbb{k}$ is the trivial representation. Then we have

$$\mathbb{k}G \cong \mathbb{k} \oplus \bigoplus_{i=2}^r \text{End } V_i \cong \mathbb{k} \oplus \bigoplus_{i=2}^r d_i V_i \quad (6.1.18)$$

with $d_i = \dim V_i$. Schur's lemma then tells us that every homomorphism of G -modules $\mathbb{k} \rightarrow \mathbb{k}G$ is a scalar multiple of some fixed homomorphism $\Lambda : \mathbb{k} \rightarrow \mathbb{k}G$, and every G -module homomorphism $\mathbb{k}G \rightarrow \mathbb{k}$ is a scalar multiple of some fixed homomorphism $\varepsilon : \mathbb{k}G \rightarrow \mathbb{k}$. More symbolically, the hom-spaces $\text{Hom}_{\mathbb{k}G}(\mathbb{k}, \mathbb{k}G)$ and $\text{Hom}_{\mathbb{k}G}(\mathbb{k}G, \mathbb{k})$ are one-dimensional with bases Λ and ε respectively, so are simply $\mathbb{k}\Lambda$ and $\mathbb{k}\varepsilon$. We are free to choose these maps to be such that $\varepsilon(g) = 1$ for all $g \in G$, and $\Lambda(1) = \sum_{g \in G} g$. Then we have

$$\varepsilon(\Lambda(1)) = \varepsilon\left(\sum_{g \in G} g\right) = \sum_{g \in G} \varepsilon(g) = \sum_{g \in G} 1 = |G|. \quad (6.1.19)$$

Now, if $|G| = kp$ where $p = \text{char } \mathbb{k}$ then $|G| = 0$ in $\mathbb{k}G$ and so this sum says that $\varepsilon \circ \Lambda(1) = 0$, which means that Λ has no left-inverse since $a\varepsilon \circ \Lambda(1) = 0$ for all $a \in \mathbb{k}$, which rules out all maps $\mathbb{k}G \rightarrow \mathbb{k}$ (since all are of the form $a\varepsilon$ for some $a \in \mathbb{k}$) as inverses for Λ , since these would have to give $a\varepsilon \circ \Lambda(1) = 1$. \square

Example 6.1.20 Consider $G = \mathbb{Z}/p\mathbb{Z}$, and \mathbb{k} a field of characteristic p . Clearly, $\text{char } \mathbb{k} = p$ and $|G| = p$ are not coprime. A consequence of this is that every simple $\mathbb{Z}/p\mathbb{Z}$ -module over \mathbb{k} is trivial. This follows because in a finite group of order p we have that $x^p = 1$, so $x^p - 1$ acts as zero, but over a field of characteristic p we have that $x^p - 1 = (x - 1)^p$, and thus $(x - 1)^p$ acts as zero, so $x - 1$ acts as 0 (as 0 is the only element of the group which doesn't act as 1 when raised to the power of p), so x must act as 1.

6.2 Group Characters

Definition 6.2.1 — Group Character Let G be a group and $\rho : G \rightarrow \text{GL}(V)$ a representation on a finite dimensional space, V . Then the **character** of V is the map

$$\chi_V : G \rightarrow \mathbb{k} \quad (6.2.2)$$

$$g \mapsto \chi_V(g) = \text{tr}_V(\rho(g)). \quad (6.2.3)$$

Of course, if $\tilde{\chi}_V : \mathbb{k}G \rightarrow \mathbb{k}$ is the character of the corresponding representation of the group algebra $\mathbb{k}G$ then $\chi_V = \tilde{\chi}_V|_G$, viewing G as a subset of $\mathbb{k}G$ in the canonical way (i.e., restricting to the canonical basis).

Definition 6.2.4 — Class Function Let G be a group. A **class function** of G is a map $f : G \rightarrow \mathbb{k}$ such that $f(g) = f(hgh^{-1})$ for all $g, h \in G$. We write

$$\mathcal{X}(G) = \{f : G \rightarrow \mathbb{k} \mid f(g) = f(hgh^{-1}) \forall g, h \in G\} \quad (6.2.5)$$

for the set of all class functions.

That is, class functions are functions which are invariant under conjugation of their argument. Another way of putting this, which explains the name, is that class functions are exactly those functions which are constant on each conjugacy class. Because of this we can identify

$$\mathcal{X}(G) \cong_{\text{Set}} \text{Func}(\mathcal{C}(G), \mathbb{k}) \quad (6.2.6)$$

where $\mathcal{C}(G)$ is the set of all conjugacy classes and

$$\text{Func}(A, B) = \{f : A \rightarrow B\} = \text{Set}(A, B). \quad (6.2.7)$$

Actually, under pointwise addition and scalar multiplication $\mathcal{X}(G)$ is a vector space. Further, under mild conditions the irreducible characters provide a basis for this space.

Theorem 6.2.8. If $\text{char } \mathbb{k}$ and $|G|$ are coprime then the irreducible characters, χ_{V_i} , of G form a basis for $\mathcal{X}(G)$.

Proof. From Maschke's theorem we know that $A = \mathbb{k}G$ is semisimple. We have proven that the irreducible algebra characters χ_{V_i} form a basis for $(A/[A, A])^*$. We then have

$$\begin{aligned} (A/[A, A])^* &= \{f \in \text{Hom}_{\mathbb{k}}(\mathbb{k}G, \mathbb{k}) \mid gh - hg \in \ker f \forall g, h \in G\} \\ &= \{f \in \text{Hom}_{\mathbb{k}}(\mathbb{k}G, \mathbb{k}) \mid f(gh) - f(hg) = 0 \forall g, h \in G\} \\ &= \{f \in \text{Hom}_{\mathbb{k}}(\mathbb{k}G, \mathbb{k}) \mid f(gh) = f(hg) \forall g, h \in G\} \\ &\cong_{\mathbb{k}\text{-Vect}} \{f \in \text{Func}(G, \mathbb{k}) \mid f(gh) = f(hg) \forall g, h \in G\} \\ &= \mathcal{X}(G). \end{aligned}$$

□

Corollary 6.2.9 The number of irreducible representations of G is equal to the number of conjugacy classes:

$$|\text{Irr}(G)| = |\mathcal{C}(G)|. \quad (6.2.10)$$

Example 6.2.11 Consider the symmetric group, $G = S_n$. Using cycle notation if we write every element as a product of disjoint cycles then two elements are in the same conjugacy class if and only if they have the same cycle type.

More concretely, take S_4 , then the cycle type of $(1\ 2\ 3\ 4)$ is (4) , the cycle type of $(1\ 2)(3\ 4)$ is $(2, 2)$, the cycle type of $(1\ 2\ 3)$ is $(3, 1)$ (note that $(1\ 2\ 3) = (1\ 2\ 3)(4)$, and we have to include all elements of $\{1, 2, 3, 4\}$). So, for example, $(1\ 2\ 3)$ and $(2\ 3\ 4)$ are conjugate, and so are $(1\ 2)(3\ 4)$ and $(1\ 3)(2\ 4)$.

We can identify conjugacy classes with cycle types, and we can identify cycle types with partitions of n . A **partition** of n being a tuple $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_k)$ such that $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_k \geq 0$ $\lambda_1 + \lambda_2 + \dots + \lambda_k = n$. We write $\lambda \vdash n$ to denote that λ is a partition of n .

A common, and useful notation, for partitions is that of **Young diagrams**. Here we take a partition, λ , and write a row of λ_i boxes in the i th row (rows counted from the top down). For example, $(1\ 2)(3\ 4)$ has cycle type $\lambda = (2, 2)$, and the corresponding Young diagram is

$$\lambda = \begin{array}{|c|c|} \hline \square & \square \\ \hline \square & \square \\ \hline \end{array}. \quad (6.2.12)$$

Similarly, $(1\ 2\ 3)$ has cycle type $\mu = (3, 1)$, and the corresponding Young diagram is

$$\mu = \begin{array}{|c|c|c|} \hline \square & \square & \square \\ \hline \square & & \\ \hline \end{array}. \quad (6.2.13)$$

So, we have a bijection between

- conjugacy classes of S_n ;
- partitions of n ;
- Young diagrams with n boxes.

It will turn out that Young diagrams, and the related Young tableaux, come up a lot when we start counting things related to the symmetric group. Later, we will explicitly define the irreducible representation, V_λ , of S_n corresponding to a partition $\lambda \vdash n$.

Note that if $\text{char } \mathbb{k}$ divides $|G|$ then $\mathbb{k}G$ is not generally semisimple and we typically have $|\mathcal{C}(G)| \geq |\text{Irr}(G)|$.

Corollary 6.2.14 For a field of characteristic 0 two G -modules, V and W , are isomorphic if and only if $\chi_V = \chi_W$.

