

Chapter 5

Structure of rings

5.1 Algebras

It is time to introduce the notion of an algebra over a commutative ring. So let R be a commutative ring. An R -algebra is a ring A (unital as always) together with a multiplication $R \times A \rightarrow A$ such that

$$(A1) \quad 1_R a = a;$$

$$(A2) \quad (r + s)a = ra + sa;$$

$$(A3) \quad r(a + b) = ra + rb;$$

$$(A4) \quad (rs)a = r(sa);$$

$$(A5) \quad r(ab) = (ra)b = a(rb)$$

for all $r, s \in R, a, b \in A$. The conditions (A1)–(A4) just say that the Abelian group A is an R -module, while (A5) is “associativity”. Thus, you can think of an R -algebra instead as an R -module together with an R -bilinear multiplication making it into a ring.

Note a \mathbb{Z} -algebra is just the old definition of ring: “ \mathbb{Z} -algebras = rings” just as “ \mathbb{Z} -modules = Abelian groups”. So you should view the passage from rings to R -algebras as analogous to the passage from Abelian groups to R -modules! This is the idea of studying objects (e.g. Abelian groups, rings) *relative* to a fixed commutative base ring R .

There is an equivalent formulation of the definition of R -algebra: an R -algebra is a ring A together with a distinguished ring homomorphism

$$s : R \rightarrow A$$

such that the image of s lies in the *center* $Z(A) = \{a \in A \mid ab = ba \text{ for all } b \in A\}$. Indeed, given such a ring homomorphism, define a multiplication $R \times A \rightarrow A$ by $(r, a) \mapsto s(r)a$. Now check this satisfies the above axioms (A1)–(A5) (the last one being because $\text{im } s \subseteq Z(A)$). Conversely, given an R -algebra as defined originally, one obtains a ring homomorphism $s : R \rightarrow A$ by defining $s(r) = r1_A$, and the image lies in $Z(A)$ by (A5).

Let A be an R -algebra. Then, given an A -module M , we can in particular think of M as just an R -module, defining $rm = s(r)m$ for $r \in R, m \in M$. So you can hope to exploit the additional structure of the base ring R in studying A -modules. In particular, if $R = F$ is a field and A is an F -algebra, A and any A -module M is in particular a vector space over F . So we can talk about *finite dimensional F -algebras* and *finite dimensional modules* over an F -algebra, meaning their underlying dimension as vector spaces over F .

Note given A -modules M, N , an A -module homomorphism between them is automatically an R -module homomorphism (for the underlying R -module structure). However, it is not necessarily the

case that a ring homomorphism between two different R -algebras is an R -module homomorphism. So one *defines* an R -algebra homomorphism $f : A \rightarrow B$ between two R -algebras A and B to be a ring homomorphism in the old sense that is in addition R -linear (i.e. it is an R -module homomorphism too). *Ring homomorphisms and R -algebra homomorphisms are different things!*

Now for examples. Actually, we already know plenty. Let R be a commutative ring. Then, the polynomial ring $R[X_1, \dots, X_n]$ is evidently an R -algebra: indeed, $R[X_1, \dots, X_n]$ contains a copy of R as the subring consisting of polynomials of degree zero.

The ring $M_n(R)$ of $n \times n$ matrices over R is an R -algebra: again, it contains a copy of R as the subring consisting of the scalar matrices. But note there is a big difference between this and the previous example: $M_n(R)$ is *finitely generated* as an R -module (indeed, it is free of rank n^2) whereas $R[X_1, \dots, X_n]$ is not. In case F is a field, $M_n(F)$ is a *finite dimensional F -algebra*, $F[X_1, \dots, X_n]$ is not.

For the next example, let M be any (left) R -module. Consider the Abelian group

$$\text{End}_R(M).$$

We make it into a ring by defining the product of two endomorphisms of M simply to be their composition. Now I claim that $\text{End}_R(M)$ is in fact an R -algebra: indeed, we define $r\theta$ for $r \in R, \theta \in \text{End}_R(M)$ by setting

$$(r\theta)(m) = r(\theta(m)) (= \theta(rm))$$

for all $m \in M$. Let us check that $r\theta$ really is an R -endomorphism of M . Take another $s \in R$. Then,

$$s((r\theta)(m)) = sr(\theta(m)) = \theta(srm) = \theta(rsm) = (r\theta)(sm).$$

Note we really did use the commutativity of R !

