Introduction to Representation Theory - Week 3 - Decomposing Semisimple Rings

Antonio León Villares

October 2023

Contents

1 Recap and Important Theorems/Notation

1.1 Proposition: Simple Modules for Semisimple Rings

*Let A be a **semisimple ring**. Then, A has only **finitely** many **simple** A-**modules**, up to **isomorphism**.*
(Proposition 2.14)

1.2 Definition: Number of Isomorphism Classes

*For finite groups G, $r_k(G)$ denotes the number of **isomorphism classes** of **irreducible** k-**representations** of G.*
(Definition 2.16)

1.3 Lemma: Module Endomorphisms

*Let A be a **ring**. Then:*

1. *for each $a \in A$ **right multiplication** by a defines an A-**module endomorphism**:*
$$r_a : {}_A A \to {}_A A$$
given by:
$$b \mapsto ba$$
2. *Every A-**module endomorphism***
$$\omega : {}_A A \to {}_A A$$
is of this form
3. *The map:*
$$A^{op} \to \mathrm{End}_A({}_A A)$$
given by:
$$a \mapsto r_a$$
*is an **isomorphism** of rings*

(Lemma 3.4)

1.4 Remark: Central Elements Give Endomorphisms

Take any $z \in Z(A)$, and define an ***endomorphism****:*

$$z_V : V \to V$$

via:

$$v \mapsto z \cdot v$$

We can check that z_V is indeed an ***endomorphism****:*

$$\begin{aligned} z_V(a \cdot v) &= z \cdot (a \cdot v) \\ &= (za) \cdot v \\ &= (az) \cdot v \\ &= a \cdot z_V(v) \end{aligned}$$

1.5 Definition: k-Algebra

We say that A is a ***k-algebra*** *if it contains k as a* ***central subfield****. Moreover,* ***k-linear ring homomorphisms*** *are* ***homomorphisms of k-algebras****.*

If A is a ***semisimple ring****, we say that A is a* ***semisimple*** ***k-algebra****. (Definition 3.5)*

1.6 Theorem: Schur's Lemma

Suppose k is ***algebraically closed****. Let V be a* ***simple module*** *over a* ***finite dimensional*** ***k-algebra*** *A.*
Then, every ***A-module endomorphism*** *of V is given by the action of some* ***scalar*** *$\lambda \in K$, such that:*

$$\mathrm{End}_A(V) = k1_V$$

(Theorem 3.6)

1.7 Definition: Central Character of Modules

*Let A be a k-**algebra**, and V be an A-**module** where:*

$$\text{End}_A(V) = k1_V$$

*By **Schur's Lemma**, every $z \in Z(A)$ acts on V by **scalar multiplication**. Denote this action/endomorphism via z_V.*

---

*The **central character** of V is the **ring homomorphism**:*

$$Z(A) \to k$$
$$z \mapsto z_V$$

2 Notation for these Notes

- A will denote a **fixed semisimple ring**
- $V_1, \dots, V_r$ denotes a **complete** list of the r **representatives** for the **isomorphism classes** of **simple** A**-modules** (Proposition 2.14 above)
- we fix a **decomposition** of A as a **direct sum**[1] of **simple left ideals**:

  $$A = \bigoplus_{i=1}^{r} \bigoplus_{j=1}^{n_i} L_{i,j}$$

  where each **left ideal** $L_{i,j}$ is such that:

  $$\forall i, j, \quad L_{i,j} \cong V_i$$

  we have that $n_1, \dots, n_r \geq 1$, since each V_i must appear **at least** once within the decomposition
- each $L_{i,j}$ is **not unique** in general
- we define **left ideals** B_i via:

  $$B_i = \bigoplus_{j=1}^{n_i} L_{i,j}$$

  B_i is a left ideal because sum of left ideals are left ideals (see this proof)

3 Examples of Semisimple Rings

- any **division ring** D is **semisimple**
  - in particular, if D is a simple ring, it is semisimple (since it decomposes trivially as a sum of simle rings - D itself)

[1]Being a direct sum, each $a \in A$ is uniquely expressible as a sum of elements in $L_{i,j}$.

