LTCC Representation theory

Matt Fayers, based on notes by Markus Linckelmann

thanks to Diego Millan Berdasco for corrections

Contents

1 Basics

1.1 Some linear algebra

In this course I'll assume that you're pretty familiar with basic linear algebra. But we'll begin by revising a few simple concepts. Throughout these notes we fix a field $\mathbb{F}$, and all vector spaces will be over $\mathbb{F}$. dim will always mean dimension over $\mathbb{F}$.

Some basic notation: for any vector space V, we write id_V (or just id, if it's clear what V is) for the identity function from V to V. Also, we'll abuse notation by writing 0 instead of $\{0\}$ for the zero vector space.

Definition. Suppose V and W are vector spaces.

1. The *direct sum* $V \oplus W$ is the set of all symbols $v \oplus w$ for $v \in V$, $w \in W$, with addition and scalar multiplication defined by

$$(v \oplus w) + (v' \oplus w') = (v + v') \oplus (w + w'), \qquad x(v \oplus w) = (xv) \oplus (xw)$$

for $x \in \mathbb{F}$, $v, v' \in V$, $w, w' \in W$.

2. The *tensor product* $V \otimes W$ is the set of all formal sums of symbols $v \otimes w$ with $v \in V$ and $w \in W$, modulo the relations

$$(xv) \otimes w = v \otimes (xw), \qquad (v + v') \otimes w = v \otimes w + v' \otimes w, \qquad v \otimes (w + w') = v \otimes w + v \otimes w'$$

for $x \in \mathbb{F}$, $v, v' \in V$, $w, w' \in W$. We make $V \otimes W$ is a vector space via

$$x(v \otimes w) = (xv) \otimes w$$

for $x \in \mathbb{F}$, $v \in V$, $w \in W$.

Note that if B is a basis for V and C is a basis for W, then

$$\{b \oplus 0 \mid b \in B\} \cup \{0 \oplus c \mid c \in C\}$$

is a basis for $V \oplus W$, and

$$\{b \otimes c \mid b \in B,\ c \in C\}$$

is a basis for $V \otimes W$. Hence if V and W are finite-dimensional then

$$\dim(V \oplus W) = \dim(V) + \dim(W), \qquad \dim(V \otimes W) = \dim(V) \dim(W).$$

Definition. Suppose V is a vector space and $W \leqslant V$. The *quotient space* V/W is the set of all cosets

$$v + W = \{v + w \mid w \in W\}$$

with vector space structure given by

$$(u + W) + (v + W) = (u + v) + W, \qquad x(v + W) = (xv) + W$$

for $u, v \in V$ and $x \in \mathbb{F}$.

Suppose B is a basis for V and C is a basis for W with $C \subseteq B$. Then

$$\{ b + W \mid b \in B \setminus C \}$$

is a basis for V/W. Hence if V is finite-dimensional, then

$$\dim(V/W) = \dim(V) - \dim(W).$$

Note that we can have $u + W = v + W$ even when $u \neq v$, so we need to be careful. A precise (and useful) statement is the following.

Coset Lemma. *Suppose V is a vector space, $u, v \in V$ and $W \leqslant V$. Then $u + W = v + W$ if and only if $u - v \in W$.*

1.2 Rings

Now let's revise some basic definitions for rings.

Definition. A *ring* is a set R with two special elements 0 and 1 and two binary operations $+, \times$ such that:

- R is an abelian group under $+$, with zero element 0;
- $\times$ is associative, i.e. $r \times (s \times t) = (r \times s) \times t$ for all $r, s, t \in R$;
- $1 \times r = r \times 1 = r$ for all $r \in R$;
- (the distributive law) $r \times (s + t) = (r \times s) + (r \times t)$ and $(r + s) \times t = (r \times t) + (s \times t)$ for all $r, s, t \in R$.

We'll use standard conventions of notation, writing rs instead of $r \times s$, and writing expressions like $rs + t$ without brackets on the understanding that we do the multiplication first. We also adopt the following convention: if $r \in R$ and $X \subseteq R$, then we write rX to mean $\{ rx \mid x \in X \}$. Similarly we define Xr, rXs, XrY etc.

We refer to the element 1 as the *identity* element of R, and to 0 as the *zero element*. Note that (unlike some people) we do not require these two elements to be distinct. The only effect of this is to permit the *trivial ring* $\{0\}$ which has addition and multiplication defined in the only possible way. Very occasionally we will prove results that only hold for non-trivial rings, but in general the trivial ring will be allowed.

We'll need the following definitions in order to define an algebra.

Definition.

1. If R is a ring, the *centre* of R is the set
$$Z(R) = \{ a \in R \mid ab = ba \text{ for all } b \in R \}.$$
2. If R and S are rings, a *homomorphism* from R to S is a function $\phi : R \to S$ such that $\phi(ab) = \phi(a)\phi(b)$, $\phi(a + b) = \phi(a) + \phi(b)$ and $\phi(1_R) = 1_S$ for all $a, b \in R$.

Note that in the definition of a homomorphism, the condition $\phi(1_R) = 1_S$ rules out, for example, the trivial map which sends a to 0 for all $a \in R$ (unless S is the trivial ring).

1.3 Algebras

Now we come to algebras.

Definition. An $\mathbb{F}$-*algebra* is a ring A together with a specified ring homomorphism from $\mathbb{F}$ to $Z(A)$.

Almost always in these notes we shall be considering algebras over $\mathbb{F}$, so we will just say 'algebra' to mean '$\mathbb{F}$-algebra'.

Remarks.

1. Some people's definition of an algebra A requires that the homomorphism from $\mathbb{F}$ to $Z(A)$ be injective. The only difference between this and our definition is that it rules out the possibility that A is the trivial ring. Indeed, if A is a ring $\phi : \mathbb{F} \to A$ is a non-injective homomorphism, take $0 \neq x \in \mathbb{F}$ with $\phi(x) = 0$; then $1_A = \phi(1_{\mathbb{F}}) = \phi(xx^{-1}) = \phi(x)\phi(x^{-1}) = 0\phi(x^{-1}) = 0$, so that A is the trivial ring. We prefer to allow the trivial ring; for example, if V is a non-zero $\mathbb{F}$-vector space, then the set $\mathrm{End}_{\mathbb{F}}(V)$ of linear maps from V to V is an $\mathbb{F}$-algebra; if we want to extend this to the case $V = 0$, we need to allow the trivial ring as an algebra.

2. In the cases where A is non-trivial (so the corresponding ring homomorphism is injective), it is customary to identify $\mathbb{F}$ with its image under the homomorphism, and thereby regard $\mathbb{F}$ as a subring of $Z(A)$.

3. An algebra A is naturally a vector space over $\mathbb{F}$; if A is trivial this is obvious, while if A is non-trivial and we regard $\mathbb{F}$ as a subring of A as above, then the scalar multiplication is just given by the ring multiplication in A. This leads to an alternative definition of an algebra: it is an $\mathbb{F}$-vector space equipped with a binary operation $\times$ which which satisfies the associative and identity laws and is bilinear.

Definition. Suppose A and B are algebras. A *homomorphism* from A to B is an $\mathbb{F}$-linear map which is also a ring homomorphism.

Note that not every ring homomorphism between two algebras is an algebra homomorphism. For example, take $\mathbb{F} = A = B = \mathbb{C}$; then complex conjugation is a ring homomorphism, but is not $\mathbb{C}$-linear.

We use standard terminology associated with homomorphisms: an *isomorphism* is a homomorphism which is also a bijection (in which case its inverse is also an isomorphism), and two algebras are *isomorphic* if there is at least one isomorphism between them. An *automorphism* of an algebra A is an isomorphism from A to A. The *kernel* of a homomorphism is the set of elements that map to 0. As is always the case with linear maps, a homomorphism is injective if and only if its kernel is 0.

Definition. Suppose A is an algebra.

- A *subalgebra* of A is an $\mathbb{F}$-subspace which is also a subring (i.e. which is closed under multiplication and contains 1).
- A *left ideal* of A is an $\mathbb{F}$-subspace I of A such that $ai \in I$ for all $a \in A, i \in I$.
- A *right ideal* of A is an $\mathbb{F}$-subspace I of A such that $ia \in I$ for all $a \in A, i \in I$.

- An *ideal* of A is a left ideal which is also a right ideal.

We write $I \trianglelefteq_{\mathrm{L}} A$, $I \trianglelefteq_{\mathrm{R}} A$, $I \trianglelefteq A$ to mean that I is a left ideal, a right ideal or an ideal of A, respectively.

Some key examples: if A is a non-trivial algebra, then $\mathbb{F}$ is a subalgebra of A. If X is any subset of A, let $AX = \{ax \mid a \in A,\ x \in X\}$. Then the subspace of A spanned by AX is a left ideal of A. Similarly the subspace spanned by XA is a right ideal, and the subspace spanned by $AXA = \{axb \mid a, b \in A,\ x \in X\}$ is an ideal.

Lemma 1.1. *Suppose A is an algebra and $I \trianglelefteq A$. Then the quotient vector space A/I is an $\mathbb{F}$-algebra, with multiplication defined by $(a+I)(b+I) = ab + I$ and with identity element $1 + I$.*

Proof. Exercise. □

The next result is called the First Isomorphism Theorem for algebras. If you've seen the First Isomorphism Theorem for groups, rings, or modules, then you should have no trouble proving it.

Theorem 1.2. *Suppose A and B are algebras and $\phi : A \to B$ is a homomorphism. Then $\ker(\phi)$ is an ideal of A, $\mathrm{im}(\phi)$ is a subalgebra of B, and there is an algebra isomorphism $A/\ker(\phi) \to \mathrm{im}(\phi)$ given by $a + \ker(\phi) \mapsto \phi(a)$.*

Proof. Exercise. □

Here we collect a few more bits of terminology.

Definition. If A is an algebra and $a \in A$, then a is *invertible* if there is an element $a^{-1} \in A$ such that $aa^{-1} = 1 = a^{-1}a$.

Remarks.

1. The inverse of an invertible element is unique.
2. The set of invertible elements of A is a group under multiplication.
3. Note that we require an inverse to be *two-sided*, i.e. $aa^{-1} = 1$ and $a^{-1}a = 1$. However, if A is finite-dimensional then this is unnecessary, as we now show.

Lemma 1.3. *Suppose A is a finite-dimensional algebra, and $a, b \in A$ such that $ab = 1$. Then $ba = 1$.*

Proof. Consider the map

$$\begin{aligned} \phi : A &\longrightarrow A \\ c &\longmapsto ca. \end{aligned}$$

ϕ is a linear map, and we claim that ϕ is injective: if $\phi(c) = 0$, then $ca = 0$, so $0 = 0b = cab = c1 = c$.