We can generalize the previous two examples. Suppose now that A is a (not necessarily commutative) R -algebra and M is a left A -module. Then, the ring $D = \text{End}_A(M)$ is also an R -algebra, defining $(rd)(m) = r(d(m))$ for all $r \in R, d \in D, m \in M$.

5.1.1. Lemma. *Let A be an R -algebra, M a left A -module and $D = \text{End}_A(M)$. Then,*

$$\text{End}_A(M^{\oplus n}) \cong M_n(D)$$

as R -algebras.

Proof. Let us write elements of $M^{\oplus n}$ as column vectors

$$\begin{bmatrix} m_1 \\ \vdots \\ m_n \end{bmatrix}$$

with $m_i \in M$. Suppose we have $f \in \text{End}_A(M^{\oplus n})$. Let $f_{i,j} : M \rightarrow M$ be the map sending $m \in M$ to the i th coordinate of the vector

$$\begin{bmatrix} 0 \\ \vdots \\ 0 \\ m \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

where the m is in the j th row. Then, $f_{i,j}$ is an A -module homomorphism, so is an element of D . Moreover,

$$f \left(\begin{bmatrix} m_1 \\ \vdots \\ m_n \end{bmatrix} \right) = \begin{bmatrix} f_{1,1} & \cdots & f_{1,n} \\ \vdots & \ddots & \vdots \\ f_{n,1} & \cdots & f_{n,n} \end{bmatrix} \begin{bmatrix} m_1 \\ \vdots \\ m_n \end{bmatrix} \quad (\text{matrix multiplication!}),$$

so that f is uniquely determined by the $f_{i,j}$. Thus, we obtain an R -algebra isomorphism $f \mapsto (f_{i,j})$ between $\text{End}_A(M^{\oplus n})$ and $M_n(D)$. \square

For the final example of an algebra, let G be any group. Define the *group algebra* RG to be the free R -module on basis the elements of G . Thus an element of RG looks like

$$\sum_{g \in G} r_g g$$

for coefficients $r_g \in R$ all but finitely many of which are zero. Multiplication is defined by the rule

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

In other words, the multiplication in RG is induced by the multiplication in G and R -bilinearity. Note the RG contains a copy of R as a subring, namely, $R1_G$, so is certainly an R -algebra. The construction of the group algebra RG allows the possibility of studying the abstract group G by studying the category of RG -modules – so module theory can be applied to group theory. Note finally in case G is a finite group and F is a field, the group algebra FG is a *finite dimensional F -algebra*.

5.2 Chain conditions

Let M be a (left or right) R -module. Then, M is called *Noetherian* if it satisfies the *ascending chain condition* (ACC) on submodules. This means that every ascending chain

$$M_1 \subseteq M_2 \subseteq M_3 \subseteq \dots$$

of submodules of M eventually stabilizes, i.e. $M_n = M_{n+1} = M_{n+2} = \dots$ for sufficiently large n .

Similarly, M is called *Artinian* if it satisfies the *descending chain condition* (DCC) on submodules. So every descending chain

$$M_1 \supseteq M_2 \supseteq M_3 \supseteq \dots$$

of submodules of M eventually stabilizes, i.e. $M_n = M_{n+1} = M_{n+2} = \dots$ for sufficiently large n .

A ring R is called *left* (resp. *right*) *Noetherian* if it is Noetherian viewed as a left (resp. right) R -module. Similarly, R is called *left* (resp. *right*) *Artinian* if it is Artinian viewed as a left (resp. right) R -module. In the case of commutative rings, we can omit the left or right here, but we cannot in general as the following pathological examples show:

Exercise. (i) The ring of all 2×2 matrices of the form

$$\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$$

where $a \in \mathbb{Q}$ and $b, c \in \mathbb{R}$ is right Artinian but not left Artinian.