  - if D isn't simple, then there exists some non-trivial ideal I; in particular, $\exists a \in I$, where a is non-zero
  - since D is a division ring, $\exists a^{-1} \in D$, which implies that $aa^{-1} \in I$, so I contains the identity, and so, $I = D$

- any **matrix** over a **division ring** $M_n(D)$
  - for example, when $n = 2$:

$$\begin{pmatrix} k & k \\ k & k \end{pmatrix} = \begin{pmatrix} k & k \\ k & k \end{pmatrix} \oplus \begin{pmatrix} 0 & k \\ 0 & k \end{pmatrix}$$

    where you can check that the ddecomposition is given by simple left ideals

- direct product of matrix rings over division rings:

$$M_{n_1}(D_1) \times \ldots \times M_{n_r}(D_r)$$

4 Dimension of the Centre of a Semisimple Ring

4.1 Proposition: Bounding Dimension of the Centre from Above

Let A be a ***finite dimensional semisimple*** k***-algebra****, and suppose that k is* ***algebraically closed****. Then:*

$$\dim(Z(A)) \leq r$$

(Proposition 3.9)

Proof. By Schur's Lemma

$$\forall i \in [1, r], \quad \text{End}_A(V_i) = k1_{V_i}$$

Define a k-linear map:

$$\psi : Z(A) \to k^r \quad \psi(z) = (z_{V_1}, \ldots, z_{V_r})$$

This is k-linear because each z_{V_i} is just scalar multiplication.

Now, pick any $z \in Z(A)$ such that:

$$\psi(z) = 0 \in k^r$$

This is possible if and only if:

$$\forall i \in [i, r], \quad z_{V_i} = 0 \in k$$

We claim that in such a case, $z = 0 \in A$.

A is semisimple, so in particular $\exists e_{i,j} \in L_{i,j}$ such that for $1 \in A$:

$$1 = \sum_{i=1}^{r} \sum_{j=1}^{n_i} e_{i,j}$$

so in particular:

$$z = z \cdot 1 = \sum_{i=1}^{r} \sum_{j=1}^{n_i} z \cdot e_{i,j} = \sum_{i=1}^{r} \sum_{j=1}^{n_i} z_{V_i} e_{i,j}$$

But we have that $z_{V_i} = 0$, which implies that $z = 0$. Hence, $\ker(\psi) = \{0\}$ and ψ is injective. That is:

$$\dim(Z(A)) \leq \dim(k^r) = r$$

as required.

□

4.2 Bounding Dimension of the Centre from Below

4.2.1 Lemma: A Decomposes into Two-Side Ideals

*Recall, A decomposes into **left ideals**:*

$$A = B_1 \oplus \ldots \oplus B_r$$

*In fact, each B_i is a **two-sided ideal** of A.*
(Lemma 3.11)

Proof. Fix $a \in A$. By definition, $L_{i,j} \subseteq B_i$. Now, consider the projection:

$$\varphi : A \to L_{\alpha,\beta}, \quad \alpha \neq i, 1 \leq \beta \leq n_\alpha$$

such that:

$$\varphi(a) = \varphi\left(\sum_{i=1}^{r} \sum_{j=1}^{n_i} \ell_{i,j}\right) = \ell_{\alpha,\beta}$$

Now, let r_a denote right multiplication by a in A. Then, we have that:

$$\varphi \circ r_a : A \to L_{\alpha,\beta}$$

If we restrict $\varphi \circ r_a$ to act on $L_{i,j}$ we thus have an A-module homomorphism:

$$\varphi \circ r_{a|L_{i,j}} : L_{i,j} \to L_{\alpha,\beta}$$

Since $i \neq \alpha$, and $L_{i,j} \cong V_i$, $L_{i,j}, L_{\alpha,\beta}$ aren't isomorphic. Hence, by