Proof. Under these conditions $\mathbb{k}G$ is semisimple, and thus we can decompose both representations as

$$V = \bigoplus_i n_i V_i, \quad \text{and} \quad W = \bigoplus_i m_i V_i \quad (6.2.15)$$

where V_i are irreducible representations and $n_i, m_i \in \mathbb{Z}_{\geq 0}$. Then we have

$$\chi_V(g) = \text{tr}_V(\rho_V(g)) \quad (6.2.16)$$

$$= \text{tr}_{\bigoplus_i n_i V_i}(n_i \rho_{V_i}(g)) \quad (6.2.17)$$

$$= \sum_i n_i \text{tr}_{V_i}(\rho_{V_i}(g)) \quad (6.2.18)$$

$$= \sum_i n_i \chi_{V_i}(g) \quad (6.2.19)$$

and similarly

$$\chi_W(g) = \sum_i m_i \chi_{V_i}(g). \quad (6.2.20)$$

Since the characters are a basis we have equality between these only if $n_i = m_i$, and thus both representations have the same decomposition, so are isomorphic. \square

There is an isomorphism of vector spaces $\mathbb{k}G \cong_{\mathbb{k}\text{-Vect}} \text{Func}(G, \mathbb{k})$ on the basis by identifying g with δ_g for $g \in G$ where

$$\delta_g(h) = \delta_{g,h} = \begin{cases} 1 & g = h \\ 0 & g \neq h \end{cases} \quad (6.2.21)$$

is the **Kronecker delta**.

We can define the **convolution** product, $*$, on $\text{Func}(G, \mathbb{k})$ by

$$(\psi * \varphi)(g) = \sum_{h \in G} \psi(h) \varphi(h^{-1}g). \quad (6.2.22)$$

This product makes $\text{Func}(G, \mathbb{k})$ an algebra, and extends the above isomorphism to an isomorphism of algebras, $\mathbb{k}G \cong_{\mathbb{k}\text{-Alg}} \text{Func}(G, \mathbb{k})$, since

$$(\delta_g * \delta_h)(k) = \sum_{\ell \in G} \delta_g(\ell) \delta_h(\ell^{-1}k) \quad (6.2.23)$$

$$= \sum_{\ell \in G} \delta_{g,\ell} \delta_{h,\ell^{-1}k} \quad (6.2.24)$$

and terms in this sum vanish except for when $g = \ell$ and $h = \ell^{-1}k$, which means that $h = g^{-1}k$, or $k = gh$. So we only get a nonzero output if $k = gh$, which means that this convolution is exactly δ_{gh} , which is of course the same as taking the product of g and h in $\mathbb{k}G$ then mapping to $\text{Func}(G, \mathbb{k})$.

Proposition 6.2.25 Let

$$\mathbf{c} = \sum_{g \in c} g \quad (6.2.26)$$

where $c \in \mathcal{C}(G)$ is some conjugacy class. Then $Z(\mathbb{k}G) = \langle \mathbf{c} \mid C \in \mathcal{C}(G) \rangle$ and $Z(\mathbb{k}G) \cong \mathcal{X}(G)$.

Proof. We first show that for each conjugacy class, c , \mathbf{c} is in $Z(\mathbb{k}G)$. To do so we show that \mathbf{c} commutes with all elements of G , so taking $g \in G$ we have

$$cg = \sum_{h \in c} hg \quad (6.2.27)$$

$$= \sum_{h \in c} ghg^{-1}g \quad (6.2.28)$$

$$= \sum_{h \in c} gh \quad (6.2.29)$$

$$= g \sum_{h \in c} h \quad (6.2.30)$$

$$= g\mathbf{c}. \quad (6.2.31)$$

Here we've used the fact that conjugation by g is a permutation on c , and thus changing h to ghg^{-1} in the sum doesn't change the sum, it just permutes the terms.

The result follows from [Lemma 6.2.32](#) applied to the special case where $X = G$ with the action given by conjugation, in which case the invariant subspace is exactly the centre of $\mathbb{k}G$. \square

Lemma 6.2.32 Let G be a finite group acting on a finite set, X . The invariant subspace of the free vector space $\mathbb{k}X$ is spanned by elements of the form $\mathbf{o} = \sum_{x \in o} x$ where o ranges over all orbits of the group action.

Proof. Consider \mathbf{o} for some orbit, \mathbf{o} , we have

$$g \cdot \mathbf{o} = \sum_{x \in \mathbf{o}} g \cdot x = \mathbf{o}. \quad (6.2.33)$$

This follows since acting with g is just a permutation of the orbit, \mathbf{o} , and thus the sum is unchanged, it's just a permutation of the terms in the sum. Conversely, suppose that $v = \sum_{x \in X} v_x x$ is invariant under the action of G . Then we have

$$g \cdot v = \sum_{x \in X} v_x (g \cdot x) \quad (6.2.34)$$

and by invariance we demand that this is equal to

$$v = \sum_{x \in X} v_x x = \sum_{g^{-1} \cdot x \in X} v_{g^{-1} \cdot x} x, \quad (6.2.35)$$

so we can conclude that $v_x = v_{g^{-1} \cdot x}$ for all $g \in G$, and thus $v_x = v_y$ whenever x and y lie in the same orbit. Hence, v is a linear combination of the elements \mathbf{o} , and so the \mathbf{o} are a basis of the invariant subspace of $\mathbb{k}X$. \square

Example 6.2.36 — Finite Abelian Group Let G be a finite abelian group. Since G is abelian every element of G is in its own conjugacy class, so

$$|\text{Irr}(G)| = |\mathcal{C}(G)| = |G|. \quad (6.2.37)$$

By the structure theorem we know that

$$G \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k} \quad (6.2.38)$$

for some $n_i \in \mathbb{Z}_{\geq 0}$. Since G is abelian Schur's lemma tells us that all representations are one dimensional. Further, these irreducible representations form a group under pointwise multiplication:

$$(\rho_1 \cdot \rho_2)(g) = \rho_1(g)\rho_2(g). \quad (6.2.39)$$

The identity, ε , is the trivial representation, $\varepsilon(g) = 1$. The inverse of ρ is the representation $g \mapsto 1/\rho(g)$.

Each irreducible representation is a map $\rho: G \rightarrow \mathbb{k}^\times \cong \text{GL}(\mathbb{k})$. Thus, in this case the representations coincide with the characters.

We call the group $G^\vee := (\text{Irr}(G), \cdot)$ the **character group** or **dual group** of G .

Consider now $G = \mathbb{Z}_n$ and $\mathbb{k} = \mathbb{C}$. Then we have the irreducible representation

$$\rho: \mathbb{Z}_n \rightarrow \mathbb{C} \quad (6.2.40)$$

$$m \mapsto e^{2\pi i m/n} \quad (6.2.41)$$

and $\mathbb{Z}_n^\vee = \{\rho^k \mid k = 1, \dots, n\}$, which clearly gives an isomorphism $\mathbb{Z}_n^\vee \cong \mathbb{Z}_n$.

In fact, for any finite abelian group we have $G^\vee \cong G$, but not uniquely. However, we do have a canonical isomorphism $G \cong (G^\vee)^\vee$ given by $g \mapsto (\chi \mapsto \chi(g))$.

6.3 Dual Representations

Definition 6.3.1 — Dual Representation Let $\rho : G \rightarrow \text{GL}(V)$ be a representation of a finite group on a finite dimensional vector space. Then the dual space, V^* , gives rise to a representation, $\rho^* : G \rightarrow \text{GL}(V^*)$, with the on $f \in V^*$ given by

$$(g \cdot f)(v) = (\rho^*(g)f)(v) = f(\rho(g^{-1})v) \quad (6.3.2)$$

for all $v \in V$.

For $\mathbb{k} = \mathbb{C}$ we can further simplify this by identifying that $\rho^*(g) = \overline{\rho(g^{-1})}^\top$. That is, g acts on V^* by the Hermitian conjugate of the action of g^{-1} on V .

Lemma 6.3.3 We have $\chi_{V^*}(g) = \chi_V(g^{-1})$.

Proof. This follows from a direct calculation:

$$\chi_{V^*}(g) = \text{tr}_{V^*}(\rho^*(g)) \quad (6.3.4)$$

$$= \text{tr}_V(\rho(g^{-1})) \quad (6.3.5)$$

$$= \chi_V(g^{-1}). \quad \square$$

Note that $\chi_V(g) = \sum_i \lambda_i$ where λ_i are the eigenvalues of $\rho(g)$. We also know that for a finite group we have $\rho(g)^{|G|} = \rho(g^{|G|}) = \rho(e) = I$, and thus the eigenvalues of $\rho(g)$ must be roots of unity. For $\mathbb{k} = \mathbb{C}$ we have $\chi_{V^*}(g) = \sum_i \lambda_i^{-1} = \overline{\chi_V(g)}$, and thus $V \cong V^*$ as G -modules if and only if $\chi_V(g) \in \mathbb{R}$ for all $g \in G$.