(ii) The ring of all 2×2 matrices of the form

$$\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$$

where $a \in \mathbb{Z}$ and $b, c \in \mathbb{Q}$ is right Noetherian but not left Noetherian.

This chapter is mainly concerned with the Artinian property, but it doesn't make sense to introduce one chain condition without the other. We will discuss Noetherian rings in detail in chapter 8. By the way, you should think of the Noetherian property as a quite weak finiteness

property on a ring, whereas the Artinian property is rather strong (see Hopkin's theorem below for the justification of this).

We already know plenty of examples of Noetherian and Artinian rings. For instance, any PID is Noetherian (Lemma 2.4.1), but it not Artinian unless it is a field (e.g. \mathbb{Z} is not Artinian: $(p) \supset (p^2) \supset \dots$ is an infinitely descending chain). The ring \mathbb{Z}_{p^n} for p prime is both Noetherian and Artinian: indeed, here there are only finitely many ideals in total, the (p^i) for $0 \leq i \leq n$.

The main source of Artinian rings is as follows. Let F be a field and suppose that R is an F -algebra. Then I claim that every R -module M which is finite dimensional as an F -vector space is both Artinian and Noetherian. Well, R -submodules of M are in particular F -vector subspaces. And clearly in a finite dimensional vector space, you cannot have infinite chains of proper subspaces. So finite dimensionality of M does the job immediately!

In particular, if the F -algebra R is *finite dimensional* as a vector space over F , then R is both left and right Artinian and Noetherian. Now you see why finite dimensional algebras over a field (e.g. $M_n(F)$, the group algebra FG for G a finite group, etc...) are particularly nice things!

5.2.1. Lemma. *Let $0 \rightarrow K \xrightarrow{i} M \xrightarrow{\pi} Q \rightarrow 0$ be a short exact sequence of R -modules. Then M is Noetherian (resp. Artinian) if and only if both K and Q are Noetherian (resp. Artinian).*

Proof. I just prove the result for the Noetherian property, the Artinian case being analogous. First, suppose M satisfies ACC. Then obviously K does as it is isomorphic to a submodule of M . Similarly Q does by the lattice isomorphism theorem for modules.

Conversely, suppose K and Q both satisfy ACC. Let $M_1 \subseteq M_2 \subseteq \dots$ be an ascending chain of R -submodules of M . Set

$$K_i = i^{-1}(i(K) \cap M_i), \quad Q_i = \pi(M_i).$$

Then, $K_1 \subseteq K_2 \subseteq \dots$ is an ascending chain of submodules of K , and $Q_1 \subseteq Q_2 \subseteq \dots$ is an ascending chain of submodules of Q . So by assumption, there exists $n \geq 1$ such that $K_N = K_n$ and $Q_N = Q_n$ for all $N \geq n$. Now, we have evident short exact sequences

$$0 \rightarrow K_n \rightarrow M_n \rightarrow Q_n \rightarrow 0$$

and

$$0 \rightarrow K_N \rightarrow M_N \rightarrow Q_N \rightarrow 0$$

for each $N \geq n$. Letting $\alpha : K_n \rightarrow K_N, \beta : M_n \rightarrow M_N$ and $\gamma : Q_n \rightarrow Q_N$ be the inclusions, one obtains a commutative diagram with α and γ being isomorphisms. Then the five lemma implies that β is surjective, hence $M_N = M_n$ for all $N \geq n$ as required. \square

5.2.2. Theorem. *If R is left (resp. right) Noetherian, then every finitely generated left (resp. right) R -module is Noetherian. Similarly, if R is left (resp. right) Artinian, then every finitely generated left (resp. right) R -module is Artinian.*

Proof. Let's do this for the Artinian case, the Noetherian case being similar. So assume that R is left Artinian and M is a finitely generated left R -module. Then, M is a quotient of a free R -module with a finite basis. So it suffices to show that $R^{\oplus n}$ is an Artinian left R -module. We proceed by induction on n , the case $n = 1$ being given. For $n > 1$, the submodule of $R^{\oplus n}$ spanned by the first $(n - 1)$ basis elements is isomorphic to $R^{\oplus(n-1)}$, and the quotient by this submodule is isomorphic to R . By induction both $R^{\oplus(n-1)}$ and R are Artinian. Hence, $R^{\oplus n}$ is Artinian by Lemma 5.2.1. \square

The next results are special ones about Noetherian rings (but see Hopkin's theorem below!)