*Let V, W be **simple A-modules**. Then, every **non-zero, A-linear map***

$$\varphi : V \to W$$

*is an **isomorphism**.*
(Lemma 2.13)

it follows that

$$\varphi \circ r_{a|L_{i,j}} : L_{i,j} \to L_{\alpha,\beta}$$

is the zero map. In particular, $\forall \alpha \neq i$, the projection:

$$L_{i,j}a \to B_\alpha$$

must be zero. In particular, since $L_{i,j}a \subseteq A$, it must be the case that:

$$L_{i,j}a \subseteq B_i$$

But B_i is a direct sum of $L_{i,j}$ for varying j, so:

$$\forall a \in A, \quad B_i a \subseteq B_i$$

Closure of B_i under subtraction follows from the fact that B_i is already a left ideal. Hence, B_i is both a left and a right ideal, as required.

□

4.2.2 Lemma: Bounding Dimension of the Centre from Below

*Let R be a k-**algebra** and suppose that for some **non-zero, two-sided ideals** $S_1, \ldots, S_r$, we have that:*

$$R = S_1 \oplus \ldots \oplus S_r$$

Then,

$$\dim(Z(R)) \geq r$$

(Lemma 3.12)

Proof. We can write:

$$R \ni 1 = \sum_{i=1}^{r} e_i$$

Now, let $a \in R$., Since S_i is a left ideal:

$$ae_i \in S_i$$

However, it is also a right ideal, so:

$$e_i a \in S_1$$

Hence, decompoosing a we get that:

$$a = \sum_{i=1}^{r} ae_i = \sum_{i=1}^{r} e_i a$$

Since this decomposition is unique, and each term belongs to each of the S_i, we must have that:

$$\forall i \in [1, r], \forall a \in R, \quad ae_i = e_i a \implies e_i \in Z(A)$$

Now, we also have:

- if $i \neq j$, then using the fact that S_i are two-sided ideals:

$$e_i e_j \in S_i \cap S_j = \{0\} \implies e_i e_j = 0$$

- hence:

$$e_i = e_i \cdot 1 = e_i \sum_{j=1}^{r} = e_i^2$$

In other words, $\{e_i\}_{i \in [1,r]}$ forms a set of pairwise orthogonal idempotent elements of R.

We claim that this set is linearly independent. To this end, assume that:

$$\exists \lambda_i \in k \ : \ \sum_{i=1}^{r} \lambda_i e_i = 0 \in R$$

Multiplying this expression by e_j, and using the properties of each e_i:

$$0 = e_j \sum_{i=1}^{r} \lambda_i e_i = \lambda_j e_j$$

If $e_j = 0$, then $\forall a \in S_j, a = ae_j = 0$ which contradicts the fact that the S_j are non-zero ideals. Hence, we must have that

$$\forall j \in [1,r], \ e_j \neq 0 \implies \lambda = 0$$

so the set is indeed linearly independent over k. In particular, a basis is a minimal linearly independent spanning set, so:

$$r \leq \dim(Z(R))$$

as required.

□

4.3 Theorem: Dimension of Centre from Semisimple Ring Decomposition

Let A be a ***finite dimensional semisimple k-algebra****, and suppose that k is* ***algebraically closed****. Then:*

$$r = \dim(Z(A))$$

(Theorem 3.13)

Proof. Combine Proposition 3.9 and Lemma 3.11 ++ Proposition 3.12. □

In other words, the number of isomorphism classes of simple modules over some semisimble k-algebra is precisely the dimension fo the centre of A.