Now a linear map from a finite-dimensional vector space to itself is injective if and only if it is surjective (by the Rank–Nullity Theorem), so ϕ is surjective and hence there is $c \in A$ such that $ca = 1$. And now

$$c = c1 = cab = 1b = b$$

so that $ba = ca = 1$. □

Definition. Suppose A is an algebra. The *opposite algebra* A^{op} is the same vector space with the opposite multiplication: $a \cdot b = ba$, where $a \cdot b$ is the multiplication in A^{op} and ba is the multiplication in A.

A lot of the algebras we'll see are isomorphic to their opposites. But there are some which aren't. For example, consider the $\mathbb{R}$-algebra

$$A = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \;\middle|\; a \in \mathbb{R},\ b, c \in \mathbb{C} \right\}$$

with the usual matrix multiplication. To see why $A \ncong A^{\mathrm{op}}$, note that A has a left ideal which is one-dimensional (over $\mathbb{R}$), but doesn't have a one-dimensional right ideal (you should check these statements!). Hence A^{op} doesn't have a one-dimensional left ideal, so A and A^{op} can't be isomorphic.

Now we see two ways to combine algebras to make larger ones.

Definition. Suppose A and B are algebras.

1. The direct sum $A \oplus B$ is an algebra with multiplication $(a \oplus b)(a' \oplus b') = (aa') \oplus (bb')$.
2. The tensor product $A \otimes B$ is an algebra with multiplication defined by $(a \otimes b)(a' \otimes b') = (aa') \otimes (bb')$, extending bilinearly.

Note that if A and B are algebras, then $A \oplus 0$ and $0 \oplus B$ are both ideals in $A \oplus B$, and $A \oplus B$ is the direct sum of these ideals. This provides a way to recognise direct sums of algebras.

Proposition 1.4. *Suppose A is an algebra and I, J are ideals in A with $A = I \oplus J$ as vector spaces. Then I and J are both algebras, so $A = I \oplus J$ as algebras.*

Proof. We show that I is an algebra. Certainly I is closed under addition and multiplication since I is an ideal, and all the other properties of an algebra follow from those for A, except the existence of an identity element. To see this, write $1 = e + f$ with $e \in I$ and $f \in J$. Then for any $i \in I$ we have $i = 1i = ei + fi$, and fi lies in both I and J (since these are both ideals). So $fi = 0$, so $ei = i$. Similarly $ie = i$, so e is an identity element for I. □

1.4 Modules

Now we come to the definition of a module.

Definition. Let R be a ring. A *left R-module* is an abelian group M together with a function $\times : R \times M \to M$ such that

- $r \times (m + n) = (r \times m) + (r \times n)$,
- $(r +_R s) \times m = (r \times m) + (s \times m)$,
- $(r \times_R s) \times m = r \times (s \times m)$,
- $1 \times m = m$

for all $r, s \in R$, $m, n \in M$.

There is a corresponding definition of a *right R-module*. In these notes we'll almost always consider left modules, so we'll just say 'module' to mean 'left module'.

Of course, if $A = \mathbb{F}$ then you already know what an A-module is – it's the same thing as a vector space over $\mathbb{F}$. In general, if A is an algebra and B is a subalgebra of A then any A-module is a B-module in a natural way. In particular if A is non-trivial then $\mathbb{F}$ is a subalgebra of A so an A-module is automatically an $\mathbb{F}$-module, i.e. a vector space. So we can talk about bases for modules, finite-dimensional modules etc.

Two key examples of modules are the *zero module* 0, with the obvious vector space structure and action of A, and the *regular module*: this is A itself as a vector space, with the A-action given by the multiplication in A. We often write the regular A-module as ${}_AA$ to make it clear that we're thinking of it as a module rather than an algebra.

Now we look at submodules.

Definition. Suppose A is an algebra and M is an A-module. A *submodule* of M is a subspace which is also a module under the same operations. We write $N \leqslant M$ to mean that N is a submodule of M.

Note that a submodule of the the regular module ${}_AA$ is just the same thing as a left ideal of A.

Definition. Suppose M is an A-module and $N \leqslant M$. Then the quotient space M/N is an A-module via

$$a(m + N) = (am) + N$$

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

1.5 Module homomorphisms

As with rings, we make the usual definitions regarding homomorphisms. A *homomorphism* between two A-modules M and N is a function $\phi : M \to N$ such that $\phi(m + n) = \phi(m) + \phi(n)$ and $\phi(am) = a\phi(m)$ for $m, n \in M$ and $a \in A$. We use the terms *isomorphism*, *automorphism*, *kernel* and *image* in the usual way.

If M and N are A-modules, we write $\mathrm{Hom}_A(M, N)$ for the set of all homomorphisms from M to N. An example of such a homomorphism (which is often the only homomorphism) is the *zero homomorphism*, which maps $m \mapsto 0$ for every $m \in M$. The set $\mathrm{Hom}_A(M, N)$ is naturally an $\mathbb{F}$-vector space via

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

for $\phi, \psi \in \mathrm{Hom}_A(M, N)$, $m \in M$ and $x \in \mathbb{F}$.

An *endomorphism* of an A-module M just means a homomorphism from M to M. We write $\mathrm{End}_A(M)$ for the vector space $\mathrm{Hom}_A(M, M)$. For every $x \in \mathbb{F}$, the map $x\,\mathrm{id}_M$ is an endomorphism of M.

As well as being a vector space as described above, $\mathrm{End}_A(M)$ has another binary operation $\circ$ defined by composition:

$$(\phi \circ \psi)(m) = \phi(\psi(m)).$$

Proposition 1.5. *Suppose A is an algebra and M an A-module. The set $\mathrm{End}_A(M)$ is an algebra under the operations $+, \circ$, with $x \in \mathbb{F}$ mapping to $x\,\mathrm{id}_M$.*

Proof. Exercise. □

$\mathrm{End}_A(M)$ is referred to as the *endomorphism algebra* of M.
The case where $M = {}_AA$ is of particular interest.

Proposition 1.6. *Suppose A is an algebra. Then* $\mathrm{End}_A(A) \cong A^{\mathrm{op}}$.

Proof. Given $b \in A$, we have an endomorphism ϕ_b of A defined by $\phi_b(a) \mapsto ab$; this gives a function

$$\begin{aligned} \Phi : A &\longrightarrow \mathrm{End}_A(A) \\ b &\longmapsto \phi_b \end{aligned}$$

and since $\phi_{bc} = \phi_c \circ \phi_b$, Φ is a homomorphism from A^{op} to $\mathrm{End}_A(A)$. Φ has an inverse given by $\phi \mapsto \phi(1)$, so is an isomorphism. □

As with algebras, we have the First Isomorphism Theorem for modules.

Theorem 1.7. *Suppose A is an algebra, M and N are A-modules and $\phi : M \to N$ is a homomorphism. Then* $\ker(\phi) \leqslant M$, $\mathrm{im}(\phi) \leqslant N$ *and there is an isomorphism from* $M/\ker(\phi)$ *to* $\mathrm{im}(\phi)$ *given by* $m + \ker(\phi) \mapsto \phi(m)$.

Proof. Exercise. □

We also prove the Second and Third Isomorphism Theorems for modules. Unfortunately, there is no general agreement about which is which.

Theorem 1.8. *Suppose A is an algebra and M is an A-module, and $N, P \leqslant M$. Then $N/(N \cap P) \cong (N + P)/P$.*

Proof. We define a homomorphism

$$\begin{aligned} \phi : N &\longrightarrow M/P \\ n &\longmapsto n + P. \end{aligned}$$

The kernel of ϕ is the set of all $n \in N$ such that $n + P = 0 + P$, i.e. $n \in P$; so the kernel is $N \cap P$. We claim that the image is $(N + P)/P$. An element of $\mathrm{im}(\phi)$ has the form $n + P$ for $n \in N$; since $N \subseteq N + P$, this coset lies in $(N + P)/P$. Conversely, an element of $(N + P)/P$ can be written as $(n + p) + P$ for $n \in N$ and $p \in P$, but $(n + p) + P = n + P \in \mathrm{im}(\phi)$.

Now the First Isomorphism Theorem gives the result. □

Theorem 1.9. *Suppose A is an algebra and M is an A-module, and $P \leqslant N \leqslant M$. Then $N/P \leqslant M/P$, and $(M/P)/(N/P) \cong M/N$.*

Proof. Define a homomorphism

$$\begin{aligned} \phi : M/P &\longrightarrow M/N \\ m + P &\longmapsto m + N. \end{aligned}$$

ϕ is well-defined: if $l + P = m + P$, then $l - m \in P$, so $l - m \in N$, so $l + N = m + N$. ϕ is obviously surjective. The kernel of ϕ is the set of all $m + P$ such that $m + N = 0 + N$, i.e. $m \in N$. So $\ker(\phi) = \{ n + P \mid n \in N \} = N/P$.

Now the First Isomorphism Theorem gives the result. □

1.6 Direct sums of modules

Definition. Suppose M and N are A-modules. The direct sum $M \oplus N$ is also an A-module via

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

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

There is a natural way to think of M and N as submodules of $M \oplus N$: there are homomorphisms

$$\begin{aligned} \iota_M : M &\longrightarrow M \oplus N & \qquad \iota_N : N &\longrightarrow M \oplus N \\ m &\longmapsto m \oplus 0 & n &\longmapsto 0 \oplus n \end{aligned}$$

called the *canonical injections*. By the First Isomorphism Theorem, M is isomorphic to the submodule

$$\mathrm{im}(\iota_M) = \{ m \oplus 0 \mid m \in M \}$$

of $M \oplus N$, and we often identify M with this submodule. Similarly, we often identify N with the submodule $\{ 0 \oplus n \mid n \in N \}$. Then M and N are submodules of $M \oplus N$ with $M \cap N = 0$ and $M + N = M \oplus N$.

Conversely, if L is an A-module and M, N are submodules of L with $M \cap N = 0$ and $M + N = L$, then there is an isomorphism from $M \oplus N$ to L given by $m \oplus n \mapsto m + n$, and we often identify L with $M \oplus N$ via this isomorphism, and say that L is the direct sum of M and N.

Of course, we can extend the idea of a direct sum to more than two modules. Given a module M and a family of submodules $M_1, \ldots, M_r$, when do we have $M \cong M_1 \oplus \cdots \oplus M_r$? It's not enough to have $M = M_1 + \cdots + M_r$ and $M_i \cap M_j = 0$ for all $i \neq j$ (take $A = \mathbb{F}$, and consider three one-dimensional subspaces of $M = \mathbb{F}^2$).

Proposition 1.10. *Suppose A is an algebra and M is an A-module, and $M_1, \ldots, M_r$ are submodules of M. Then there is a homomorphism*

$$\begin{aligned} \phi : M_1 \oplus \cdots \oplus M_r &\longrightarrow M \\ m_1 \oplus \cdots \oplus m_r &\longmapsto m_1 + \cdots + m_r. \end{aligned}$$

ϕ is an isomorphism provided $M_1 + \cdots + M_r = M$ and $M_i \cap (\sum_{j \neq i} M_j) = 0$ for every i.