5.2.3. Lemma. *Let R be a left Noetherian ring and M be a finitely generated left R -module. Then every R -submodule of M is also finitely generated.*

Proof. By Theorem 5.2.2, M is Noetherian. Let N be an arbitrary R -submodule of M and let \mathcal{A} be the set of finitely generated R -submodules of M contained in N . Note \mathcal{A} is non-empty as the zero module is certainly there!

Now I claim that \mathcal{A} contains a maximal element. Well, pick $M_1 \in \mathcal{A}$. If M_1 is maximal in \mathcal{A} , we are done. Else, we can find $M_2 \in \mathcal{A}$ with $M_1 \supset M_2$. Repeat. The process must terminate, else we construct an infinite ascending chain of submodules of $N \subseteq M$, contradicting the fact that M is Noetherian. (*Warning:* as with all such arguments we have secretly appealed to the axiom of choice here! Hungerford gives the logically correct argument, see VIII.1.4).

So now let N' be a maximal element of \mathcal{A} . Say N' is generated by m_1, \dots, m_n . Now take any $m \in N$. Then, (m_1, \dots, m_n, m) is a finitely generated submodule of M contained in N and containing N' . By maximality of N' , we therefore have that

$$N' = (m_1, \dots, m_n, m),$$

i.e. $m \in N'$. This shows that $N = N'$, hence N is finitely generated. \square

5.2.4. Corollary. *Let R be a ring. Then, The following are equivalent:*

- (i) R is left Noetherian;
 - (ii) every left ideal of R is finitely generated;
- (Similar statements hold on the right, of course).

Proof. (i) \Rightarrow (ii). This is a special case of Lemma 5.2.3, taking $M = R$.

(ii) \Rightarrow (i). Let $I_1 \subseteq I_2 \subseteq \dots$ be an ascending chain of left ideals of R . Then, $I = \bigcup_{n \geq 1} I_n$ is also a left ideal of R , hence finitely generated, by a_1, \dots, a_m say. Then for some sufficiently large n , all of a_1, \dots, a_m lie in I_n . Hence $I_n = I$ and R is Noetherian. \square

Now you see that – for commutative rings – Noetherian is an obvious generalization of a PID. Instead of insisting all ideals are generated by a single element, one has that every ideal is generated by finitely many elements.

5.3 Wedderburn structure theorems

Now we have the basic language of algebras and of Artinian rings and modules, we can begin to discuss the structure of rings. The first step is to understand the structure of *semisimple rings*. Recall that an R -module M is *simple* or *irreducible* if it is non-zero and has no submodules other than M and (0) .

Schur's lemma. *Let M be a simple R -module. Then, $\text{End}_R(M)$ is a division ring.*

Proof. Let $f : M \rightarrow M$ be a non-zero R -endomorphism of M . Then, $\ker f$ and $\text{im } f$ are both R -submodules of M , with $\ker f \neq M$ and $\text{im } f \neq (0)$ since f is non-zero. Hence, since M is simple, $\ker f = (0)$ and $\text{im } f = M$. This shows that f is a bijection, hence invertible. \square

Throughout the section, we will also develop parallel but stronger versions of the results dealing with finite dimensional algebras over algebraically closed fields (recall a field F is algebraically closed if every monic $f(X) \in F[X]$ has a root in F).

Relative Schur's lemma. *Let F be an algebraically closed field and A be an F -algebra. Let M be a simple A -module which is finite dimensional as an F -vector space. Then, $\text{End}_R(M) = F$.*

Proof. Let $f : M \rightarrow M$ be an A -endomorphism of M . Then in particular, $f : M \rightarrow M$ is an F -linear endomorphism of a finite dimensional vector space. Since F is algebraically closed, f has an eigenvector $v_\lambda \in M$ of eigenvalue $\lambda \in F$ (because the characteristic polynomial of f has a root in F).