5 Conjugacy Classes

5.1 Definition: Number of Conjugacy Classes of a Group

For a ***finite group*** *G we denote with $s(G)$ the number of* ***conjugacy classes*** *of G.*
(Definition 3.14)

5.2 Conjugacy Class Sums

5.2.1 Definition: Conjugacy Class Sums

Let G be a ***finite group*** *with* ***conjugacy classes****:*

$$C_1, \dots, C_2$$

Define the ***conjugacy class sum*** *of C_i via:*

$$\hat{C}_i = \sum_{x \in C_i} x \in kG$$

That is, $\hat{C}_i$ is the ***formal sum*** *in kG containing all elements of the conjugacy class C_i.*
(Proposition 3.15)

5.2.2 Proposition: Conjugacy Class Sums Define Basis for Centre of Group Ring

Let G be a ***finite group*** *with* ***conjugacy classes****:*

$$C_1, \dots, C_2$$

Then,

$$\{\hat{C}_1, \dots, \hat{C}_2\}$$

is a ***basis*** *for $Z(kG)$ as a* ***vector space****, and thus:*

$$\dim(Z(kG)) = s(G)$$

(Proposition 3.15)

Proof. □

5.2.3 Corollary: Conjugacy Classes and Simple Submodules

*Let G be a **finite group**, with k an **algebraically closed field** and $|G| \neq 0$ in k. Then:*

$$r_k(G) = s(G)$$

(Corollary 3.16)

Proof. By repeatedly applying Maschke's Theorem:

Let

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

*be a **representation**, and let U be a G-**stable subspace**.*
*A G-**stable complement** for U in G is a G-**stable subspace** W such that:*

$$V = U \oplus W$$

where recall, this means that:

- $U + W = V$
- $U \cap W = \{0\}$

(Definition 1.19)

we see that we can write kG as a direct sum of simple subalgebras, and so, kG is semisimple. Then, by:

*Let G be a **finite group** with **conjugacy classes**:*

$$C_1, \dots, C_2$$

Then,

$$\{\hat{C}_1, \dots, \hat{C}_2\}$$

*is a **basis** for $Z(kG)$ as a **vector space**, and thus:*

$$\dim(Z(kG)) = s(G)$$

(Proposition 3.15)

we have that $Z(kG) = s(G)$. Finally by:

*Let A be a **finite dimensional semisimple k-algebra**, and suppose that k is **algebraically closed**. Then:*

$$r = \dim(Z(A))$$

(Theorem 3.13)

we have that $r_k(G) = s(G)$ as required.

□

5.3 Lemma: Decomposing Modules as Product of Rings

1. *Each B_i is a **ring** with **identity element** e_i*
2. *A is **isomorphic** to the **product** of rings (B_i, e_i):*

$$A \cong B_1 \times \ldots B_r$$

3. *Each B_i is itself a **semisimple ring**, with **unique** simple module V_i*

(Lemma 3.17)

Proof.

(1)

By

*Recall, A decomposes into **left ideals**:*

$$A = B_1 \oplus \ldots \oplus B_r$$

*In fact, each B_i is a **two-sided ideal** of A.*
(Lemma 3.11)

we can think of B_i as a subgroup of the additive group defining the ring A, and which is stable under multiplication by elements of A (since B_i is a two-sided ideal). Hence, in particular, it is a subset of A which is closed under addition and multiplication, and contains inverses. We are just missing the identity element. In the proof of

*Let R be a k-**algebra** and suppose that for some **non-zero, two-sided ideals** $S_1, \ldots, S_r$, we have that:*

$$R = S_1 \oplus \ldots \oplus S_r$$

Then,

$$\dim(Z(R)) \geq r$$

(Lemma 3.12)

we found an orthogonal idempotent basis for a k-algebra R via:

$$R \ni 1 = \sum_{i=1}^{r} e_i$$

We also saw that:

$$\forall a \in A, \ ae_i = e_i a$$

and that ae_i corresponds to the B_i component of a along the decomposition:

$$A = B_1 \oplus \ldots \oplus B_r$$

In particular, for any $a \in B_i$, we must have that:

$$ae_i = e_i a = a$$

which implies that e_i must be the multiplicative identity element in B_i.