Proof. It is easy to check that ϕ is a homomorphism. Clearly $\mathrm{im}(\phi) = M_1 + \cdots + M_r$, so ϕ is surjective if and only if $M_1 + \cdots + M_r = M$. Now we claim that ϕ is injective if and only if $M_i \cap (\sum_{j \neq i} M_j) = 0$ for every i. If ϕ fails to be injective, take a non-zero element $m_1 \oplus \cdots \oplus m_r$ in its kernel. Since this is non-zero, there must be some i such that $m_i \neq 0$. But now

$$m_i = -\sum_{j \neq i} m_j \in M_i \cap (\sum_{j \neq i} M_j),$$

so $M_i \cap (\sum_{j \neq i} M_j) \neq 0$. Conversely, suppose that for some i we have $M_i \cap (\sum_{j \neq i} M_j) \neq 0$. This means we can find $m_j \in M_j$ for each j such that $0 \neq m_i = -\sum_{j \neq i} m_j$. But then $m_1 \oplus \cdots \oplus m_r$ is a non-zero element of $\ker(\phi)$, so ϕ is not injective. $\square$

Often we will want to consider a direct sum $M \oplus \cdots \oplus M$ of copies of the same module, and we may write $M^{\oplus n}$ for the direct sum of n copies of M. Given such a direct sum, we let ι_i be the ith canonical injection from M to $M^{\oplus n}$, i.e. the map which sends

$$m \longmapsto 0 \oplus \cdots \oplus 0 \oplus m \oplus 0 \oplus \cdots \oplus 0$$

with m in the ith position. We also let $\pi_i : M^{\oplus n} \to M$ be the ith canonical projection, which maps

$$m_1 \oplus \cdots \oplus m_n \longmapsto m_i.$$

Then ι_i, π_i are homomorphisms, and we have

$$\begin{aligned} \pi_i \circ \iota_i &= \mathrm{id}_M, \\ \pi_i \circ \iota_j &= 0 \qquad \text{if } i \neq j, \\ \sum_{i=1}^{n} \iota_i \circ \pi_i &= \mathrm{id}_{M^{\oplus n}}. \end{aligned}$$

The endomorphism ring of $M^{\oplus n}$ is easy to describe; if B is any algebra, let $\mathrm{Mat}_n(B)$ denote the algebra of $n \times n$ matrices over B, with the usual addition and multiplication. (n.b. You have to be slightly careful with multiplication, if B is not commutative: the product of two matrices m, n is given by $(mn)_{ij} = \sum_k m_{ik} n_{kj}$, not $\sum_k n_{kj} m_{ik}$.

Proposition 1.11. *Suppose A is an algebra and M is an A-module, and n is a non-negative integer. Then*

$$\mathrm{End}_A(M^{\oplus n}) \cong \mathrm{Mat}_n(\mathrm{End}_A(M)).$$

Proof. Suppose $\alpha \in \mathrm{End}_A(M^{\oplus n})$. Define a matrix $\Phi(\alpha)$ by setting $\Phi(\alpha)_{ij} = \pi_i \circ \alpha \circ \iota_j$ for each i, j. Then $\Phi(\alpha)_{ij} \in \mathrm{End}_A(M)$, so we have a map $\Phi : \mathrm{End}_A(M^{\oplus n}) \to \mathrm{Mat}_n(\mathrm{End}_A(M))$. It's easy to check that Φ is linear, and in fact it's an algebra homomorphism, since for $\alpha, \beta \in \mathrm{End}_A(M^{\oplus n})$ we have

$$\begin{aligned} \Phi(\alpha \circ \beta)_{ij} &= \pi_i \circ \alpha \circ \beta \circ \iota_j \\ &= \pi_i \circ \alpha \circ \left(\sum_{k=1}^{n} \iota_k \circ \pi_k \right) \circ \beta \circ \iota_j \\ &= \sum_{k=1}^{n} (\pi_i \circ \alpha \circ \iota_k) \circ (\pi_k \circ \beta \circ \iota_j) \\ &= \sum_{k=1}^{n} \Phi(\alpha)_{ik} \circ \Phi(\beta)_{kj} \\ &= (\Phi(\alpha)\Phi(\beta))_{ij}. \end{aligned}$$

To show that Φ is bijective, we construct its inverse: given a matrix $\phi \in \mathrm{Mat}_n(\mathrm{End}_A(M))$, define $\alpha \in \mathrm{End}_A(M^{\oplus n})$ by

$$\alpha = \sum_{i,j} \iota_i \circ \phi_{ij} \circ \pi_j.$$

Then α is the unique element of $\mathrm{End}_A(M^{\oplus n})$ satisfying $\Phi(\alpha) = \phi$. □

1.7 Decomposable modules, simple modules and maximal submodules

Definition. Suppose A is an algebra and M is an A-module. M is *reducible* if it has a proper non-zero submodule, and *irreducible* (or *simple*) if it is non-zero and not reducible. M is *decomposable* if it can be written as the direct sum of two non-zero submodules, and *indecomposable* if it is non-zero and not decomposable.

Note that we do not consider the zero module to be either reducible or irreducible, or decomposable or indecomposable (in the same way that 1 is neither a prime number nor a composite number).

Example. A decomposable module must be reducible, but the converse is not true in general. Take A to be the algebra

$$\mathcal{T}_2(\mathbb{F}) = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \;\middle|\; a, b, c \in \mathbb{F} \right\}$$

and let M be the natural module $\mathbb{F}^2$.

You can check that the only proper non-zero submodule of M is the set

$$\left\{ \begin{pmatrix} x \\ 0 \end{pmatrix} \;\middle|\; x \in \mathbb{F} \right\}.$$

So M is reducible (as it has a proper non-zero submodule) but indecomposable (as it can't be written as a direct sum of proper submodules).

Definition. Suppose A is an algebra and M is an A-module. A *maximal* submodule of M is a submodule $N < M$ such that there is no other submodule P with $N < P < M$.

Proposition 1.12. *Suppose A is an algebra and M is an A-module, and $N \leqslant M$. Then M/N is a simple module if and only if N is a maximal submodule of M.*

Proof. Suppose N is not a maximal submodule. If $N = M$, then M/N is the zero module, which by definition is not simple. Otherwise, there is P with $N < P < M$. Then P/N is a proper non-zero submodule of M/N, so M/N is not simple.

Conversely, suppose M/N is not simple. If M/N is the zero module, then $N = M$, so N is by definition not maximal. Otherwise, there is a proper non-zero submodule L of M/N. But then if we set $P = \{ m \in M \mid m + N \in L \}$, then $N < P < M$, so N is not a maximal submodule of M. □

Now we consider composition series.

Definition. Suppose A is an algebra and M is an A-module. A *composition series* for M is a finite chain of submodules

$$M_0 > \cdots > M_r$$

such that $M_0 = M$, $M_r = 0$ and M_i/M_{i+1} is simple for each i.

Every finite-dimensional module has a composition series: if $M \neq 0$, then take a submodule $M_1 < M$ of largest possible dimension; this must then be a maximal submodule. Then find a maximal submodule M_2 of M_1, and so on until you reach the zero module; this must happen, because the dimension is decreasing at each step.

Theorem 1.13 (Jordan–Hölder Theorem)**.** *Suppose A is an algebra and M is an A-module. Suppose that*

$$M_0 > \cdots > M_r$$
$$N_0 > \cdots > N_s$$

are both composition series for M. Then $r = s$, and the simple modules $M_0/M_1, \ldots, M_{r-1}/M_r$ are isomorphic to the simple modules $N_0/N_1, \ldots, N_{r-1}/N_r$ in some order.

First we need a lemma.

Lemma 1.14. *Suppose A is an algebra and M is an A-module. Suppose N and U are submodules of M, and that V is a maximal submodule of U. Then exactly one of the following occurs:*

- *$U \cap N = V \cap N$, and $U/V \cong (U+N)/(V+N)$;*
- *$U + N = V + N$, and $U/V \cong (U \cap N)/(V \cap N)$.*

Proof. Note that

$$V \leqslant (U \cap N) + V \leqslant U.$$

V is a maximal submodule of U, which means we must have equality in one (and only one) of these inequalities.

- If $V = (U \cap N) + V$, then $U \cap N \subseteq V$, so $U \cap N \subseteq V \cap N$, and so $U \cap N = V \cap N$ (since obviously $V \cap N \subseteq U \cap N$). Now we claim that $U \cap (V+N) = V$. Certainly $U \cap (V+N) \geqslant V$, since $U \geqslant V$ and $V + N \geqslant V$. For the other direction, take an element $u \in U \cap (V+N)$; since $u \in V + N$, we can write $u = v + n$ with $v \in V$ and $n \in N$. Then $n = u - v \in U$, since both u and v lie in U. So $n \in U \cap N = V \cap N$, so $n \in V$, so $u = v + n \in V$.

  Now we apply Theorem 1.8 and get

$$\frac{U+N}{V+N} = \frac{U+(V+N)}{V+N} \cong \frac{U}{U \cap (V+N)} = \frac{U}{V}.$$

- Alternatively, if $(U \cap N) + V = U$, then $U + N = (U \cap N) + V + N = V + N$, and by Theorem 1.8

$$\frac{U \cap N}{V \cap N} = \frac{U \cap N}{V \cap (U \cap N)} \cong \frac{(U \cap N) + V}{V} = \frac{U}{V}.$$ □

Proof of the Jordan–Hölder Theorem . If $r = 0$ then $M = 0$ and the result is trivial, so assume $r \geqslant 1$, and let $N = N_1$. Then we have chain of modules

$$\begin{array}{ccccccc} M_0 + N & \geqslant & M_1 + N & \geqslant & \cdots & \geqslant & M_r + N. \\ \| & & & & & & \| \\ M & & & & & & N \end{array}$$

But N is a maximal submodule of M, so we must have equality in all of these inequalities except one; that is, there is i such that

$$M_0 + N = \cdots = M_i + N > M_{i+1} + N = \cdots = M_0 + N.$$

Now by Lemma 1.14 we have $M_i \cap N = M_{i+1} \cap N$, while $M_{j+1} \cap N$ is a maximal submodule of $M_j \cap N$ for all $j \neq i$. Hence we have a new composition series (of length r) for M, namely

$$M > \underset{\substack{\| \\ N}}{M_0 \cap N} > \cdots > M_i \cap N > M_{i+2} \cap N > \cdots > M_r \cap N.$$

Now we have two composition series for N, of lengths $r-1$ and $s-1$, namely

$$M_0 \cap N > \cdots > M_i \cap N > M_{i+2} \cap N > \cdots > M_r \cap N$$

and

$$N_1 > N_2 > \cdots > N_s.$$

By induction we get $r-1 = s-1$, and the simple modules

$$\frac{M_0 \cap N}{M_1 \cap N}, \ldots, \frac{M_{i-1} \cap N}{M_i \cap N}, \frac{M_{i+1} \cap N}{M_{i+2} \cap N}, \ldots, \frac{M_{r-1} \cap N}{M_r \cap N}$$

are isomorphic to

$$\frac{N_1}{N_2}, \ldots, \frac{N_{r-1}}{N_r}$$

in some order. By Lemma 1.14 this means that

$$\frac{M_0}{M_1}, \ldots, \frac{M_{i-1}}{M_i}, \frac{M_{i+1}}{M_{i+2}}, \ldots, \frac{M_{r-1}}{M_r}$$

are isomorphic to

$$\frac{N_1}{N_2}, \ldots, \frac{N_{r-1}}{N_r}$$

in some order; also by Lemma 1.14, the remaining simple module M_i/M_{i+1} is isomorphic to $(M_i + N)/(M_{i+1} + N) = M/N$, which completes the proof. □

If M has a composition series $M_0 > \cdots > M_r$, the simple modules M_i/M_{i+1} are called the *composition factors* of M. The Jordan–Hölder Theorem just says that the composition factors are well-defined up to isomorphism and re-ordering.