6.4 Tensor Products of Representations

Definition 6.4.1 Let $\rho_V : G \rightarrow \text{GL}(V)$ and $\rho_W : G \rightarrow \text{GL}(W)$ be representations of G . Then there is a representation

$$\rho_V \otimes \rho_W : G \rightarrow \text{GL}(V) \otimes \text{GL}(W) \cong \text{GL}(V \otimes W) \quad (6.4.2)$$

given by

$$(\rho_V \otimes \rho_W)(g) = \rho_V(g) \otimes \rho_W(g). \quad (6.4.3)$$

Note that the character of a tensor product of representations is given by

$$\chi_{V \otimes W}(g) = \chi_V(g) \chi_W(g). \quad (6.4.4)$$

Example 6.4.5 — Schur–Weyl Duality Consider the group $G = \mathrm{GL}(V)$. Then $V^{\otimes n}$ carries a left G -module structure given on simple tensors by

$$g \cdot (v_{i_1} \otimes \cdots \otimes v_{i_n}) = (g \cdot v_{i_1} \otimes \cdots \otimes g \cdot v_{i_n}) \quad (6.4.6)$$

where $g \cdot v_{i_k}$ is the obvious action of $g \in \mathrm{GL}(V)$ on $v_{i_k} \in V$.

The space $V^{\otimes n}$ also naturally carries a right S_n -module action, given on simple tensors by

$$(v_{i_1} \otimes \cdots \otimes v_{i_n}) \cdot w = v_{i_{w(1)}} \otimes \cdots \otimes v_{i_{w(n)}}. \quad (6.4.7)$$

That is, $w \in S_n$ just permutes the terms in the tensor product.

These two actions are compatible, in a sense they “commute”, since it doesn’t matter if we act with $g \in \mathrm{GL}(V)$ on v_{i_k} then rearrange the order of the factors, or if we rearrange the order of the factors then act with g .

The result is that $V^{\otimes n}$ is a $(\mathrm{GL}(V), S_n)$ -bimodule.

6.5 Orthogonality of Characters

For this section we will work over $\mathbb{k} = \mathbb{C}$.

Lemma 6.5.1 Let G be a finite group. Then we may define a bilinear form

$$\langle -, - \rangle : \mathcal{X}(G) \times \mathcal{X}(G) \rightarrow \mathbb{C} \quad (6.5.2)$$

by

$$\langle \psi, \varphi \rangle := \frac{1}{|G|} \sum_{g \in G} \psi(g) \overline{\varphi(g)}. \quad (6.5.3)$$

This gives a well-defined Hermitian inner product on $\mathcal{X}(G)$.

Proof. Linearity in the first argument and conjugate linearity in the second follow because we defined the inner product as a sum over ψ and $\overline{\varphi}$. Conjugate symmetry is clear from the definition. This is positive definite, for $\psi \neq 0$ we have

$$\langle \psi, \psi \rangle = \frac{1}{|G|} \sum_{g \in G} \psi(g) \overline{\psi(g)} = \frac{1}{|G|} \sum_{g \in G} |\psi(g)|^2 \quad (6.5.4)$$

which is clearly a sum of non-negative terms and so is positive, since at least one term must be nonzero as $\psi \neq 0$. \square

Theorem 6.5.5. Let V and W be G -modules, then

$$\langle \chi_V, \chi_W \rangle = \dim(\mathrm{Hom}_G(V, W)). \quad (6.5.6)$$

In particular, if V and W are irreducible then

$$\langle \chi_V, \chi_W \rangle = \begin{cases} 1 & V \cong W, \\ 0 & \text{otherwise.} \end{cases} \quad (6.5.7)$$

Proof. By definition we have

$$\langle \chi_V, \chi_W \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_V(g) \overline{\chi_W(g)} \quad (6.5.8)$$

$$= \frac{1}{|G|} \sum_{g \in G} \chi_V(g) \chi_{W^*}(g) \quad (6.5.9)$$

$$= \frac{1}{|G|} \sum_{g \in G} \chi_{V \otimes W^*}(g) \quad (6.5.10)$$

$$= \frac{1}{|G|} \sum_{g \in G} \text{tr}_{V \otimes W^*}(\rho(g)) \quad (6.5.11)$$

$$= \text{tr}_{V \otimes W^*} \left(\frac{1}{|G|} \sum_{g \in G} \rho(g) \right). \quad (6.5.12)$$

Now, we can identify that

$$P = \frac{1}{|G|} \sum_{g \in G} g \in Z(\mathbb{C}G). \quad (6.5.13)$$

Thus, what we have above is $\text{tr}_{V \otimes W^*}(\rho(P))$.

If $X \in \text{Irr}(G)$ then

$$P|_X = \begin{cases} \text{id}_X & X \cong \mathbb{C}, \\ 0 & \text{otherwise.} \end{cases} \quad (6.5.14)$$

Thus, for any representation, X , $P|_X$ is projection onto X^G , the subspace fixed by the action of G . Hence,

$$\text{tr}_{V \otimes W^*}(\rho(P)) = \dim(\text{Hom}_G(\mathbb{C}, V \otimes W^*)) \quad (6.5.15)$$

$$= \dim(V \otimes W^*)^G \quad (6.5.16)$$

$$= \dim \text{Hom}_G(V, W) \quad (6.5.17)$$

having used the fact that $V \otimes W^* \cong \text{Hom}_{\mathbb{C}}(V, W)$ and $\text{Hom}_{\mathbb{C}}(V, W)^G \cong \text{Hom}_G(V, W)$. \square

Corollary 6.5.18 A G -module, V , is simple if and only if $\langle \chi_V, \chi_V \rangle = 1$.

Theorem 6.5.19. Let $g, h \in G$, then

$$\sum_{X \in \text{Irr}(G)} \chi_X(g) \overline{\chi_X(h)} = \begin{cases} |Z_g| & g \text{ conjugate to } h, \\ 0 & \text{otherwise,} \end{cases} \quad (6.5.20)$$

where $Z_g = \{h \in G \mid gh = hg\}$ is the centraliser of g in G .

Proof. We start with the following calculation:

$$\sum_{X \in \text{Irr}(G)} \chi_X(g) \overline{\chi_X(h)} = \sum_{X \in \text{Irr}(G)} \chi_X(g) \chi_{X^*}(h) \quad (6.5.21)$$

$$= \sum_{X \in \text{Irr}(G)} \text{tr}_X(\rho_X(g)) \text{tr}_{X^*}(\rho_{X^*}(h)) \quad (6.5.22)$$

$$= \text{tr}_{\bigoplus_{X \in \text{Irr}(G)} X \otimes X^*}(\rho_X(g) \otimes \rho_{X^*}(h)) \quad (6.5.23)$$

$$= \text{tr}_{\bigoplus_{X \in \text{Irr}(G)} X \otimes X^*}(\rho_X(g) \otimes \rho_X(h^{-1})) \quad (6.5.24)$$

$$= \text{tr}_{\bigoplus_{X \in \text{Irr}(G)} \text{End } X}(x \mapsto \rho(g)x\rho(h^{-1})) \quad (6.5.25)$$

$$= \text{tr}_{\mathbb{C}G}(y \mapsto gyh^{-1}). \quad (6.5.26)$$

Here we've used the fact that $X \otimes X^* \cong \text{End } X$, with the isomorphism given by $A \otimes B \mapsto (x \mapsto Ax B^*)$. We've then used the fact that

$$\mathbb{C}G \cong \bigoplus_{X \in \text{Irr}(G)} \text{End } X, \quad (6.5.27)$$

since $\mathbb{C}G$ is semisimple.

We now consider cases, the first being when g and h are not conjugate. Suppose that g_i generate G . Then $gg_i h^{-1} \neq g_i$. Thus, the map $y \mapsto gyh^{-1}$, viewed as a matrix, has no on-diagonal elements, and so has vanishing trace.

If instead g and h are conjugate then using the fact that characters are class functions and applying the same logic as above we have

$$\sum_{X \in \text{Irr}(G)} \chi_X(g) \overline{\chi_X(h)} = \sum_{X \in \text{Irr}(G)} \chi_X(g) \overline{\chi_X(g)} \quad (6.5.28)$$

$$= \text{tr}_{\mathbb{C}G}(y \mapsto gyg^{-1}). \quad (6.5.29)$$

Further, viewing $y \mapsto gyg^{-1}$ as a matrix we can see that the (y, y) component on the diagonal is 1 precisely if $yg = gy$, and 0 otherwise. That is, there are precisely as many 1s on the diagonal as elements of Z_g , and so $\text{tr}_{\mathbb{C}G}(y \mapsto gyg^{-1}) = |Z_g|$. \square

6.5.1 Unitary Representations

Definition 6.5.30 — Unitary Representation Let G be a group and consider a complex vector space, V , equipped with an inner product, $\langle -, - \rangle$. We say that the representation $\rho : G \rightarrow \text{GL}(V)$ is **unitary** if $\rho(g)$ is a unitary operator, that is, if

$$\langle \rho(g)v, \rho(g)w \rangle = \langle v, w \rangle \quad (6.5.31)$$

for all $g \in G$ and $v, w \in V$.