Now consider $f - \lambda \text{id}_M$. It is also an A -endomorphism of M , and moreover its kernel is non-zero as v_λ is annihilated by $f - \lambda \text{id}_M$. Hence since M is irreducible, the kernel of $f - \lambda \text{id}_M$ is all of M , i.e. $f = \lambda \text{id}_M$. This shows that the only R -endomorphisms of M are the scalars, as required. \square

Now, let R be a non-zero ring. Call R *left semisimple* if ${}_R R$ is semisimple as a left R -module (recall section 4.3). Similarly, R is *right semisimple* if R_R is semisimple as a right R -module. Finally, R is *simple* if it has no two-sided ideals other than R and (0) .

Warning: In Hungerford, a more general definition of semisimple is used. I believe the term “semiprimitive” should be used for the rings called semisimple rings in Hungerford, and that “semisimple” should mean what it does here! Just beware that semisimple rings mean different things to different people. But the two definitions (ours and Hungerford’s) agree in case the ring is Artinian.

Wedderburn’s first structure theorem. *The following conditions on a non-zero ring R are equivalent:*

- (i) R is simple and left Artinian;
- (i') R is simple and right Artinian;
- (ii) R is left semisimple and all simple left R -modules are isomorphic;
- (ii') R is right semisimple and all simple right R -modules are isomorphic;
- (iii) R is isomorphic to the matrix ring $M_n(D)$ for some $n \geq 1$ and D a division ring.

Moreover, the integer n and the division ring D in (iii) are determined uniquely by R (up to isomorphism).

Proof. First, note the condition (iii) is left-right symmetric. So let us just prove the equivalence of (i),(ii) and (iii).

(i) \Rightarrow (ii). Let U be a minimal left ideal of R . This exists because R is left Artinian so we have DCC on left ideals! Then, $U = Rx$ for any non-zero $x \in U$, and Rx is a simple left R -module. Since R is a simple ring, the non-zero two-sided ideal RxR must be all of R . Hence,

$$R = RxR = \sum_{a \in R} Rxa.$$

Note each Rxa is a homomorphic image of the simple left R -module Rx , so is either isomorphic to Rx or zero. Thus we have written ${}_R R$ as a sum of simple R -modules, so by Lemma 4.3.1, there exists a subset $S \subseteq R$ such that

$$R = \bigoplus_{a \in S} Rxa$$

with each Rxa for $a \in S$ being isomorphic to U . Hence, R is left semisimple.

Moreover, if M is any simple left R -module, then $M \cong R/J$ for a maximal left ideal J of R . We can pick $a \in S$ such that $xa \notin J$. Then, the quotient map $R \rightarrow R/J$ maps the simple submodule Rxa of R to a non-zero submodule of M . Hence using simplicity, $M \cong Rxa$. This shows all simple R -modules are isomorphic to U .

(ii) \Rightarrow (iii). Let U be a simple left R -module. We have that

$$R = \bigoplus_{a \in S} Ra$$

for some subset S of R , where each left R -module Ra is isomorphic to U . I claim that S is finite. Indeed, 1_R lies in $\bigoplus_{a \in S} Ra$ hence in $Ra_1 \oplus \cdots \oplus Ra_n$ for some finite subset $\{a_1, \dots, a_n\}$ of S . But 1_R generates R as a left R -module, so in fact $\{a_1, \dots, a_n\} = S$.