1.8 Representations of algebras and the structure homomorphism

If A is an algebra, a *representation* A is a homomorphism $A \to \mathrm{End}_{\mathbb{F}}(M)$ for some vector space M. In fact, representations of A and A-modules are effectively the same thing, as we now show.

If M is an A-module and $a \in A$, then the map

$$\begin{aligned} \phi_a : M &\longrightarrow M \\ m &\longmapsto am \end{aligned}$$

is a linear map from M to M. So we have a function

$$\begin{aligned} \phi : A &\longrightarrow \mathrm{End}_{\mathbb{F}}(M) \\ a &\longmapsto \phi_a, \end{aligned}$$

and the axioms for a module guarantee that ϕ is an algebra homomorphism, i.e. a representation of A. This is sometimes called the *structure homomorphism*.

Conversely, if M is an $\mathbb{F}$-vector space and $\phi : A \to \mathrm{End}_{\mathbb{F}}(M)$ is a representation, then M becomes a module via $am = \phi(a)(m)$.

One can define homomorphisms between representations so that they correspond to module homomorphisms.

There is also the notion of a representation of a group G (over $\mathbb{F}$): this a homomorphism from G to the group $\mathrm{GL}(M)$ of invertible elements of $\mathrm{End}_{\mathbb{F}}(M)$, for some vector space M. Extending linearly, a representation of a group naturally gives a representation of the group algebra $\mathbb{F}G$; conversely, a representation of $\mathbb{F}G$ restricts to a representation of G (since in an algebra homomorphism, an invertible element must map to an invertible element). So representations of G over $\mathbb{F}$ naturally correspond to representations of $\mathbb{F}G$, and therefore to $\mathbb{F}G$-modules.

2 Semisimple modules and semisimple algebras

In this section we'll look at some particularly well-behaved modules and algebras. We start with modules; we'll give two different definitions which will turn out to be equivalent.

Definition. Suppose A is an algebra and M is an A-module. We say M has the *complement property* if for every $N \leqslant M$ there is $P \leqslant M$ such that $M = N \oplus P$.

Lemma 2.1. *Suppose A is an algebra and M is an A-module with the complement property. Then any submodule of M also has the complement property.*

Proof. Let $L \leqslant M$, and suppose $N \leqslant L$. We need to show there is $P \leqslant L$ such that $L = N \oplus P$. Using the complement property for M, there is $Q \leqslant M$ such that $M = N \oplus Q$. Now we claim that $L = N \oplus (L \cap Q)$. Certainly $N \cap (L \cap Q) = 0$, since $N \cap Q = 0$. Also, given $l \in L$, we can write $l = n + q$ with $n \in N$ and $q \in Q$, since $M = N + Q$. But then $q = l - n \in L$, so $q \in L \cap Q$, so $l \in N + (L \cap Q)$. □

Now here's a different-looking definition.

Definition. Suppose A is an algebra and M is an A-module. M is *semisimple* if it is the sum of its simple submodules.

Proposition 2.2. *Suppose A is an algebra and M is a finite-dimensional A-module. The following are equivalent.*

1. *M is semisimple.*
2. *M is a direct sum of finitely many simple submodules.*
3. *M has the complement property.*

Proof.
(2⇒1) Trivial.

(1⇒3) Suppose $N \leqslant M$, and take a submodule $P \leqslant M$ of largest possible dimension such that $N \cap P = 0$ (there must be a largest possible, since we are working inside a finite-dimensional module M). Then we claim that $M = N + P$, which means that $M = N \oplus P$. If $N + P < M$, then there must be some simple submodule S of M which is not contained in $N + P$ (because if $N + P$ contains all the simple submodules of M, then it contains their sum, namely M). Now $S \cap (N + P) < S$, so $S \cap (N + P) = 0$, since S is simple. Now we claim that $N \cap (P + S) = 0$. Take an element of $N \cap (P + S)$, and write it as $n = p + s$ for some $n \in N$, $p \in P$ and $s \in S$. Then $n - p = s \in (N + P) \cap S = 0$. So $n = p \in N \cap P$, so $n = p = 0$.

But now we have a submodule $P + S$ which satisfies $P + S > P$ and satisfies $N \cap (P + S) = 0$. This contradicts the choice of P.

(3⇒2) We use induction on $\dim(M)$. If $M = 0$ then the result is trivial, so assume $M \neq 0$. Then M has at least one simple submodule S (take a non-zero submodule of smallest possible dimension). By the complement property, there is $P \leqslant M$ such that $M = S \oplus P$. By Lemma 2.1, P also has the complement property. So by induction (2) also holds for P: that is, there is a finite set $\mathcal{T}$ of simple submodules of P such that $P = \bigoplus_{T \in \mathcal{T}} T$. And now $M = P \oplus S = \bigoplus_{T \in \mathcal{T} \cup \{S\}} T$, so (2) holds for M. □

We remark that this proposition holds more generally – we can take M to be any semisimple module for any ring – but this requires Zorn's Lemma, and we must allow infinite direct sums.

Corollary 2.3. *Suppose A is an algebra and M is a finite-dimensional semisimple A-module. Then every submodule and every quotient of M is semisimple.*

Proof. Suppose $N \leqslant M$. Since M has the complement property, so does N, by Lemma 2.1.

To show that M/N is semisimple too, take $P \leqslant M$ such that $M = N \oplus P$. Then P is also semisimple, and hence so is

$$\frac{M}{N} = \frac{N+P}{N} \cong \frac{P}{N \cap P} = P. \qquad \square$$

We are going to prove Wedderburn's Theorem on semisimple algebras. First we need to look more closely at simple modules and simple submodules.

Theorem 2.4 (Schur's Lemma)**.** *Suppose A is an algebra and S and T are simple A-modules. If $\phi : S \to T$ is a homomorphism, then ϕ is either an isomorphism or zero.*

Proof. Suppose ϕ is not zero. Then $\ker(\phi)$ is a proper submodule of S, so is 0 (since S is simple). So ϕ is injective. $\mathrm{im}(\phi)$ is a non-zero submodule of T, so is T (since T is simple). So ϕ is surjective, so ϕ is an isomorphism. $\square$

This shows in particular that if S is a simple A-module, then $\mathrm{End}_A(S)$ is a *division algebra*, i.e. a non-trivial algebra in which every non-zero element is invertible.

Now we give a lemma about semisimple modules which will be useful later.

Lemma 2.5. *Suppose A is an algebra and M is an A-module, and that we can write $M = \sum_{T \in \mathcal{T}} T$, where $\mathcal{T}$ is a family of simple submodules of M. Then every simple submodule of M is isomorphic to one of the modules in $\mathcal{T}$.*

Proof. Suppose S is a simple submodule of M. Since M is semisimple we can find $P \leqslant M$ such that $M = S \oplus P$. Let $\pi_S : S \oplus P \to S$ be the canonical projection for this direct sum. Then $\pi_S(T)$ must be non-zero for some $T \in \mathcal{T}$, since if $\pi_S(T) = 0$ for every T, then $\pi_S(\sum_{T \in \mathcal{T}} T) = 0$, so that π_S is zero.

So the restriction $\pi_S|_T$ is a non-zero homomorphism between simple modules T and S. By Schur's Lemma, this is an isomorphism. $\square$

Now we come to simple and semisimple algebras.

Definition. Suppose A is an algebra. A is a *simple algebra* if it is non-trivial and has no proper non-zero ideals. A is a *semisimple algebra* if ${}_AA$ is a semisimple module.

We should think of semisimple algebras as being the easiest type of algebras to understand: the condition that ${}_AA$ is semisimple in fact implies that *every* finite-dimensional A-module is semisimple. So in order to understand all A-modules, we just need to understand what the simple modules look like and take direct sums of them.

It turns out that finite-dimensional simple algebras are easy to describe.

Theorem 2.6. *Suppose A is a finite-dimensional algebra. The following are equivalent.*

1. *A is a simple algebra.*

2. *There is a simple A-module S and a positive integer n such that ${}_AA \cong S^{\oplus n}$.*
3. *There is a positive integer n and a finite-dimensional division algebra D such that $A \cong \mathrm{Mat}_n(D)$ as algebras.*

Proof.

(1⇒2) Let S be a simple submodule of ${}_AA$. (There certainly is such a submodule, since A is non-zero and finite-dimensional – just take a submodule of ${}_AA$ of smallest dimension.) Given $a \in A$, Sa is another submodule of ${}_AA$. Moreover, there is a surjective homomorphism

$$\begin{aligned} \phi : S &\longrightarrow Sa \\ s &\longmapsto sa. \end{aligned}$$

Since S is simple, we have either $Sa = 0$ or $Sa \cong S$. Now let $I = SA$. Then I is an ideal in A, and is non-zero (as it contains S) so (since A is simple) $I = A$. So $A = SA = \sum_{a \in A} Sa$. Discarding those Sa which equal 0, we have that ${}_AA$ is a sum of simple submodules all isomorphic to S. In particular, ${}_AA$ is semisimple, so ${}_AA$ is a direct sum of finitely many simple submodules, and by Lemma 2.5 these submodules are all isomorphic to S, i.e. ${}_AA \cong S^{\oplus n}$ for some n.

(2⇒3) Suppose ${}_AA \cong S^{\oplus n}$. Recall from Proposition 1.6 that $A^{\mathrm{op}} \cong \mathrm{End}_A({}_AA)$. So

$$\begin{aligned} A &\cong \mathrm{End}_A({}_AA)^{\mathrm{op}} \\ &\cong \mathrm{End}_A(S^{\oplus n})^{\mathrm{op}} \\ &\cong \mathrm{Mat}_n(\mathrm{End}_A(S))^{\mathrm{op}} && \text{by Proposition 1.11} \\ &\cong \mathrm{Mat}_n(\mathrm{End}_A(S)^{\mathrm{op}}) \end{aligned}$$

with the last isomorphism defined by mapping a matrix to its transpose. By Schur's Lemma $\mathrm{End}_A(S)$ is a division algebra, and hence so is $\mathrm{End}_A(S)^{\mathrm{op}}$.