Alternatively, a **unitary representation** of G is a homomorphism $\rho : G \rightarrow \text{U}(V) \subseteq \text{GL}(V)$ where

$$\text{U}(V) = \{ \varphi \in \text{GL}(V) \mid \langle \varphi(v), \varphi(u) \rangle = \langle v, u \rangle \} \quad (6.5.32)$$

is the **unitary group**.

Unitary representations are particularly important in quantum mechanics. The idea is that V is a state space, that is V is the space of possible wave functions, ψ (or $|\psi\rangle$). As is standard we restrict to normalised wavefunctions. To each quantity we may want to measure we associate some element of V^* , which we write as $\langle \varphi |$ if the corresponding element of V is $|\varphi\rangle$ (note that there is a canonical isomorphism $V \cong V^*$ because we have the inner product (Riesz representation theorem)). Then the probability of being measured to be in the state $|\varphi\rangle$ when in the state $|\psi\rangle$ is $\langle \varphi | \psi \rangle = \langle \varphi, \psi \rangle$.

A unitary representation, $\rho : G \rightarrow \text{U}(V)$, is then interpreted as a symmetry of our system, since the probabilities that we measure are unaffected by this action.

Consider a complex vector space, V . Note that $V \otimes V$ inherits the inner product $\langle u_1 \otimes v_1, u_2 \otimes v_2 \rangle_{V \otimes V} = \langle u_1, v_1 \rangle_V \langle u_2, v_2 \rangle_V$. Without further knowledge of V there are two unitary representations of S_2 on $V \otimes V$, they are $u \otimes v \mapsto v \otimes u$ and $u \otimes v \mapsto -v \otimes u$.

The physical interpretation of this is that if V is the state space of a single particle then $V \otimes V$ is the state space of two identical particles. The two options for S_2 actions then correspond to the two fundamental types of particles. If $u \otimes v \mapsto v \otimes u$ we call the particles **bosons**, and if $u \otimes v \mapsto -v \otimes u$ we call the particles **fermions**.

It turns out that if we're given a finite dimensional complex representation, $\rho : G \rightarrow \text{GL}(V)$, of a *finite* group we can always construct a new inner product on V such that this is a unitary representation.

Theorem 6.5.33. Let G be a finite group and V a complex finite-dimensional inner product space with inner product $\langle -, - \rangle$. Let $\rho : G \rightarrow \text{GL}(V)$ be a representation of G . Then there exists an inner product, $(-, -)$, on V with respect to which ρ gives a unitary representation.

Proof. We define an inner product on V by

$$(u, v) = \sum_{g \in G} \langle \rho(g)u, \rho(g)v \rangle. \quad (6.5.34)$$

That this is linear follows from the fact that the action of G is linear and

$\langle -, - \rangle$ is linear. The fact that this is positive definite follows because each term in the sum is nonnegative, and for $u \neq v$ we must have $\rho(g)u \neq \rho(g)v$ since $\rho(g)$ is invertible, and thus $\langle \rho(g)u, \rho(g)v \rangle \neq 0$ for $u \neq v$.

That this new inner product is invariant under the action of G follows from a simple calculation:

$$\langle \rho(g)u, \rho(g)v \rangle = \sum_{h \in G} \langle \rho(h)\rho(g)u, \rho(h)\rho(g)v \rangle \quad (6.5.35)$$

$$= \sum_{h \in G} \langle \rho(hg)u, \rho(hg)v \rangle \quad (6.5.36)$$

$$= \sum_{k \in G} \langle \rho(k)u, \rho(k)v \rangle \quad (6.5.37)$$

$$= \langle u, v \rangle, \quad (6.5.38)$$

where we've reindexed the sum with $k = hg$. \square

Another nice property of unitary representations is that since they respect the inner product we get all of the structure of vector spaces that comes with it, including the splitting of short exact sequences, which is just a fancy way of saying that given a vector space, V , with subspace $W \subseteq V$ we always have the orthogonal complement, $W' = \{w' \in V \mid \langle w, w' \rangle = 0 \forall w \in W\}$, which is such that $V \cong W \oplus W'$.

Theorem 6.5.39. Any finite dimensional unitary representation of any group is completely reducible.

Proof. Let V be a finite dimensional unitary representation of a group, G . If V is irreducible we are done. Else, let $W \subseteq V$ be a subrepresentation. Then $W' = \{w' \in V \mid \langle w, w' \rangle = 0\}$ is a subrepresentation also since if $w' \in W'$ then $\rho(g)w' \in W'$ because for any $w \in W'$ we have $\langle w, \rho(g)w' \rangle = \langle \rho(g)\tilde{w}, \rho(g)w' \rangle = \langle \tilde{w}, w' \rangle = 0$ where $\tilde{w} = \rho(g)^{-1}w$ is an element of W because W is closed under the action of g^{-1} . Thus, W and W' are subrepresentations, and as vector spaces we know that $V \cong W \oplus W'$. If either of W or W' is not irreducible we may iterate this process. Eventually this process will terminate as at each iteration the dimensions of the new spaces are lower than the dimension of the original space, and we started with a finite dimensional space. \square

Seven

Applications of Characters

7.1 Computing Tensor Products

Suppose we have simple G -modules, V and W . Then the tensor product $V \otimes W$ is again a G -module with the action $g \cdot (v \otimes w) = (g \cdot v) \otimes (g \cdot w)$. Assuming that $\mathbb{k}G$ is semisimple (so $\text{char } \mathbb{k}$ and $|G|$ are coprime) we can decompose $V \otimes W$ as a direct sum of simple G -modules:

$$V \otimes W = \bigoplus_{U \in \text{Irr}(G)} N_{VW}^U U. \quad (7.1.1)$$

Here the coefficients, N_{VW}^U , are just the multiplicities of U in this decomposition. These are nonnegative integer values.

We can compute the coefficients, N_{VW}^U , using characters. First, note that the character of $V \otimes W$ is $\chi_{V \otimes W} = \chi_V \chi_W$ and using the above decomposition we have

$$\chi_{V \otimes W} = \sum_{U \in \text{Irr}(G)} N_{VW}^U \chi_U. \quad (7.1.2)$$

Taking inner products on both sides and using the orthogonality of irreducible characters we have

$$\langle \chi_{V \otimes W}, \chi_U \rangle = \left\langle \sum_{U' \in \text{Irr}(G)} N_{VW}^{U'} \chi_{U'}, \chi_U \right\rangle \quad (7.1.3)$$

$$= \sum_{U' \in \text{Irr}(G)} N_{VW}^{U'} \langle \chi_{U'}, \chi_U \rangle \quad (7.1.4)$$

$$= \sum_{U' \in \text{Irr}(G)} N_{VW}^{U'} \delta_{U'U} \quad (7.1.5)$$

$$= N_{VW}^U. \quad (7.1.6)$$

Here $\delta_{U'U} = 0$ if $U' \not\cong U$ and $\delta_{U'U} = 1$ if $U' \cong U$ as G -modules. So, by computing characters we can completely determine the decomposition of $V \otimes W$ into irreducibles, and since this decomposition is unique (up to order and isomorphism) we have completely determined $V \otimes W$.

7.2 Frobenius–Schur Indicator

7.2.1 Bilinear Forms and Dual Spaces

Suppose V is a finite dimensional vector space over \mathbb{k} . Then we know that $V \cong V^*$, but there is no canonical choice of isomorphism. If we fix some isomorphism

$\delta : V \rightarrow V^*$ then we can define a nondegenerate bilinear form $\langle -, - \rangle_\delta : V \times V \rightarrow \mathbb{k}$ by

$$\langle u, v \rangle_\delta = \delta(u)(v). \quad (7.2.1)$$

Conversely, if we have a nondegenerate bilinear form $\langle -, - \rangle : V \times V \rightarrow \mathbb{k}$ then we may define an isomorphism $\varphi : V \rightarrow V^*$ by $u \mapsto \varphi_u$ where $\varphi_u(v) = \langle u, v \rangle$.

However, this doesn't *quite* determine a *unique* isomorphism, because we made the arbitrary choice to define $\varphi_u(v)$ to be $\langle u, v \rangle$, rather than $\langle v, u \rangle$. To fix this we can just assume that $\langle -, - \rangle$ is not just a bilinear form, but either a symmetric or antisymmetric bilinear form. Then φ is uniquely determined for symmetry, or determined up to a sign for antisymmetry. We can always construct a symmetric bilinear form by symmetrising, if $\langle -, - \rangle$ has no specific symmetry then $\langle u, v \rangle = [\langle u, v \rangle \pm \langle v, u \rangle]/2$ is symmetric for $+$ and antisymmetric for $-$.