Thus,

$$R \cong U^{\oplus n}$$

for some n , uniquely determined as the composition length of ${}_R R$. Now, by Schur’s lemma, $\text{End}_R(U) \cong D$, where D a Division ring uniquely determined up to isomorphism as the endomorphism ring of a simple left R -module. Hence applying Lemma 5.1.1,

$$\text{End}_R({}_R R) \cong \text{End}_R(U^{\oplus n}) \cong M_n(D).$$

Now finally, we observe that

$$\text{End}_R({}_R R) \cong R^{\text{op}},$$

the isomorphism in the forward direction being determined by evaluation at 1_R . To see that this is an isomorphism, one constructs the inverse map, namely, the map sending $r \in R$ to $f_r : {}_R R \rightarrow {}_R R$ with $f_r(s) = sr$ for each $s \in R$ (“ f_r is right multiplication by r ”). Now we have shown that

$$R^{\text{op}} \cong M_n(D).$$

Hence, noting that matrix transposition is an isomorphism between $M_n(D)^{\text{op}}$ and $M_n(D^{\text{op}})$, we get that

$$R \cong M_n(D^{\text{op}})$$

and D^{op} is also a division ring.

(iii) \Rightarrow (i). We know that $M_n(D)$ is simple as it is Morita equivalent to D , which is a division ring (or you can prove this directly!). It is left Artinian for instance because $M_n(D)$ is finite dimensional over the division ring D . This gives (i). \square

Corollary. *Every simple left (or right) Artinian ring R is an algebra over a field.*

Proof. Observe $M_n(D)$ is an algebra over $Z(D)$, which is a field. \square

The relative version for finite dimensional algebras over algebraically closed fields is as follows:

Relative first structure theorem. *Let F be an algebraically closed field and A be a finite dimensional F -algebra (hence automatically left and right Artinian).*

- (i) A is simple;
- (ii) A is left semisimple and all simple left R -modules are isomorphic;
- (ii') A is right semisimple and all simple right R -modules are isomorphic;
- (iii) A is isomorphic to the matrix ring $M_n(F)$ for some n (indeed, $n^2 = \dim A$).

Proof. The proof is the same, except that one gets that the division ring D equals F since one can use the stronger relative Schur's lemma. \square

Wedderburn's second structure theorem. *Every left (or right) semisimple ring R is isomorphic to a finite product of matrix rings over division rings:*

$$R \cong M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r)$$

for uniquely determined $n_i \geq 1$ and division rings D_i . Conversely, any such ring is both left and right semisimple.

Proof. Since R is left semisimple, we can decompose ${}_R R$ as $\bigoplus_{i \in I} U_i$ where each U_i is simple. Note 1_R already lies in a sum of finitely many of the U_i , hence the index set I is actually finite. Now gather together isomorphic U_i 's to write

$${}_R R = H_1 \oplus \cdots \oplus H_m$$

where

$$H_i \cong L_i^{\oplus n_i}$$

for irreducible R -modules L_i and integers $n_i \geq 1$, with $L_i \not\cong L_j$ for $i \neq j$. By Schur's lemma, $D_i = \text{End}_R(U_i)$ is a division ring. Moreover, there are no R -module homomorphisms between H_i and H_j for $i \neq j$, because none of their composition factors are isomorphic. Hence:

$$\begin{aligned} R &\cong \text{End}_R({}_R R)^{\text{op}} \cong \text{End}_R(H_1 \oplus \cdots \oplus H_m)^{\text{op}} \cong \text{End}_R(H_1)^{\text{op}} \times \cdots \times \text{End}_R(H_m)^{\text{op}} \\ &\cong M_{n_1}(D_1)^{\text{op}} \times \cdots \times M_{n_m}(D_m)^{\text{op}} \cong M_{n_1}(D_1^{\text{op}}) \times \cdots \times M_{n_m}(D_m^{\text{op}}). \end{aligned}$$

The integers n_i are uniquely determined as the multiplicities of the irreducible left R -modules in a composition series of ${}_R R$, while the division rings D_i are uniquely determined up to isomorphism as the endomorphism rings of the simple left R -modules.

For the converse, we need to show that a product of matrix algebras over division rings is left and right semisimple. This follows because a single matrix algebra $M_n(D)$ over a division ring is both left and right semisimple according to the first Wedderburn structure theorem. \square

The theorem shows:

Corollary. *A ring R is left semisimple if and only if it is right semisimple.*

So we can now just call R *semisimple* if it is either left or right semisimple in the old sense. Also:

Corollary. *Any semisimple ring is both left and right Artinian.*

Proof. A product of finitely many matrix rings over division algebras is left and right Artinian. \square

Finally, we need to give the relative version:

Relative second structure theorem. *Let F be an algebraically closed field and A be a finite dimensional F -algebra that is semisimple. Then,*

$$A \cong M_{n_1}(F) \times \cdots \times M_{n_r}(F)$$

for uniquely determined integers $n_i \geq 1$.