(3⇒1) Exercise. □

Proposition 2.7. *Suppose A is a finite-dimensional semisimple algebra. Then A is a direct sum of simple algebras.*

Proof. We use induction on $\dim(A)$. Assuming A is non-trivial, let S be a simple submodule of ${}_AA$. Let N be the sum of all submodules of ${}_AA$ isomorphic to S, and let P be the sum of all the simple submodules of ${}_AA$ not isomorphic to S. Then $N + P = A$ because A is semisimple, and we claim $N \cap P = 0$. If $N \cap P \neq 0$, then $N \cap P$ has a simple submodule, say T. But then by Lemma 2.5 $T \cong S$ and $T \ncong S$; contradiction.

So $A = N \oplus P$ as vector spaces. We we claim $N \trianglelefteq A$: certainly $N \trianglelefteq_{\mathrm{L}} A$, because it's a sum of submodules of ${}_AA$. To see that N is closed under right multiplication, take $U \leqslant {}_AA$ with $U \cong S$, and $a \in A$. Then Ua is a submodule of ${}_AA$, and there is a surjective homomorphism $U \to Ua$ given by $u \mapsto ua$. So Ua is either 0 or isomorphic to S, so $Ua \subseteq N$. Similarly $P \trianglelefteq A$, so by Proposition 1.4 $A = N \oplus P$ as algebras.

Now we claim N is a simple algebra. As an A-module, N is a sum of submodules isomorphic to S. Hence N is a semisimple A-module, and so in fact is a direct sum of finitely many

simple modules, and by Lemma 2.5 these are all isomorphic to S. So $N \cong S^{\oplus n}$ as A-modules, and hence as N-modules. So by Theorem 2.6 N is a simple algebra.

P is also a semisimple A-module, and hence a semisimple algebra, so by induction is a direct sum of simple algebras. Hence $A = N \oplus P$ is too. □

Corollary 2.8 (Wedderburn's Theorem)**.** *Suppose A is a finite-dimensional semisimple algebra. Then there are division algebras $D_1, \ldots, D_r$ and positive integers $n_1, \ldots, n_r$ such that $A \cong \bigoplus_{i=1}^{r} \mathrm{Mat}_{n_i}(D_i)$.*

We will see in the next section that the decomposition in Wedderburn's Theorem is unique up to isomorphism.

3 Idempotents

Definition. Suppose A is an algebra. An *idempotent* in A is an element $e \in A$ such that $e^2 = e$. Two idempotents e, f are *orthogonal* if $ef = fe = 0$. An idempotent is *primitive* if it is non-zero and cannot be written as the sum of two non-zero orthogonal idempotents. A *primitive decomposition* of an idempotent e is a finite set of pairwise orthogonal primitive idempotents whose sum is e.

Let's observe a few basic facts about idempotents.

- 0 and 1 are idempotents.
- If e is an idempotent, then $1 - e$ is an idempotent which is orthogonal to e.
- If e and f are orthogonal idempotents, then $e + f$ is an idempotent.
- If e and f are idempotents which commute, then ef is an idempotent.
- The only invertible idempotent is 1: if e is an invertible idempotent, then multiplying both sides of the equation $e^2 = e$ by e^{-1} gives $e = 1$.

Proposition 3.1. *Suppose A is a finite-dimensional algebra and $e \in A$ is an idempotent. Then e has a primitive decomposition.*

Proof. Note that eA is a vector subspace of A. We use induction on $\dim(eA)$. If $e = 0$, then the empty set is a primitive decomposition of e. If e is primitive, then $\{e\}$ is a primitive decomposition of e. Otherwise, we can write $e = f + g$ where f and g are non-zero orthogonal idempotents. Then we claim $eA = fA \oplus gA$ as vector spaces. To see this, note that any element of eA can be written as $ea = (f + g)a = fa + ga \in fA + gA$, so that $eA = fA + gA$, while any element of $fA \cap gA$ can be written as $fa = gb$, so that $fa = f^2a = fgb = 0b = 0$; so $fA \cap gA = 0$.

fA and gA are obviously non-zero (they contain f and g respectively) and so both have dimension smaller than $\dim(eA)$. Hence by the inductive hypothesis f has a primitive decomposition $\{f_1, \ldots, f_r\}$ and g has a primitive decomposition $\{g_1, \ldots, g_s\}$. We claim that $\{f_1, \ldots, f_r, g_1, \ldots, g_s\}$ is a primitive decomposition of e; to see this we just need to show that f_i and g_j are orthogonal for all i, j. Note that if we multiply both sides of the equation $f = f_1 + \cdots + f_r$ on the left by f_i, we get $f_i f = f_i$. Similarly $gg_j = g_j$, so that $f_i g_j = f_i(fg)g_j = 0$. In the same way $g_j f_i = 0$, and we're done. □

An idempotent in A gives us a smaller algebra inside A, as follows.

Proposition 3.2. *Suppose A is an algebra and $e \in A$ is an idempotent. Then eAe is an algebra under the same operations as A, with identity element e. $eAe = A$ if and only if $e = 1$.*

Proof. It is easy to check that eAe is a vector subspace of A, and it is closed under multiplication since $(eae)(ebe) = e(aeb)e$. The fact that e is an identity element follows from the fact that e is an idempotent.

Clearly $1A1 = A$. Now suppose $eAe = A$. Then in particular there is $a \in A$ such that $eae = 1$. So e is an invertible idempotent, so $e = 1$. □

Note that (unless $e = 1$) eAe is *not* a subalgebra of A, since it has a different identity element.

Proposition 3.3. *Suppose A is an algebra and $e \in A$ is an idempotent. The following are equivalent.*

1. *e is a primitive idempotent in A.*
2. *e is a primitive idempotent in eAe.*
3. *e is the only non-zero idempotent in eAe.*

Proof.

(2⇒1) Suppose (1) is not true, so that we can write $e = f + g$ where f, g are non-zero orthogonal idempotents in A. Multiplying both sides on the right by f, we get $ef = f$; similarly $fe = f$, so $f = efe \in eAe$. Similarly $g \in eAe$, so we can write e as the sum of non-zero orthogonal idempotents in eAe, so e is not primitive in eAe.

(3⇒2) This is trivial.

(1⇒3) Suppose e is not the only non-zero idempotent in eAe, and let f be another one. Note that $ef = fe = f$, since e is the identity element of eAe. Let $g = e - f$. Then

$$g^2 = (e-f)^2 = e^2 - ef - fe + f^2 = e - f - f + f = g$$

and

$$fg = f(e-f) = fe - f^2 = f - f = 0$$

and similarly $gf = 0$. Also g is non-zero because $f \neq e$, so we can write e as a sum $f + g$ of two orthogonal non-zero idempotents, so e is not primitive. □

There is a connection between idempotents and direct sums. Suppose M is an A-module and ϵ is an idempotent in $\mathrm{End}_A(M)$. Then we have a decomposition

$$M = \mathrm{im}(\epsilon) \oplus \ker(\epsilon)$$

as A-modules (exercise). These two summands are both non-zero unless ϵ is the identity or the zero map. Conversely, if U and V are submodules of M with $M = U \oplus V$, we get an idempotent endomorphism $\epsilon : u \oplus v \mapsto u \oplus 0$.

As a consequence, we see that M is indecomposable if and only if there are no idempotents in $\mathrm{End}_A(M)$ apart from id_M and the zero map. If we consider the special case $M = {}_AA$, we see (using Proposition 1.6) that ${}_AA$ is indecomposable if and only if A has no non-trivial idempotents.

Now we consider the connection between idempotents and direct sum decompositions of algebras. Suppose B and C are algebras, and consider the algebra $B \oplus C$. The element $1_B \oplus 0_C$ in this algebra is an idempotent, and is also *central*, i.e. lies in the centre of $B \oplus C$. Similarly $0_B \oplus 1_C$ is a central idempotent, and the sum of these two idempotents is the identity element $1_B \oplus 1_C$.

We will now show that the reverse is true, i.e. a central idempotent in an algebra A gives a direct sum decomposition of A. Note that when e is a central idempotent in A then $eAe = eA = Ae$.

Proposition 3.4. *Suppose A is an algebra and e is a central idempotent in A. Then there is an algebra isomorphism*

$$\begin{aligned} \phi : A &\longrightarrow Ae \oplus A(1-e) \\ a &\longmapsto ae \oplus a(1-e). \end{aligned}$$

Proof. It is easy to check that ϕ is $\mathbb{F}$-linear; the fact that it is an algebra homomorphism follows from the fact that e is a central idempotent. To see that ϕ is injective, suppose $\phi(a) = 0 \oplus 0$. Then $ae = a(1-e) = 0$, and adding gives $0 = a(e+1-e) = a$. Finally we show that ϕ is surjective: an arbitrary element $be \oplus c(1-e)$ of $Ae \oplus A(1-e)$ can be written as $\phi(be + c(1-e))$. □

When e is a central idempotent in A, we abuse notation by identifying A with $Ae \oplus A(1-e)$ via the isomorphism above.

Corollary 3.5. *Suppose A is an algebra. Then A is an indecomposable algebra if and only if 1 is a primitive central idempotent, i.e. a primitive idempotent in $Z(A)$.*

We can extend this to more than two summands: if we can write 1 as a sum of orthogonal central idempotents $e_1, \ldots, e_r$, then there is a corresponding decomposition $A \cong Ae_1 \oplus \cdots \oplus Ae_r$. If 1 has a primitive decomposition in $Z(A)$, then we can write A as a direct sum of indecomposable algebras. If A is finite-dimensional, then $Z(A)$ is also finite-dimensional, so by Proposition 3.1 there is such a decomposition. In fact, there is only one, as we shall see in the next theorem. First we need a simple lemma.

Lemma 3.6. *Suppose A is an algebra. Then any two primitive central idempotents in A are either orthogonal or equal.*

Proof. Suppose e and f are primitive central idempotents. Then $e = e1 = ef + e(1-f)$, with ef and $e(1-f)$ both being central idempotents. Since e is a primitive central idempotent, it cannot be written as a sum of two non-zero central idempotents, so either $ef = 0$ or $e(1-f) = 0$. Applying the same reasoning to ef and $(1-e)f$, we find that either $ef = 0$ or $(1-e)f = 0$. So either $ef = 0$ (in which case $fe = 0$, so e and f are orthogonal), or $f = ef = e$. □

Theorem 3.7. *Suppose A is an algebra, and that E is a primitive decomposition of 1 in $Z(A)$.*

1. *E is the unique primitive decomposition of 1 in $Z(A)$.*
2. *E consists of all the primitive central idempotents in A.*
3. *A has only finitely many central idempotents.*

Proof. The elements of E are primitive central idempotents in A, and we claim that every primitive central idempotent lies in E, which proves (1) and (2). If f is a primitive central idempotent not in E, then by Lemma 3.6 f is orthogonal to every element of E. But then

$$f = 1f = \sum_{e \in E} ef = 0,$$

a contradiction. So E does contain every primitive central idempotent in A.