(2)

We can define the isomorphism via:

$$\forall a \in A, a \mapsto (ae_1, \ldots, ae_r) \in B_1 \times \ldots \times B_r$$

(3)

We want to show that $L_{i,j}$ is a simple B_i module. To this end, suppose that U is a B_i-submodule of $L_{i,\ell}$. Then, for some $jneqi$ consider:

$$B_j U \subseteq B_j B_i = (B_j e_j)(e_i B_i) = B_j(e_j e_i) B_i = 0 \implies B_j U = 0$$

where we've used the fact that e_i forms an orthogonal set. Moreover, since U is a B_i-submodule (as $L_{i,j} \subseteq B_i$), we have that:

$$B_i U \leq U$$

Thus:

$$AU = \left(\bigoplus_{j=1}^{r} B_j \right) U \leq U$$

which implies that U is an A-submodule of $L_{i,\ell}$. But since $L_{i,\ell}$ is simple by definition:

$$U = L_{i,\ell} \text{ or } U = \{0\}$$

so $L_{i,\ell}$ is indeed a simple B_i-module aswell, and thus, B_i is semisimple. In particular, since $L_{i,j} \cong V_i$, it follows that V_i is the only simple B_i-module, up to isomorphism by:

*Let A be a **semisimple ring**. Then, A has only **finitely** many **simple** A**-modules**, up to **isomorphism**.*
(Proposition 2.14)

□

5.4 Proposition: Ring Isomorphism Between Left Modules and Matrices

*Let B be a **semisimple ring** with exactly one simple module V, up to **isomorphism**. Suppose that:*

$$B \cong \underbrace{V \oplus \ldots \oplus V}_{n \text{ times}}$$

is a left B-module, and let:

$$D = \mathrm{End}_B(V)$$

*Then there is a **ring isomorphism**:*

$$B \cong M_n(D^{op})$$

(Proposition 3.18)

Proof. Firstly, notice that if we think of B as a B-module, it follows that:

$$_B B \cong V^n$$

By part 3) of

Let A be a ***ring****. Then:*

1. *for each $a \in A$* ***right multiplication*** *by a defines an A-**module endomorphism**:*
$$r_a : {}_A A \to {}_A A$$
given by:
$$b \mapsto ba$$
2. *Every A-**module endomorphism***
$$\omega : {}_A A \to {}_A A$$
is of this form
3. *The map:*
$$A^{op} \to \mathrm{End}_A({}_A A)$$
given by:
$$a \mapsto r_a$$
is an ***isomorphism*** *of rings*

(Lemma 3.4)

we have that
$$B \cong \mathrm{End}_B({}_B B)^{op} \cong \mathrm{End}_B(V^n)^{op} \cong M_n(D)^{op} \cong M_n(D^{op})$$
(since the opposite is a self-inverse, and the endomorphisms of a vector space are isomorphic to the matrix ring).

- **How is this isomorphism defined?**
  - consider the isomorphism:
$$\mathrm{End}_B(V^n) \cong M_n(D) = M_n(\mathrm{End}_B(V))$$
  - let φ_{ij} be B-module endomorphisms of V, arranged as a $n \times n$ matrix
  - then, thinking of the elements of V^n as column vectors, we can map:
$$(\varphi_{ij}) \mapsto \left(\begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \mapsto (\varphi_{ij}) \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \right)$$

□

5.5 Artin-Weddernburn Theorem

5.5.1 Theorem: Artin-Weddernburn

> *Suppose that k is an* ***algebraically closed field*** *and that A is a* ***finite dimensional semisimple*** k***-algebra****.*
> *Then there exist* ***positive integers*** $n_1, \ldots, n_r$ *and a* k***-algebra isomorphism****:*
> $$A \cong M_{n_1}(k) \times \ldots \times M_{n_r}(k)$$
> *(Theorem 3.19)*

Proof. By

> 1. *Each B_i is a* ***ring*** *with* ***identity element*** e_i
> 2. *A is* ***isomorphic*** *to the* ***product*** *of rings (B_i, e_i):*
> $$A \cong B_1 \times \ldots B_r$$
> 3. *Each B_i is itself a* ***semisimple ring****, with* ***unique*** *simple module V_i*
>
> *(Lemma 3.17)*

we can decompose A intor a product of semisimple rings B_i, with unique simple module V_i (up to isomorphism). Moreover, by