This analysis also carries over from the theory of vector spaces to a G -module, M . The dual, M^* , is a G -module with the action defined by $g \cdot f(v) = f(g^{-1} \cdot v)$. The only subtlety being that to get a left action we use g^{-1} in the action. The only change we need to make is that the nondegenerate (anti)symmetric bilinear form needs to be invariant under the action of G . That is, we should have $\langle g \cdot u, g \cdot v \rangle = \langle u, v \rangle$ for all $u, v \in M$. For example, if M is equipped with an inner product then G should act unitarily on M . Thus, if $\langle -, - \rangle$ is a symmetric G -invariant bilinear form on M then we may define an isomorphism $\varphi : M \rightarrow M^*$ by $u \mapsto \varphi_u$ where $\varphi_u(v) = \langle u, v \rangle$. This is an isomorphism of vector spaces, and it's an isomorphism of G -modules because

$$\varphi(g \cdot u)(v) = \varphi_{g \cdot u}(v) = \langle g \cdot u, v \rangle \quad (7.2.2)$$

and

$$(g \cdot \varphi(u))(v) = (g \cdot \varphi_u)(v) = \varphi_u(g^{-1} \cdot v) = \langle u, g^{-1} \cdot v \rangle. \quad (7.2.3)$$

These are equal, to see this simply act on the arguments of the first with g^{-1} , which doesn't change anything as $\langle -, - \rangle$ is G -invariant, and we get

$$\langle g \cdot u, v \rangle = \langle g^{-1} \cdot (g \cdot u), g^{-1} \cdot v \rangle = \langle g^{-1} g \cdot u, g^{-1} \cdot v \rangle = \langle u, g^{-1} \cdot v \rangle. \quad (7.2.4)$$

The question then becomes when does a given G -module, M , admit such a nondegenerate (anti)symmetric invariant bilinear form? There are three possibilities, which we classify as follows.

Definition 7.2.5 Let G be a finite group and M a G -module. We say that M is of

- (-1) **complex type** if $M^* \not\cong M$ as G -modules;
- (0) **real type** if M admits a nondegenerate symmetric invariant bilinear form;
- (1) **quaternionic type** if M admits a nondegenerate antisymmetric invariant bilinear form.

This naming convention comes from considering $\text{End}_{\mathbb{R}G} M$, for a simple G -module, M , over \mathbb{R} . This is the space of linear maps $M \rightarrow M$ which commute

with the action of *real* linear combinations of group elements. It turns out that $\text{End}_{\mathbb{R}G} M$ is isomorphic to one of \mathbb{R} , \mathbb{C} , or \mathbb{H} , precisely when M is of real, complex, or quaternionic type.

If instead we consider M to be a simple G -module over $\text{Mat}_{2 \times 2}(\mathbb{C})$ then $\text{End}_{\mathbb{C}G} M$ is isomorphic to one of \mathbb{C} , $\mathbb{C} \times \mathbb{C}$, or \mathbb{C} when M is of real, complex, or quaternionic type. Note that these endomorphism rings over \mathbb{C} are the result of applying the extension of scalars functor, $- \otimes_{\mathbb{R}} \mathbb{C}$, to the endomorphism rings over \mathbb{R} .

7.2.2 The Frobenius–Schur Indicator

Definition 7.2.6 — Frobenius–Schur Indicator Let G be a finite group and M a simple G -module. The **Frobenius–Schur indicator** is defined to be

$$\text{FS}(M) := \frac{1}{|G|} \sum_{g \in G} \chi_M(g^2) \quad (7.2.7)$$

where χ_M is the character of M .

Theorem 7.2.8 — Frobenius–Schur. Let G be a finite group. Then the number of involutions in G , that is, the number of elements of order at most 2, is precisely

$$\sum_{M \in \text{Irr}(G)} \dim(M) \text{FS}(M). \quad (7.2.9)$$

Proof. Consider some representation, M , and some $A \in \text{End}_{\mathbb{C}G} M$. Let $\lambda_1, \dots, \lambda_n$ be the eigenvalues of A . We consider $S^2 M$ and $\Lambda^2 M$. These spaces are both formed as quotients of $M \otimes M$ by the ideal generated by $v \otimes w \pm w \otimes v$. Since A acts on $M \otimes M$ as $A \otimes A$ and this action factors through the quotient $A \otimes A$ acts on both of these spaces. We have that

$$\text{tr}_{S^2 M}(A \otimes A) = \sum_{1 \leq i < j \leq n} \lambda_i \lambda_j. \quad (7.2.10)$$

This holds for diagonal matrices when \otimes is the Kronecker product, which is defined by $A \otimes B = (a_{ij} B)$ and so for a diagonal matrix the diagonal is just all products $\lambda_i \lambda_j$. Since the trace is invariant under a basis change this result must also hold for diagonalisable matrices. Finally, it holds for all matrices by continuity because the diagonalisable matrices are dense in all matrices. Similarly, we have

$$\text{tr}_{\Lambda^2 M}(A \otimes A) = \sum_{1 \leq i < j \leq n} \lambda_i \lambda_j, \quad (7.2.11)$$

which again, clearly holds for diagonal matrices with the antisymmetrised Kronecker product, since there $\lambda_i^2 = 0$. Thus, we have

$$\text{tr}_{S^2 M}(A \otimes A) - \text{tr}_{\Lambda^2 M}(A \otimes A) = \sum_{1 \leq i \leq n} \lambda_i^2 = \text{tr}_M A^2. \quad (7.2.12)$$

Thus, for $g \in G$, we can take A to be the corresponding action of g and we get

$$\chi_M(g^2) = \chi_{S^2M}(g) - \chi_{\Lambda^2M}(g). \quad (7.2.13)$$

Note that g is *not* squared on the right because by definition of S^2M and Λ^2M g acts as $g \otimes g$ does on $M \otimes M$, so the squaring is automatic in the definition of the action.

Then summing this result over G and dividing by $|G|$ we get

$$\frac{1}{|G|} \sum_{g \in G} \chi_M(g^2) = \frac{1}{|G|} \sum_{g \in G} \chi_{S^2M}(g) - \frac{1}{|G|} \sum_{g \in G} \chi_{\Lambda^2M}(g). \quad (7.2.14)$$

The left hand side is exactly $\text{FS}(M)$. We have the following vector space decomposition into symmetric and antisymmetric parts:

$$M \otimes M \cong S^2M \oplus \Lambda^2M. \quad (7.2.15)$$

In the finite-dimensional case we also have

$$M \otimes M \cong M \otimes M^* \cong \text{End}_{\mathbb{C}} M. \quad (7.2.16)$$

Thus, we have

$$S^2M \oplus \Lambda^2M \cong \text{End}_{\mathbb{C}} M \quad (7.2.17)$$

as vector spaces. Denote by X^G the fixed points of the action of G on X , that is, $X^G = \{x \in X \mid g \cdot x = x\}$. This clearly distributes over direct sums, and we have

$$(S^2M)^G \oplus (\Lambda^2M)^G \cong (\text{End}_{\mathbb{C}} M)^G = \text{End}_{\mathbb{C}G} M \quad (7.2.18)$$

where we have identified in the last equality that an endomorphism is fixed under the action of G precisely if it commutes with the action of G . Taking dimensions we have

$$\dim(S^2M)^G + \dim(\Lambda^2M)^G = \dim(\text{End}_{\mathbb{C}G} M). \quad (7.2.19)$$

Since M is simple we know that any G -module endomorphism of M is just scalar multiplication, and thus $\dim(\text{End}_{\mathbb{C}G} M) \leq 1$. Since dimensions are integers this leaves us with just two options on the right, either both dimensions are 0, or one is 0 and the other is 1. Thus,

$$\dim(S^2M)^G - \dim(\Lambda^2M)^G \in \{-1, 0, 1\}. \quad (7.2.20)$$

Note that the above quantity is the correct way to generalise the Frobenius-Schur indicator to fields other than \mathbb{C} .