For the last part, suppose g is a central idempotent in A, and consider the elements ge, for $e \in E$. Using the same argument as in the proof of Lemma 3.6, we have either $ge = e$ or $ge = 0$ for each $e \in E$. If we let $F = \{e \in E \mid ge = e\}$, then

$$g = g1 = \sum_{e \in E} ge = \sum_{e \in F} e.$$

So every central idempotent can be written as a sum of distinct elements of E. So the number of central idempotents is $2^{|E|}$. □

In view of Theorem 3.7, we see that if A has a direct sum decomposition $A = A_1 \oplus \cdots \oplus A_r$ with $A_1, \ldots, A_r$ being indecomposable algebras, then this decomposition is unique: $A_1, \ldots, A_r$ must be the algebras $Ae_1, \ldots, Ae_r$, where $e_1, \ldots, e_r$ are the primitive central idempotents in A. These indecomposable algebras are called the *blocks* of A, and the primitive central idempotents are sometimes called the *block idempotents*.

Let's see how blocks and modules interact. Suppose A is an algebra, and e is a central idempotent in A. Then as above we have an algebra decomposition $A = Ae \oplus A(1-e)$. If M is an A-module, then we also have a module decomposition $M = eM \oplus (1-e)M$. Note that e acts as the identity on the summand eM, and hence eM can be viewed as a module for the algebra Ae; on the other hand, this summand is annihilated by $A(1-e)$, since $(1-e)e = 0$. Similarly, the summand $(1-e)M$ is naturally a module for $A(1-e)$ and is annihilated by Ae.

Conversely, suppose N is an Ae-module and P is an $A(1-e)$-module. Then the vector space $N \oplus P$ is naturally a module for A, via

$$a(n \oplus p) = aen \oplus a(1-e)p.$$

So we see that when e is a central idempotent in A, every A-module is just a direct sum of an Ae-module and an $A(1-e)$-module. In particular, an indecomposable A-module is either an indecomposable Ae-module or an indecomposable $A(1-e)$-module.

Of course, all this extends to more than two summands: if we have a decomposition $A = Ae_1 \oplus \cdots \oplus Ae_r$ (where $e_1, \ldots, e_r$ are orthogonal central idempotents) then an A-module decomposes as a direct sum $e_1M \oplus \cdots \oplus e_rM$, where e_iM is an Ae_i-module which is annihilated by the other Ae_js. In particular, if M is indecomposable, then $M = e_iM$ for some i.

In the case where 1 has a primitive decomposition in $Z(A)$ and $A = Ae_1 \oplus \cdots \oplus Ae_r$ is the decomposition of A into blocks, we say that a module M *lies in* or *belongs to* Ae_i if $M = e_iM$. Every indecomposable module must lie in some block; so to understand the indecomposable modules for A, we just need to understand the indecomposable modules for the blocks of A.

Now we return to Wedderburn's Theorem. We begin with a lemma.

Lemma 3.8. *If A is an indecomposable algebra and $n \in \mathbb{N}$, then $\mathrm{Mat}_n(A)$ is an indecomposable algebra.*

Proof. The centre of $\mathrm{Mat}_n(A)$ consists of all scalar matrices aI where $a \in Z(A)$. Hence $Z(\mathrm{Mat}_n(A)) \cong Z(A)$ as algebras; since $Z(A)$ contains no idempotents other than 0 and 1, neither does $Z(\mathrm{Mat}_n(A))$. □

Now we can show that the decomposition in Wedderburn's Theorem is unique, i.e. if A is an algebra and $A \cong \bigoplus_{i=1}^r \mathrm{Mat}_{n_i}(D_i)$ with each D_i a division algebra, then the integers $n_1, \ldots, n_r$ and the division algebras $D_1, \ldots, D_r$ are uniquely determined.

It follows from Lemma 3.8 each $\mathrm{Mat}_{n_i}(D_i)$ is an indecomposable algebra, so if we write $A = A_1 \oplus \cdots \oplus A_r$ with $A_i \cong \mathrm{Mat}_{n_i}(D_i)$ for each i, then $A_1, \ldots, A_r$ are the blocks of A, and these are uniquely determined. It then remains to show that if D and E are division algebras with $\mathrm{Mat}_n(D) \cong \mathrm{Mat}_m(E)$, then $m = n$ and $D \cong E$. The fact that $D \cong E$ comes from Theorem 2.6, since D^{op} is isomorphic the endomorphism algebra of the unique simple $\mathrm{Mat}_n(D)$-module. Now the fact that $m = n$ follows by considering dimensions.

4 The Jacobson radical

Now we consider algebras which are not semisimple. A non-semisimple algebra A has a certain ideal called the *Jacobson radical* which (if A is finite-dimensional) measures how far A is from being semisimple.

Definition. Suppose A is an algebra and M is an A-module. If X is a subset of M, the *annihilator* of X is the set

$$\mathrm{Ann}(X) = \{ a \in A \mid aX = 0 \}.$$

If X just consists of a single element x, then we usually write $\mathrm{Ann}(x)$ instead of $\mathrm{Ann}(\{x\})$.

Note that the annihilator of X is a left ideal in A. If X is a submodule of M, then $\mathrm{Ann}(X)$ is also a right ideal of A.

Definition. Suppose A is an algebra. The *Jacobson radical* of A is the intersection of the annihilators of all the simple A-modules. We write $J(A)$ for the Jacobson radical of A.

We'll see several equivalent definitions of $J(A)$. From now on, whenever we consider an algebra A, we will write J for $J(A)$.

Lemma 4.1. *Suppose A is an algebra and M is an A-module. Then JM is contained in every maximal submodule of M. Hence if M is finite-dimensional and non-zero, then $JM < M$.*

Proof. Suppose N is a maximal submodule of M. Then M/N is a simple module, so $J(M/N) = 0$, which is the same as saying that $JM \subseteq N$.

If M is finite-dimensional and non-zero, then M has at least one maximal submodule N (just take a proper submodule of largest possible dimension), so $JM \leqslant N < M$. □

Corollary 4.2 (Nakayama's Lemma)**.** *Suppose A is an algebra and M is a finite-dimensional A-module. If $N < M$, then $N + JM < M$.*

Proof. Since $N < M$, we can find a maximal submodule $L < M$ such that $N \leqslant L$. But by Lemma 4.1 $JM \leqslant L$, so $N + JM \leqslant L$. □

Proposition 4.3. *Suppose A is a finite-dimensional algebra. Then J is the intersection of all the maximal left ideals of A. Moreover, there is a finite set $\{I_1, \ldots, I_r\}$ of maximal left ideals of A such that $J = I_1 \cap \cdots \cap I_r$.*

Proof. Let N be the intersection of all the maximal left ideals of A. By Lemma 4.1 (with $M = {}_AA$) J is contained in every maximal left ideal, so is contained in N. If J is properly contained in N, then there is a simple A-module S which is not annihilated by N. Hence in particular there is $s \in S$ such that $Ns \neq 0$. Since $N \leqslant_{\mathrm{L}} A$, Ns is a submodule of S, so (since S is simple) $Ns = S$. Hence there is $n \in N$ such that $ns = s$. This means that $1 - n \in \mathrm{Ann}(s)$, which is a proper left ideal of A. Since A is finite-dimensional, we can find a maximal left ideal I containing $\mathrm{Ann}(s)$, so $1 - n \in I$. But also $n \in I$ (since n is contained in every maximal left ideal of A), and hence $1 \in I$, so $I = A$. Contradiction.

For the second part, let $\hat{J}$ be the left ideal of smallest dimension which can be written as the intersection of finitely many maximal left ideals of A. Then $\hat{J} \supseteq J$, and if $\hat{J} \supset J$, then there is some maximal left ideal I which does not contain $\hat{J}$. But then $\hat{J} \cap I$ is a smaller left ideal which can be written as the intersection of finitely many maximal left ideals; contradiction. So $\hat{J} = J$. □

We remark that the first statement in Proposition 4.3 holds more generally – for any ring, not just for a finite-dimensional algebra – but this relies on Zorn's Lemma (to show that every proper left ideal is contained in a maximal left ideal).

It would appear that the definition of J is asymmetric – it is phrased in terms of (left) modules, or (via Proposition 4.3) left ideals. So there ought to be a corresponding 'right Jacobson radical'. In fact we'll see that this is the same as J, using nilpotent ideals.

Definition. Suppose A is an algebra and $I \trianglelefteqslant A$. For any $n \geqslant 0$ we define

$$I^n = \{ a_1 \dots a_n \mid a_1, \dots, a_n \in I \}.$$

We say I is *nilpotent* if $I^n = 0$ for some n.

Lemma 4.4. *Suppose A is an algebra and $I \trianglelefteqslant A$ is nilpotent. Then $IS = 0$ for every simple A-module S. Hence $I \subseteq J$.*

Proof. Take n such that $I^n = 0$. Then

$$S = I^0 S \geqslant IS \geqslant I^2 S \geqslant \cdots \geqslant I^n S = 0.$$

But S has only two submodules (S and 0), so there is some m such that $I^m S = S$ while $I^{m+1} S = 0$. But then

$$IS = I(I^m S) = I^{m+1} S = 0. \qquad \square$$

Proposition 4.5. *Suppose A is a finite-dimensional algebra. Then J is nilpotent.*

Proof. Applying Lemma 4.1 repeatedly, we have $\dim(J^m M) \leqslant \dim(M) - m$ for any m. Apply this to $M = {}_A A$, and observe that $J^m = J^m A$, so that $J^{\dim(A)} = 0$. $\square$

Now we can give some equivalent definitions of the Jacobson radical.

Corollary 4.6. *Suppose A is a finite-dimensional algebra. Then J equals:*

- *the unique maximal nilpotent ideal in A;*
- *the intersection of the annihilators of all the simple right A-modules;*
- *the intersection of all the maximal right ideals of A.*

Proof. By Lemma 4.4 and Proposition 4.5 J is nilpotent and contains every nilpotent ideal, so is the unique maximal nilpotent ideal of A. Since this description of J is left–right symmetric, we can repeat everything with the intersection of the annihilators of all the simple right modules and the intersection of all the maximal right ideals, and find that these also equal the maximal nilpotent ideal of A, i.e. J. $\square$

Now we look at the connection between the Jacobson radical and semisimplicity.