> *Let B be a* ***semisimple ring*** *with exactly one simple module V, up to* ***isomorphism****. Suppose that:*
> $$B \cong \underbrace{V \oplus \ldots \oplus V}_{n \text{ times}}$$
> *is a left B-module, and let:*
> $$D = \text{End}_B(V)$$
> *Then there is a* ***ring isomorphism****:*
> $$B \cong M_n(D^{op})$$
> *(Proposition 3.18)*

it follows that each $B_i \cong M_n(D^{op})$ where $D = \text{End}_{B_i}(V_i)$ is a division ring. But by Schur's Lemma:

> *Suppose k is **algebraically closed**. Let V be a **simple module** over a **finite dimensional** k**-algebra** A.*
> *Then, every A**-module endomorphism** of V is given by the action of some **scalar** $\lambda \in K$, such that:*
>
> $$\text{End}_A(V) = k1_V$$
>
> *(Theorem 3.6)*

we have that:

$$D^{op} \cong k$$

so the result follows.

□

5.5.2 Corollary: Decomposing Group Ring

> *Suppose that k is **algebraically closed**.*
> *Let G be a **finite group** such that $|G| \neq 0$ in k, and let*
>
> $$V_1, \ldots, V_r$$
>
> *be a complete list of **pairwise nonisomorphic simple** kG**-modules**.*
> *Then:*
>
> 1. *kG (as a kG-module) is such that:*
>
> $$kG \cong V_1^{\dim(V_1)} \oplus \ldots \oplus V_r^{\dim(V_r)}$$
>
> 2. $$|G| = \sum_{i=1}^{r} \dim(V_i)^2$$
>
> *(Corollary 3.20)*

Proof. By the Corollary to Mascheke's Theorem, since $|G|$ isn't 0 in k, kG is a semisimple module, so by the Artin-Weddernburn Theorem above, there exists an isomorphism:

$$kG \cong M_{n_1}(k) \times \ldots \times M_{n_r}(k)$$

Now, by problem sheet 1, k^n is a simple $M_n(k)$ module:

Let $V = k^n$, and $A = M_n(k)$. Let $v \in V$ be any non-zero column vector, and consider the A-submodule generated by v:

$$u = Av$$

Let $e_1, \dots, e_n$ denote the n standard basis vectors of V (such that $(e_i)_j = \delta_{ij}$). Now, since v is non-zero, there is some component v_j which is non-zero. Thus, define matrices $A_\ell \in M_n(k)$ via:

$$(A_\ell)_{ab} = v_j^{-1} \delta_{\ell i} \delta_{jb}$$

Then, it follows that:

$$A_\ell v = e_\ell$$

In other words, all of the standard basis vectors of V are within the subspace U, which implies that $U = V$ whenever U is generated by a single non-zero vector in V.
For more general subspaces $U \leq V$, if U is non-zero, it must contain at least one non-zero vector v_U, and so:

$$Av_U \leq U \;\wedge Av_U = V \implies U = V$$

Hence, V is a simple A-module.

Moreover, $M_n(k)$ is isomorphic to the direct sum of n of these modules:

Let L_ℓ be the ideal generated by the set:

$$\{Z_{\ell b} \mid b \in [1, n\}$$

where $Z_{\ell b}$ is an elementary matrix, with a 1 at entry ℓ, b and 0s elsewhere. Notice, L_ℓ contains all matrices which have at least one non-zero element in their ℓth row, and 0s in every other row.
Each L_ℓ is simple (since they are in 1-1 correspondence with the A-module k^n which is simple), and certainly:

$$A = L_1 \oplus \ldots \oplus L_n$$

(since by definition $\bigcap_{\ell \in [1,n]} L_\ell = \{0\}$ and any matrix in $M_n(k)$ can be expressed as a sum of matrices who only contain entries in certain rows).

Thus, we have that $n_i = \dim(V_i)$.

The second statement follows from the fact that $|G| = \dim(kG)$.

□