Let I be the number of involutions of G . Then

$$I = \sum_{g \in G} [g^2 = 1] \quad (7.2.21)$$

where $[\varphi]$ is the Iverson bracket, $[\varphi] = 1$ if φ is true, and $[\varphi] = 0$ if φ is false. The second orthogonality relation (Theorem 6.5.19) tells us that

$$[g^2 = 1] = \frac{1}{|G|} \sum_{M \in \text{Irr}(G)} \chi_M(g^2) \overline{\chi_M(1)}, \quad (7.2.22)$$

since this result should vanish if g^2 is not conjugate to 1 and should be $|Z_g|$ otherwise. Then we note that g^2 is conjugate to the identity if and only if g^2 is the identity. Further, $|Z_g| = |G|$ if $g^2 = 1$. Thus, we have that

$$I = \frac{1}{|G|} \sum_{g \in G} \sum_{M \in \text{Irr}(G)} \chi_M(g^2) \overline{\chi_M(1)}. \quad (7.2.23)$$

Since $\chi_M(1) = \dim M$ this simplifies to

$$I = \frac{1}{|G|} \sum_{g \in G} \sum_{M \in \text{Irr}(G)} \dim(M) \chi_M(g^2) = \sum_{M \in \text{Irr}(G)} \dim(M) \text{FS}(M). \quad (7.2.24)$$

□

The proof of the following result is some fairly involved linear algebra, but essentially comes down to the universal property of the tensor/symmetric/exterior product giving a correspondence between bilinear forms and linear maps, and the bilinear forms inherit the (anti)symmetry of the symmetric/exterior product.

Proposition 7.2.25 Let G be a finite group, and M a simple G -module. Then $\text{FS}(M)$ is -1 if M is of complex type, 0 if M is of real type, and 1 if M is of quaternionic type.

Example 7.2.26 This example assumes some knowledge about the basics of representations of S_n , a topic we have yet to cover, so maybe come back later if you're not familiar with these ideas.

It is a fact that $\text{FS}(M) = 1$ for any simple S_n -module, that is, all S_n -modules are of real type. Simple S_n -modules are indexed by standard tableaux of shape λ with λ a partition of n . Thus, the number of involutions in S_n is precisely

$$\sum_{\lambda \vdash n} |\text{SYT}(\lambda)| \quad (7.2.27)$$

where $\text{SYT}(\lambda)$ is the set of standard Young tableau of shape λ .

7.3 Burnside's Theorem

7.3.1 Statement of Theorem

The next example of an application of character theory is Burnside's theorem, a result in number theory. While Burnside's theorem is relatively easy to state its

proof requires some number theory. The result is famous for being one of the first results in group theory which was first proven through representation theory.

Before we state the theorem recall the following definition from group theory.

Definition 7.3.1 — Solvable Group A group, G , is **solvable** if there exists a series of nested normal subgroups

$$\{1\} = G_1 \triangleleft G_2 \triangleleft \cdots \triangleleft G_n = G \quad (7.3.2)$$

such that G_{i+1}/G_i is abelian.

Theorem — Burnside's Theorem. Any group, G , of order $p^a q^b$ with p and q primes and $a, b \in \mathbb{Z}_{\geq 0}$ is solvable.

7.3.2 Algebraic Integers

Definition 7.3.3 — Algebraic Integers A complex number, $z \in \mathbb{C}$, is an

- **algebraic number** if it is a root of some polynomial in $\mathbb{Q}[x]$;
- **algebraic integer** if it is a root of some *monic*^a polynomial in $\mathbb{Z}[x]$.

We write $\overline{\mathbb{Q}}$ and $\overline{\mathbb{Z}}$ for the sets of algebraic numbers and integers respectively.

^aRecall that a polynomial is **monic** if the coefficient of the highest degree term is 1.

Example 7.3.4

- $\mathbb{Z} \subseteq \overline{\mathbb{Z}}$: $n \in \mathbb{Z}$ is a root of $x - n$.
- $\mathbb{Q} \cap \overline{\mathbb{Z}} = \mathbb{Z}$: Suppose a/b is rational and reduced, then any rational polynomial with a/b as a root has a factor of $x - a/b$, to get an integer polynomial we have to scale this to $bx - a$. Thus, any integer polynomial with a/b as a root has a factor of $bx - a$, which means it cannot be monic, since any monic polynomial factors as $(x - \alpha_1) \cdots (x - \alpha_m)$ for some roots $\alpha_i \in \mathbb{C}$. Thus, a/b is an algebraic integer only if $b = 1$, in which case $a/b = a$ is an integer.

Lemma 7.3.5 $z \in \mathbb{C}$ is an algebraic number (integer) if and only if it is an eigenvalue of some $n \times n$ matrix over \mathbb{Q} (\mathbb{Z}).

Proof. If z is an algebraic number (integer) then it is a root of the monic polynomial

$$p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \quad (7.3.6)$$

where $a_i \in \mathbb{Q}$ ($a_i \in \mathbb{Z}$). Note that we are always free to rescale a rational polynomial to be monic. Let

$$A = \begin{pmatrix} 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & \dots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & -a_{n-1} \end{pmatrix}. \quad (7.3.7)$$

Then the characteristic polynomial of A is

$$-\det(A - xI) = p(x), \quad (7.3.8)$$

and thus z is an eigenvalue of A .

Conversely, suppose that z is an eigenvalue of some $n \times n$ rational (integer) matrix, A . Then z is a root of the characteristic polynomial of A . The characteristic polynomial of a matrix over \mathbb{Q} (\mathbb{Z}) is always monic over \mathbb{Q} (\mathbb{Z}), and thus z is an algebraic number (integer). \square

Proposition 7.3.9

- $\overline{\mathbb{Z}}$ is a ring; and
- $\overline{\mathbb{Q}}$ is a field.

Proof. STEP 1: $\overline{\mathbb{Q}}$ AND $\overline{\mathbb{Z}}$ ARE RINGS

We will prove that $\overline{\mathbb{Q}}$ is a ring, the proof for $\overline{\mathbb{Z}}$ is analogous. Take $\alpha, \beta \in \overline{\mathbb{Q}}$, then there are matrices $A \in \text{Mat}_m(\mathbb{Q})$ and $B \in \text{Mat}_n(\mathbb{Q})$ such that α and β are eigenvalues of A and B respectively. Let $v \in \mathbb{C}^m$ and $w \in \mathbb{C}^n$ be the corresponding eigenvectors. Consider $A \otimes \text{id}_{\mathbb{C}^n} \pm \text{id}_{\mathbb{C}^m} \otimes B$. A calculation shows that $v \otimes w$ is an eigenvector of this matrix with eigenvalue $\alpha \pm \beta$:

$$(A \otimes \text{id}_{\mathbb{C}^n} \pm \text{id}_{\mathbb{C}^m} \otimes B)(v \otimes w) \quad (7.3.10)$$

$$= (A \otimes \text{id}_{\mathbb{C}^n})(v \otimes w) \pm (\text{id}_{\mathbb{C}^m} \otimes B)(v \otimes w) \quad (7.3.11)$$

$$= Av \otimes w \pm v \otimes Bw \quad (7.3.12)$$

$$= \alpha v \otimes w \pm v \otimes \beta w \quad (7.3.13)$$

$$= (\alpha \pm \beta)(v \otimes w). \quad (7.3.14)$$

Thus, $\alpha \pm \beta$ is an eigenvalue of some $(m+n) \times (m+n)$ matrix over \mathbb{Q} , and hence $\alpha \pm \beta \in \overline{\mathbb{Q}}$.

Similarly, $\alpha\beta$ is an eigenvalue of $A \otimes B$ with eigenvector $v \otimes w$:

$$(A \otimes B)(v \otimes w) = Av \otimes Bw = \alpha v \otimes \beta w = (\alpha\beta)(v \otimes w). \quad (7.3.15)$$

Thus, $\alpha\beta$ is an eigenvalue of some $mn \times mn$ matrix over \mathbb{Q} , and so $\alpha\beta \in \overline{\mathbb{Q}}$. These results, along with the inherited distributivity law from \mathbb{C} , prove that $\overline{\mathbb{Q}}$ is a ring.

STEP 2: $\overline{\mathbb{Q}}$ IS A FIELD

Suppose that $\alpha \in \overline{\mathbb{Q}} \setminus \{0\}$. Then there exists some matrix, $A \in \text{Mat}_{m \times m}(\mathbb{Q})$ such that α is a root of $p(x) = \det(A - xI)$. We can multiply this whole equation by α^m and it follows from properties of determinants that $\alpha^m p(x) = \det(\alpha A - \alpha x I)$. Then, $\alpha^m p(1/\alpha) = \det(\alpha A - I)$, which vanishes when αA has eigenvalue 1, and since αA has the same eigenvalues as A but multiplied by α this shows that some eigenvalue, β , is such that $\alpha\beta = 1$, in other words, $\beta = 1/\alpha$, so $1/\alpha \in \overline{\mathbb{Q}}$. Thus, $\overline{\mathbb{Q}}$ contains multiplicative inverses of nonzero elements, and so is a field (it is clearly commutative and has no zero divisors as it is a subring of \mathbb{C}). \square

7.3.3 Towards a Proof of Burnside's Theorem

Many quantities that arise in representation theory are naturally algebraic integers. We will use this to restrict the possible values that certain quantities can take, which will be important in our proof of Burnside's theorem.