Proposition 4.7. *Suppose A is a finite-dimensional algebra. Then ${}_A A / J$ is a semisimple module. Hence A is a semisimple algebra if and only if $J = 0$.*

Proof. By Proposition 4.3 we can write $J = I_1 \cap \cdots \cap I_r$ with $I_1, \ldots, I_r$ maximal left ideals. Then we have an injective homomorphism

$$\begin{aligned} \frac{{}_AA}{J} &\longrightarrow \frac{{}_AA}{I_1} \oplus \cdots \oplus \frac{{}_AA}{I_r} \\ a+J &\longmapsto a+I_1 \oplus \cdots \oplus a+I_r. \end{aligned}$$

So ${}_AA/J$ is isomorphic to a submodule of ${}_AA/I_1 \oplus \cdots \oplus {}_AA/I_r$, which is semisimple, so ${}_AA/J$ is semisimple.

In particular, if $J = 0$, then ${}_AA$ is a semisimple module, so A is a semisimple algebra. Conversely, if ${}_AA$ is a semisimple module, then $J = JA = 0$, since J annihilates every simple module. □

Now we consider an A-module M, and look at the submodule JM.

Proposition 4.8. *Suppose A is a finite-dimensional algebra and M is an A-module. Then $JM = 0$ if and only if M is semisimple.*

Proof. Since J annihilates every simple module, it annihilates every semisimple module, so $JM = 0$ if M is semisimple.

Conversely, suppose $JM = 0$. Note that M is the sum of all the submodules Am, where $m \in M$; so to show that M is semisimple we just need to show that each Am is semisimple.

There is a surjective homomorphism

$$\begin{aligned} \phi : {}_AA &\longrightarrow Am \\ a &\longmapsto am \end{aligned}$$

by assumption J lies in the kernel of this homomorphism. So $Am \cong {}_AA/\ker(\phi)$ is isomorphic to a quotient of ${}_AA/J$, which is semisimple; so Am is semisimple too. □

Corollary 4.9. *Suppose A is a finite-dimensional algebra and M is an A-module. Then JM is the smallest submodule of M such that M/JM is semisimple i.e. if $N \leqslant M$ with M/N semisimple, then $N \geqslant JM$.*

Proof. If M/N is semisimple, then by Proposition 4.8 $J(M/N)$ is zero, which is the same as saying $JM \leqslant N$. □

As a special case (taking $M = {}_AA$) we see that A/J is a semisimple A-module, and hence a semisimple A/J-module, and so A/J is a semisimple algebra. And Corollary 4.9 implies that J is minimal with this property.

Moreover, A/J has exactly the same simple modules as A, as we now show. In general, given an ideal I in A, any A/I-module naturally becomes an A-module (via $am = (a+I)m$ which is annihilated by I. Conversely, every A-module annihilated by I can naturally be made into an A/I-module. This procedure respects submodules, so it sends simple modules to simple modules. In the case where $I = J$, every simple A-module is annihilated by J, so simple modules of A/J correspond to simple modules of A.

So if you have an algebra and you're only interested in its simple modules, then quotienting out J is a way of getting rid of the non-semisimplicity while preserving the simple modules.

5 Local algebras and indecomposable modules

Lemma 5.1. *Suppose A is an algebra and ${}_AA = U \oplus V$ as modules. Then there is an idempotent $e \in A$ such that $U = Ae$ and $V = A(1-e)$.*

Proof. First of all the fact that $A = U + V$ means that we can write $1 = e + (1-e)$ where $e \in U$ and $1 - e \in V$. Now observe that

$$U \geqslant Ae \ni (1-e)e = e - e^2 = e(1-e) \in A(1-e) \leqslant V.$$

But $U \cap V = 0$, so $e - e^2 = 0$, i.e. e is idempotent.

We have $Ae \leqslant U$ and $A(1-e) \leqslant V$ with $A = U \oplus V$. But $A = Ae + A(1-e)$, since every $a \in A$ can be written $a = ae + a(1-e)$, so in fact $Ae = U$ and $A(1-e) = V$. □

As a consequence we see that ${}_AA$ is indecomposable if and only if 1 is a primitive idempotent in A. We give a name to this property.

Definition. Suppose A is a non-trivial algebra. A is *local* if 1 is a primitive idempotent in A.

In fact, there are many other characterisations of a local algebra in the finite-dimensional case: one can prove that a non-zero finite-dimensional A is local if and only if any of the following hold:

- ${}_AA$ is indecomposable;
- the set of non-invertible elements of A is an ideal;
- A has a unique maximal left ideal;
- A/J is a division algebra;
- every element of A is either invertible or nilpotent.

We will assume that the last of these conditions from from A being local (we won't need the other characterisations).

Proposition 5.2. *Suppose A is a local finite-dimensional algebra, and $I \lhd A$. Then A/I is local.*

Proof. Supposing that A/I is not local, there is an idempotent $a + I$ in A/I other than $1 + I$ or $0 + I$. We will show that we can 'lift' this idempotent to A, i.e. there is an idempotent $e \in A$ such that $e + I = a + I$.

The fact that $a + I$ is an idempotent means that $a^2 - a \in I$. So $a^2 - a$ is not invertible (because otherwise 1 would be in I, so that $I = A$) and so (using the fact we're taking for granted above) $a^2 - a$ is nilpotent, so there is n such that $(a^2 - a)^n = 0$. This equation can be re-written as $a^n = a^{n+1}b$ for some $b \in A$ with $ab = ba$. Let $e = a^n b^n$. Then $eab = e$, and hence $e = e(ab)^n = e^2$.

So we've found an idempotent $e \in A$, but we have to show that $e + I = a + I$. Since $a + I$ is idempotent, we have $a + I = a^k + I$ for all k, so that

$$a + I = a^n + I = a^{n+1}b + I = (a^{n+1} + I)(b + I) = (a + I)(b + I) = ab + I$$

and this gives

$$a + I = (a + I)^n = (ab + I)^n = e + I.$$

So A contains an idempotent e, and the fact that $e + I = a + I$ means that $e \neq 0, 1$, contradicting the fact that A is local. □

Our aim is to consider the modules Ae for e a primitive idempotent, and show that these are in bijection with simple modules.

Proposition 5.3. *Suppose A is an algebra, and $e \in A$ is idempotent. Then* $\mathrm{End}_A(Ae) \cong (eAe)^{\mathrm{op}}$.

Proof. Given $ebe \in eAe$, there is an endomorphism ϕ_{ebe} of Ae given by $ae \mapsto aebe$. So we have a map

$$\begin{aligned} eAe &\longrightarrow \mathrm{End}_A(Ae) \\ ebe &\longmapsto \phi_{ebe} \end{aligned}$$

and it is easy to check that this is an algebra homomorphism $(eAe)^{\mathrm{op}} \to \mathrm{End}_A(Ae)$. It has an inverse

$$\begin{aligned} \mathrm{End}_A(Ae) &\longrightarrow eAe \\ \phi &\longmapsto \phi(e) \end{aligned}$$

and so is a bijection. □

Corollary 5.4. *Suppose A is a finite-dimensional algebra and $e \in A$ is a primitive idempotent. Then Ae/Je is a simple A-module, and is the unique simple quotient of Ae.*

Proof. From Corollary 4.9 Ae/Je is semisimple. So we just need to show that Ae/Je is indecomposable, since an indecomposable semisimple module is simple. We saw in Section 3 that a module M is indecomposable if and only if $\mathrm{End}_A(M)$ is local, so we need to show that $\mathrm{End}_A(Ae/Je)$ is local.

We claim that $\mathrm{End}_A(Ae/Je)$ is isomorphic to a quotient of $\mathrm{End}_A(Ae)$. Given $\phi \in \mathrm{End}_A(Ae)$, we have $\phi(Je) \subseteq Je$, so we can define $\bar{\phi} \in \mathrm{End}_A(Ae/Je)$ by $\bar{\phi}(ae + Je) = \phi(ae) + Je$. So we have a homomorphism

$$\begin{aligned} \mathrm{End}_A(Ae) &\longrightarrow \mathrm{End}_A(Ae/Je) \\ \phi &\longmapsto \bar{\phi} \end{aligned}$$

and it is easy to check that this is surjective. So $\mathrm{End}_A(Ae/Je)$ is isomorphic to a quotient of $\mathrm{End}_A(Ae)$. Since e is primitive, the algebra eAe is local (Proposition 3.3), so $\mathrm{End}_A(Ae) \cong (eAe)^{\mathrm{op}}$ is local, and so by Proposition 5.2 $\mathrm{End}_A(Ae/Je)$ is local, as required.

For the second statement, the fact that Ae/Je is simple implies that Je is a maximal submodule of Ae; we need to show that there are no other maximal submodules. Suppose N is a maximal submodule of Ae; then Ae/N is simple, so $J(Ae/N) = 0$, i.e. $Je \leqslant N$. Since Je is a maximal submodule of Ae, this gives $Je = N$. □

The idea is that the modules Ae (where e is a primitive idempotent) are as important as the simple modules, and are in a kind of duality with the simple modules. Corollary 5.4 allows us to define a function from the set of (isomorphism classes of) modules Ae to the set of simple modules via $Ae \mapsto Ae/Je$, and we will see that this is a bijection. First we show that it is surjective.

Proposition 5.5. *Suppose A is a finite-dimensional algebra and S is a simple A-module. Then there is a primitive idempotent $e \in A$ such that $Ae/Je \cong S$.*

Proof. Let E be a primitive decomposition of 1 in A. Since $1S = S \neq 0$, there must be some $e \in E$ and $s \in S$ such that $es \neq 0$. Define a homomorphism

$$\begin{aligned} \phi : Ae &\longrightarrow S \\ ae &\longmapsto aes. \end{aligned}$$

ϕ is non-zero, so must be surjective since S is simple. So S is isomorphic to a simple quotient of Ae, so by the second statement in Corollary 5.4 $S \cong Ae/Je$. □

6 Projective modules

In this section we consider the module $F_n = {}_AA^{\oplus n}$ for $n \geqslant 0$. In this module we write 1_i for the element $0 \oplus \cdots \oplus 0 \oplus 1 \oplus 0 \oplus \cdots \oplus 0$, with the 1 in the ith position.

Lemma 6.1. *Suppose A is an algebra and M is a finite-dimensional A-moduleand $m_1, \ldots, m_n \in M$. Then there is a unique homomorphism $\phi : F_n \to M$ such that $\phi(1_i) = m_i$ for each i. Hence M is isomorphic to a quotient of F_n for some n.*

Proof. ϕ can be (and must be) defined by

$$\phi(a_1 \oplus \cdots \oplus a_n) = a_1m_1 + \cdots + a_nm_n.$$

For the second part, if we take $\{m_1, \ldots, m_n\}$ to be a generating set for M, then the homomorphism ϕ above is surjective, so by the First Isomorphism Theorem M is isomorphic to a quotient of F_n. □

Definition. Suppose A is an algebra and P is a finite-dimensional A-module. P is *projective* if there is an A-module Q such that $P \oplus Q \cong F_n$ for some n.

A key example of a projective module is the module Ae for $e \in A$ idempotent. This is projective since $F_1 = {}_AA = Ae \oplus A(1-e)$.

Lemma 6.2. *Suppose A is an algebra and e is an idempotent in A. Then Ae is an indecomposable module if and only if e is primitive.*

Proof. If e is not primitive, say if $e = f + g$ with f and g orthogonal idempotents, then $Ae = Af \oplus Ag$, so Ae is decomposable.

Conversely, suppose Ae is decomposable, say $Ae = P \oplus Q$ with $P, Q \neq 0$. Then

$$Ae/Je = (P \oplus Q)/J(P \oplus Q) \cong P/JP \oplus Q/JQ$$

with P/JP and Q/JQ both non-zero by Lemma 4.1. Hence Ae/Je is not simple, so by Corollary 5.4 e is not primitive. □

In fact, every indecomposable projective A-module is isomorphic to Ae for some primitive idempotent $e \in A$. (This requires the Krull–Schmidt Theorem, which says that a decomposition of a module as a direct sum of indecomposable modules is unique up to isomorphism.)

Now here are some equivalent conditions to the projective property.

Proposition 6.3. *Suppose A is an algebra and P is an A-module. The following are equivalent.*

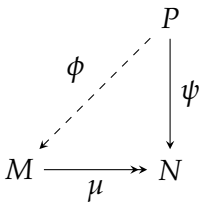
1. *P is projective.*
2. *If M and N are A-modules, $\mu : M \to N$ is a surjective homomorphism and $\psi : P \to N$ is a homomorphism, then there is a homomorphism $\phi : P \to M$ such that $\mu \circ \phi = \psi$.*
3. *If M is an A-module and $\mu : M \to P$ is a surjective homomorphism, then there is a homomorphism $\phi : P \to M$ such that $\mu \circ \phi = \mathrm{id}_P$.*

Proof.
(1⇒2) Take an A-module Q such that $F = P \oplus Q$ is free, and let X be a basis for F. Extend ψ to a homomorphism from F to N by mapping Q to 0. For any $x \in X$ we have $\psi(x) \in N$, and since μ is surjective we can choose $m_x \in M$ such that $\mu(m_x) = \psi(x)$. So we have a function from X to M given by $x \mapsto m_x$, and by Lemma 6.1 there is a homomorphism $\phi : F \to M$ such that $\phi(x) = m_x$ for each x. Hence $\mu(\phi(x)) = \psi(x)$ for each x. But by the uniqueness in Lemma 6.1 we have $\mu \circ \phi = \psi$. Now restrict ϕ to P to get the desired homomorphism.

(2⇒3) (3) is just a special case of (2), taking $N = P$ and $\psi = \mathrm{id}_P$.

(3⇒1) By Lemma 6.1 we can find a free A-module F and a surjective homomorphism $\mu : F \to P$. By (3), there is a homomorphism $\phi : P \to F$ such that $\mu \circ \phi = \mathrm{id}_P$. This means in particular that ϕ is injective, so we can identify P with $\mathrm{im}(\phi)$. It is easy to check that $F = \ker(\mu) \oplus \mathrm{im}(\phi) = \ker(\mu) \oplus P$, so P is projective. □

Condition (2) in the above proposition is often illustrated by the following diagram.



Here the double-headed arrow indicates a surjective homomorphism, and the dashed arrow indicates the map whose existence property (2) guarantees. Note that in (3) we always have $M = \mathrm{im}(\phi) \oplus \ker(\mu)$ (exercise).

Recall that above we defined a surjective function

$$\{\text{indecomposable projective modules}\} \longrightarrow \{\text{simple modules}\}$$
$$Ae \longmapsto Ae/Je.$$

Now we can show that this function is injective as well.

Proposition 6.4. *Suppose A is an algebra and S is a simple A-module. If P and Q are projective A-modules such that $P/JP \cong Q/JQ \cong S$, then $P \cong Q$.*

Proof. The fact that $P/JP \cong Q/JQ \cong S$ means that there are surjective homomorphisms $\pi : P \to S$ and $\rho : Q \to S$ such that $\ker(\pi) = JP$ and $\ker(\rho) = JQ$. Since P is projective, we can find a homomorphism $\phi : P \to Q$ such that $\rho \circ \phi = \pi$; we need to show that ϕ is an isomorphism.

First we show that ϕ is surjective. Given $q \in Q$, take $p \in P$ such that $\pi(p) = \rho(q)$. Then $q - \phi(p) \in \ker(\rho)$, so $q \in \mathrm{im}(\phi) + \ker(\rho)$. So $Q = \mathrm{im}(\phi) + \ker(\rho) = \mathrm{im}(\phi) + JQ$, so by Nakayama's Lemma $Q = \mathrm{im}(\phi)$, i.e. ϕ is surjective. Now the fact that Q is projective means that there is a homomorphism $\psi : Q \to P$ such that $\phi \circ \psi = \mathrm{id}_Q$. As observed above this means that $P = \mathrm{im}(\psi) \oplus \ker(\phi)$. But P is indecomposable (because $P/JP \cong S$ which is indecomposable) and $\mathrm{im}(\psi) \neq 0$, so $\ker(\phi) = 0$, and hence ϕ is an isomorphism. □

7 Representation theory of finite groups

In this section we let G be a finite group, and consider $\mathbb{F}G$-modules. Now we have three special constructions for modules.

The trivial module: Let $M = \mathbb{F}$, and make this an $\mathbb{F}G$-module by setting $gm = m$ for all $g \in G$ and $m \in M$.

Dual modules: If M is an $\mathbb{F}G$-module, let M^* be the dual vector space, i.e. $\mathrm{Hom}_{\mathbb{F}}(M, \mathbb{F})$. Then we can make M^* into an $\mathbb{F}G$-module via

$$(g\phi)(m) = \phi(g^{-1}m) \qquad \text{for all } g \in G,\ m \in M,\ \phi \in M^*.$$

(More generally we can do this whenever we have an algebra A with an *anti-automorphism*, i.e. an isomorphism $A \to A^{\mathrm{op}}$.)

Tensor products of modules: If M, N are $\mathbb{F}G$-modules, we can make $M \otimes N$ into an $\mathbb{F}G$-module via

$$g(m \otimes n) = (gm) \otimes (gn) \qquad \text{for all } g \in G,\ m \in M,\ n \in N.$$

(Be careful – this does not imply that $a(m \otimes n) = (am) \otimes (an)$ for all $a \in \mathbb{F}G$.)

Theorem 7.1 (Maschke's Theorem)**.** *Suppose $\mathbb{F}$ has characteristic zero. Then $\mathbb{F}G$ is a semisimple algebra.*

Proof. We need to show that ${}_{\mathbb{F}G}\mathbb{F}G$ is a semisimple module, and we do this using the complement property. So suppose $N \leqslant {}_{\mathbb{F}G}\mathbb{F}G$. We can certainly find a vector subspace R of $\mathbb{F}G$ such that $\mathbb{F}G = N \oplus R$ as vector spaces. Let $\pi : {}_{\mathbb{F}G}\mathbb{F}G \to N$ be the canonical projection for this direct sum, and define $\overline{\pi} : \mathbb{F}G \to \mathbb{F}G$ by

$$\overline{\pi}(m) = \frac{1}{|G|} \sum_{g \in G} g^{-1}\pi(gm).$$

Then $\overline{\pi}$ is a homomorphism, since for any $h \in G$

$$\begin{aligned} \overline{\pi}(hm) &= \frac{1}{|G|} \sum_{g \in G} g^{-1}\pi(ghm) \\ &= \sum \frac{1}{|G|} \sum_{g \in G} hg^{-1}\pi(gm) && \text{replacing } g \text{ with } gh^{-1} \\ &= h\overline{\pi}(m). \end{aligned}$$

Note also that (since $N = \mathrm{im}(\pi)$ and N is closed under the action of G) $\mathrm{im}(\bar{)}\pi \subseteq N$. Also, since π acts as the identity on N, so does $\overline{\pi}$: for $n \in N$,

$$\overline{\pi}(n) = \frac{1}{|G|}\sum_{g\in G} g^{-1}\pi(gn) = \frac{1}{|G|}\sum_{g\in G} g^{-1}gn = n.$$

This implies that $\mathrm{im}(\bar{)}\pi = N$, and also that $\overline{\pi}^2 = \overline{\pi}$: for any $m \in \mathbb{F}G$ we have $\overline{\pi}(m) \in N$, and hence $\overline{\pi}(\overline{\pi}(m)) = \overline{\pi}(m)$.

Hence

$$\begin{aligned}\mathbb{F}G &= \mathrm{im}(\overline{\pi}) \oplus \ker(\overline{\pi}) \\ &= N \oplus \ker(\overline{\pi}).\end{aligned}$$ □

Using Wedderburn's Theorem, this implies that if $\mathbb{F}$ is an algebraically closed field of characteristic 0 then the number of simple $\mathbb{F}G$-modules equals $\dim(Z(\mathbb{F}G))$, which is the number of conjugacy classes in G. For arbitrary group algebras, the number of simple modules is at most the number of conjugacy classes in G.

Here's a result at the opposite extreme.

Proposition 7.2. *Suppose* $\mathrm{char}\,\mathbb{F}$ *is a prime* p*, and* $|G| = p^n$*. Then the only simple* $\mathbb{F}G$*-module is the trivial module.*

Proof. We use induction on n. Assuming $n > 0$, it is a basic fact from group theory that G has non-trivial centre. So take $1 \neq g \in Z(G)$. If M is any module, then (since $g \in Z(G)$) any eigenspace for the action of g on M is a submodule. So if M is simple then a non-zero eigenspace must be the whole of M, i.e. g acts as a scalar on M. Now in $\mathbb{F}G$ we have $0 = g^{p^n} - 1 = (g-1)^{p^n}$, so the only eigenvalue g can have is 1. Hence g acts as the identity on M. So if we let $N = \langle g\rangle \trianglelefteq G$, we can make M into a module for $\mathbb{F}(G/N)$ via

$$(hN)m = hm \qquad \text{for all } h \in G,\ m \in M.$$

M is then a simple $\mathbb{F}(G/N)$-module, so by induction is the trivial $\mathbb{F}(G/N)$-module. And hence M is the trivial $\mathbb{F}G$-module. □

Now here's a converse to Maschke's Theorem.

Proposition 7.3. *Suppose* $\mathrm{char}(\mathbb{F})$ *is a prime dividing* $|G|$*. Then* $\mathbb{F}G$ *is not semisimple.*

Proof. Let $a = \sum_{g\in G} g$. Then $\mathbb{F}a$ is an ideal in $\mathbb{F}G$, since $ga = ag = a$ for every $g \in G$. Furthermore, a^2 equals $|G|$ times a, but $|G|$ is zero in $\mathbb{F}$ by assumption, so $a^2 = 0$, and hence $\mathbb{F}a$ is a non-zero nilpotent ideal in $\mathbb{F}G$. By Lemma 4.4 $J(\mathbb{F}G)$ contains every nilpotent ideal, and so is non-zero, and hence $\mathbb{F}G$ is not semisimple. □