Lemma 7.3.16 Let G be a finite group and M a finite-dimensional G -module. Then $\chi_M(g)$ is an algebraic integer for every $g \in G$.

Proof. Since G is finite each $g \in G$ has finite order, n , and thus the eigenvalues of $\rho_M(g)$ are n th roots of unity, and so in $\overline{\mathbb{Z}}$ as they satisfy the monic polynomial $x^n - 1 = 0$. The trace is the sum of the eigenvalues, and $\overline{\mathbb{Z}}$ is a ring, so is closed under addition, and thus $\chi_M(g) \in \overline{\mathbb{Z}}$. \square

Proposition 7.3.17 Let G be a finite group and consider the set of conjugacy classes, $\mathcal{C}(G) = \{[g_1], \dots, [g_n]\}$, with chosen representatives. Define

$$c_i = \sum_{g \in [g_i]} g \in \mathbb{C}G, \quad (7.3.18)$$

then for any simple G -module, M , we have $c_i|_M = \lambda_i \text{id}_M$ where

$$\lambda_i = |[g_i]| \frac{\chi_M(g_i)}{\chi_M(1)} \quad (7.3.19)$$

are algebraic integers.

Proof. First note that the c_i are central in $\mathbb{C}G$ since

$$c_i g = \sum_{g' \in [g_i]} g' g = \sum_{g'' \in [g_i]} g g'' = g \sum_{g'' \in [g_i]} g'' = g c_i \quad (7.3.20)$$

where we've reindexed the sum with $g'' = g^{-1}g'g$, which doesn't change the value as we're still summing over the whole conjugacy class, just in a different order.

Thus, by Schur's lemma we know that the c_i act as a scalar on any simple G -module. Call this scalar λ_i . Consider the group ring, $\mathbb{Z}G$. This is finitely generated (since G is a finite generating set). Thus, each c_i must satisfy

some monic integer polynomial equation, and this carries through to the scalars, λ_i , which shows they are algebraic integers. Viewing c_i as an operator on M we know that $c_i = \lambda_i \text{id}_M$, and we can take the trace of this to get

$$\text{tr}_M c_i = \text{tr}_M(\lambda_i \text{id}_M) = \lambda_i \dim M = \lambda_i \chi_M(1). \quad (7.3.21)$$

We also have

$$\text{tr}_M c_i = \sum_{g \in [g_i]} \text{tr}_M \rho_M(g) = \sum_{g \in [g_i]} \chi_M(g) = |[g_i]| \chi_M(g_i) \quad (7.3.22)$$

since the character is constant on conjugacy classes. Equating these we get the desired result. \square

Theorem 7.3.23 — Frobenius Divisibility. Let G be a finite group and M a simple G -module over \mathbb{C} . Then $\dim M$ divides $|G|$.

Proof. With notation as in the statement of [Proposition 7.3.17](#) we claim that

$$\sum_i \lambda_i \overline{\chi_M(g_i)} \in \overline{\mathbb{Z}} \quad (7.3.24)$$

where the sum is over all conjugacy classes. Since $\overline{\mathbb{Z}}$ is a ring and [Proposition 7.3.17](#) shows that the λ_i are algebraic integers it is sufficient to show that $\overline{\chi_M(g_i)}$ are algebraic integers. Since G is finite we know that $\rho_M(g_i)^{|G|} = \text{id}_M$, and hence $\chi_M(g_i)$ must be sums of roots of unity, which are algebraic integers, so $\chi_M(g_i)$ are algebraic integers, and hence $\overline{\chi_M(g_i)}$ are algebraic integers, as they are roots of the conjugate polynomial.

From [Proposition 7.3.17](#) we also have

$$\sum_i \lambda_i \overline{\chi_M(g_i)} = \sum_i |[g_i]| \frac{\chi_M(g_i) \overline{\chi_M(g_i)}}{\chi_M(1)} \quad (7.3.25)$$

$$= \sum_{g \in G} \frac{\chi_M(g) \overline{\chi_M(g)}}{\dim M} \quad (7.3.26)$$

$$= \frac{|G|}{\dim M} \langle \chi_M, \chi_M \rangle \quad (7.3.27)$$

$$= \frac{|G|}{\dim M}. \quad (7.3.28)$$

This shows that this quantity is rational, as clearly $|G|$ and $\dim M$ are integers. Since the left-hand-side is in $\overline{\mathbb{Z}}$ and the right-hand-side is in \mathbb{Q} they must actually be in $\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$, and thus $\dim M$ divides $|G|$. \square

Lemma 7.3.29 If ξ_1, \dots, ξ_n are roots of unity such that $a := (\xi_1 + \dots + \xi_n)/n$ is an algebraic integer then either $\xi_1 = \dots = \xi_n$ or $\xi_1 + \dots + \xi_n = 0$.

Proof. If the ξ_i are not all equal then it follows from the geometry of roots of unity that $|a| < 1$. Suppose that $p(x)$ is the minimal polynomial with a as a root, then any other root, a' , of this polynomial must also be a root of unity, and as such $|a'| \leq 1$ also. The product of all roots of p is an integer, and since they all have absolute value at most 1, and $|a| < 1$ it follows that this integer has absolute value less than 1, and so must be 0. Thus, $a = 0$, and since $1/n \neq 0$ we achieve the desired result. \square

Theorem 7.3.30. Let G be a finite group and M a simple G -module. Let $C \in \mathcal{C}(G)$ be a conjugacy class such that $\gcd(|C|, \dim M) = 1$. Then either $\chi_M(g) = 0$ or $\rho_M(g) = \varepsilon \text{id}_M$ for some $\varepsilon \in \mathbb{C}$ for all $g \in C$.

Proof. Since $\gcd(|C|, \dim M) = 1$ there exist integers a and b such that

$$a|C| + b \dim M = 1. \quad (7.3.31)$$

Multiplying by $\chi_M(g)/\dim M$ we get

$$\frac{|C|\chi_M(g)}{\dim M} + b\chi_M(g) = \frac{\chi_M(g)}{\dim M} = \frac{\varepsilon_1 + \dots + \varepsilon_n}{n} \quad (7.3.32)$$

where ε_i are the eigenvalues of $\rho_M(g)$ and n is the dimension of M . Then the left-hand-side is an algebraic integer, since a is an integer, $|C|\chi_M(g)/\dim M$ is an algebraic integer by Proposition 7.3.17, b is an integer, and $\chi_M(g)$ is an algebraic integer as it is a sum of the eigenvalues of $\rho_M(g)$ which are roots of unity as g has finite order as G is finite. Thus, $(\varepsilon_1 + \dots + \varepsilon_n)/n$ is an algebraic integer by Lemma 7.3.29, so it is either 0 or $\varepsilon_1 = \dots = \varepsilon_n = \varepsilon$, in which case $\rho_M(g) = \varepsilon \text{id}_M$. \square

Theorem 7.3.33. Let G be a finite group and $C \in \mathcal{C}(G)$ a conjugacy class such that $|C| = p^k$ for p some prime and $k \in \mathbb{Z}_{>0}$. Then G has a proper nontrivial normal subgroup.

Proof. We may always split the set of simple G -modules as

$$\text{Irr } G = \{\mathbb{C}\} \sqcup D \sqcup N \quad (7.3.34)$$

where \mathbb{C} is the trivial representation, and D and N are the sets of “divisible” and “not divisible” dimension irreducible representations. That is,

$$D = \{M \in \text{Irr } G \mid p \mid \dim M\}, \quad \text{and} \quad N = \{M \in \text{Irr } G \mid p \nmid \dim M\}. \quad (7.3.35)$$

We claim that there exists some $M \in N$ such that $\chi_M(g) \neq 0$. To see this first note that if $M \in D$ then p divides $\dim M$, so $(\dim M)/p$ is an integer, and hence an algebraic integer. Thus,

$$a = \sum_{M \in D} \frac{1}{p} (\dim M) \chi_M(g) \quad (7.3.36)$$

is an algebraic integer. Taking some $g \in C$ we know that $g \neq 1$ since $|C| = p^k \neq 1$ and the identity is always in a conjugacy class on its own. Thus, by the second orthogonality relation we know that [Theorem 6.5.19](#)

$$\sum_{M \in \text{Irr}(G)} \overline{\chi_M(e)} \chi_M(g) = 0 \quad (7.3.37)$$

and of course the character of the identity is just the dimension, so this is nothing but

$$\sum_{M \in \text{Irr}(G)} (\dim M) \chi_M(g) = 0. \quad (7.3.38)$$

We can rewrite this sum in terms of the decomposition of $\text{Irr}(G)$ as

$$0 = \chi_{\mathbb{C}}(g) + \sum_{M \in D} (\dim M) \chi_M(g) + \sum_{M \in N} (\dim M) \chi_M(g) \quad (7.3.39)$$

$$= 1 + pa + \sum_{M \in N} (\dim M) \chi_M(g). \quad (7.3.40)$$

Here we've used the fact that the character of the trivial representation is identically 1, as well as [Equation \(7.3.36\)](#) to identify a . Since $pa \neq -1$, as p is a prime and a an integer, we know that

$$\sum_{M \in N} (\dim M) \chi_M(g) \neq 0 \quad (7.3.41)$$

and thus there must be some $M \in N$ such that $\chi_M(g) \neq 0$.

Now fix $M \in N$ to be such that $\chi_M(g) \neq 0$ for $g \in C$. Since $p \nmid \dim M$ we know that $|C| = p^k$ doesn't divide M , and since p is prime $\dim M$ doesn't divide $|C|$ either. Thus, $\gcd(|C|, \dim M) = 1$, and since $\chi_M(g) \neq 0$ we know that $\rho_M(g) = \varepsilon \text{id}_M$ for some ε for all $g \in C$ by [Theorem 7.3.30](#).

Now define the subgroup

$$H = \langle gh^{-1} \mid g, h \in C \rangle. \quad (7.3.42)$$

This is not equal to $\{1\}$ as $|C| > 1$ so there exist distinct g and h in C and $gh^{-1} \neq 1$ as inverses are unique. By construction, H is normal since conjugation simply permutes the, since for all $k \in G$ we have

$$kgh^{-1}k^{-1} = kgk^{-1}kh^{-1}k^{-1} = \hat{g}\hat{h}^{-1} \quad (7.3.43)$$

for some $\hat{g}, \hat{h} \in C$ by definition of a conjugacy class.

Further, H acts trivially on M . To see this take $g, h \in C$, and then we know that $\rho_M(g) = \varepsilon_g \text{id}_M$ and $\rho_M(h) = \varepsilon_h \text{id}_M$ for some scalars $\varepsilon_g, \varepsilon_h \in \mathbb{C}$. Thus,

$\chi_M(g) = \varepsilon_g \dim M$ and $\chi_M(h) = \varepsilon_h \dim M$, but characters are constant on conjugacy classes, so it must be that $\varepsilon_g = \varepsilon_h$. Thus, H simply acts by some scalar multiple, $\varepsilon = \varepsilon_1 = \varepsilon_h$, and we're free to choose $\varepsilon = 1$, as we know that H does not act as zero.

Finally, it must be that $H \subsetneq G$, since if $G = H$ then G acts trivially on M , but by definition M is not the trivial representation. \square

7.3.4 Proof of Burnside's Theorem

Finally, we're ready to put all of these technical results together to prove Burnside's theorem. We'll do this in two cases. The first is to prove that if the order of G has a unique prime factor then G is solvable, then the main result can be prove assuming two distinct prime factors.

Proposition 7.3.44 Let G be a group of order p^a for some prime, p , and $a \in \mathbb{Z}_{\geq 0}$. Then G is solvable.

Proof. First note that if $a = 0$ then G is trivial and is trivially solvable. We then induct on a . Suppose that the statement is true for all $a < n$ for some integer n . Now take $|G| = p^n$.

The class equation is a result from group theory which tells us that

$$|G| = |Z(G)| + \sum_i [G : Z_{g_i}] \quad (7.3.45)$$

where the sum is over conjugacy classes. The order of any conjugacy class of G must divide $|G|$, and so it follows that all conjugacy classes have size p^{k_i} for some $k_i \in \mathbb{Z}_{\geq 0}$. Then we have that $|G| = p^n = |Z(G)| + \sum_i p^{k_i}$. Thus, p must divide $|Z(G)|$, and so $Z(G)$ is nontrivial.

If G is abelian then G is solvable. If G is not abelian then $Z(G)$ is an abelian subgroup, which is solvable, meaning there exist normal subgroups

$$\{1\} \triangleleft Z_1 \triangleleft Z_2 \triangleleft \cdots \triangleleft Z_n = Z(G). \quad (7.3.46)$$

Quotients of successive terms are abelian as every group in this chain is abelian. Then $Z(G)$ is normal in G since everything in G commutes with everything in $Z(G)$. Further, $G/Z(G)$ is abelian. Thus, we have a chain of normal subgroups,

$$\{1\} \triangleleft Z_1 \triangleleft Z_2 \triangleleft \cdots \triangleleft Z_n = Z(G) \triangleleft G \quad (7.3.47)$$

such that quotients of successive subgroups are abelian. This proves G is solvable. \square

Theorem 7.3.48 — Burnside's Theorem. Any group, G , of order $p^a q^b$ with p and q primes and $a, b \in \mathbb{Z}_{\geq 0}$ is solvable.

Proof. First, since the trivial group is solvable and [Proposition 7.3.44](#) shows that all p -groups (that is, groups of order p^a) are solvable we may assume that p and q are distinct with $a, b \neq 0$. Finally, if G is abelian it is solvable, so we may assume that G is nonabelian, and in particular that $Z(G) \subsetneq G$. The proof is by contradiction, so assume G has order $p^a q^b$ and isn't solvable. Further, suppose that G is the smallest such G . Then G must be simple, else one of its normal subgroups would have this property. We then know from [Theorem 7.3.33](#) that G cannot have a conjugacy class, $C \in \mathcal{C}(G)$, of order p^k or q^k for $k \geq 1$. Thus, all conjugacy classes are either singletons or have order divisible by pq . However, we also know that

$$p^a q^b = |G| = \sum_{C \in \mathcal{C}(G)} |C| = 1 + \sum_{C \in \mathcal{C}(G) \setminus \{1\}} |C| \quad (7.3.49)$$

and the only way this can hold is if there is some $C \in \mathcal{C}(G)$ with $|C| = 1$, as if all conjugacy classes other than $\{1\}$ have order divisible by pq then 1 plus this sum cannot be divisible by pq . Thus, whatever element is in this C with $|C| = 1$ must be central. Hence, G has nontrivial centre, and thus has a normal subgroup, the centre of G . This is a contradiction of the simplicity, and hence a contradiction of our assumption of non-solvability. \square

Appendices

A

Complex, Real and Quaternionic Types

A.1 Complexification

Let G be a finite group and let M be a simple G -module over \mathbb{R} . We first consider the complexification, $M_{\mathbb{C}} := \mathbb{C} \otimes_{\mathbb{R}} M$ which is a complex vector space with scalar multiplication defined by $w(z \otimes m) = (wz) \otimes m$ for $w, z \in \mathbb{C}$ and $m \in M$. It is convention to simply write zm for $z \otimes m$. This is simply extension of scalars, we can identify $M_{\mathbb{C}}$ as “ M but we define formal multiplication by complex numbers”.

The complexified space, $M_{\mathbb{C}}$, is a G -module still, it just inherits the action of G on M . Specifically, $g \cdot (z \otimes m) = z \otimes (g \cdot m)$ for $g \in G$, $z \in \mathbb{C}$, and $m \in M$. We usually just write $g \cdot zm = z(g \cdot m)$.

For $x, y \in \mathbb{R}$ with $z = x + iy$ we can write $z \otimes m$ as

$$(x + iy) \otimes m = x \otimes m + iy \otimes m = x(1 \otimes m) + y(i \otimes m). \quad (\text{A.1.1})$$

This lets us decompose $M_{\mathbb{C}}$ as

$$M_{\mathbb{C}} = (1 \otimes M) \oplus (i \otimes M). \quad (\text{A.1.2})$$

This is somewhat sloppy notation, we really have $(\mathbb{R}1 \otimes_{\mathbb{R}} M) \oplus (\mathbb{R}i \otimes_{\mathbb{R}} M)$, and since $\mathbb{R}c \cong \mathbb{R}$ and $\mathbb{R} \otimes M \cong M$ for any real vector space, M , we have that $M_{\mathbb{C}} \cong M \oplus M$, where the first copy is thought of as the real part, and the second as the imaginary part. This gives a second way of thinking of the complexification of M , it’s exactly the same process that we apply to get the complex numbers out of the reals. We’ll use the familiar notation of \mathbb{C} to write $m \in M_{\mathbb{C}}$ as $a + ib$ when we view it like this. With this interpretation the action of “multiplication by i ” is $a + ib \mapsto -b + ia$. This can be encoded in the block matrix

$$J = \begin{pmatrix} 0 & -\text{id}_V \\ \text{id}_V & 0 \end{pmatrix}. \quad (\text{A.1.3})$$

The action of $g \in G$ on $M_{\mathbb{C}}$ when viewed as $M \oplus M$ is $g \cdot (a + ib) = (g \cdot a) + i(g \cdot b)$. This extends to $g \in \mathbb{R}G$. Note that we still consider the real group algebra, and any complex coefficient we might want to include is treated separately by the action of $x\text{id}_{M_{\mathbb{C}}} + Jy$.