Proof. Just use the relative Schur's lemma in the same proof. \square

This theorem lays bare the structure of finite dimensional semisimple algebras over algebraically closed fields: A is uniquely determined up to isomorphism by the integers n_i , which are precisely the dimensions of the simple A -modules. This has a very important application to the study of finite groups, indeed, it is the starting point for the study of *character theory* of finite groups. To give you a glimpse, and convince you that semisimple algebras are rather common, let us prove:

Maschke's theorem. *Let G be a finite group and F be a field either of characteristic 0 or of characteristic p coprime to the order of G . Then, the group algebra FG is a semisimple algebra.*

Proof. It is certainly enough to show that every left FG -module M is semisimple. We just need to show that every short exact sequence

$$0 \longrightarrow K \longrightarrow M \xrightarrow{\pi} Q \longrightarrow 0$$

of FG -modules splits. Well, pick any F -linear map $\theta : Q \rightarrow M$ such that $\pi \circ \theta = \text{id}_Q$. The problem is that θ need not be an FG -module map.

Well, for $g \in G$, define a new F -linear map

$${}^g\theta : Q \rightarrow M, \quad x \mapsto g\theta(g^{-1}x).$$

Then,

$$(\pi \circ {}^g\theta)(x) = \pi(g\theta(g^{-1}x)) = g(\pi \circ \theta)(g^{-1}x) = gg^{-1}x = x$$

so each ${}^g\theta$ also satisfies $\pi \circ {}^g\theta = \text{id}_Q$. Now define

$$Av\theta = \frac{1}{|G|} \sum_{g \in G} {}^g\theta$$

(note $|G|$ is invertible in F by assumption on characteristic). This is another F -linear map such that $\pi \circ Av\theta = \text{id}_Q$. Moreover, $Av\theta$ is even an FG -module map:

$$hAv\theta(x) = \frac{1}{|G|} \sum_{g \in G} hg\theta(g^{-1}x) = \frac{1}{|G|} \sum_{g \in G} g\theta(g^{-1}hx) = Av\theta(hx).$$

Hence, $Av\theta$ defines the required splitting. \square

Thus for example if G is a finite group, the group algebra $\mathbb{C}G$ is isomorphic to a product of matrix algebras over \mathbb{C} . One gets

5.4 The Jacobson radical

I want to explain in this section how understanding of the case of semisimple rings gives information about more general rings. The key notion is that of the Jacobson radical, which will be defined using the following equivalent properties:

Jacobson radical theorem. *Let R be a ring, $a \in R$. The following are equivalent:*

- (i) a annihilates every simple left R -module;
- (i)' a annihilates every simple right R -module;
- (ii) a lies in every maximal left ideal of R ;
- (ii)' a lies in every maximal right ideal of R ;
- (iii) $1 - xa$ has a left inverse for every $x \in R$;
- (iii)' $1 - xa$ has a right inverse for every $x \in R$;
- (iv) $1 - xay$ is a unit for every $x, y \in R$.

Proof. Since (iv) is left-right symmetric, I will only prove equivalence of (i)–(iv).

(i) \Rightarrow (ii). If I is a maximal left ideal of R , then R/I is a simple left R -module. So, $a(R/I) = 0$, i.e. $a \in I$.

(ii) \Rightarrow (iii). Assume (ii) holds but $1 - xa$ does not have a left inverse for some $x \in R$. Then, $R(1 - xa) \neq R$. So, there exists a maximal left ideal I with

$$R(1 - xa) \leq I < R.$$

But then, $1 - xa \in I$, and $a \in I$ by assumption. Hence, $1 \in I$ so $I = R$, a contradiction.

(iii) \Rightarrow (i). Let M be a simple left R -module. Take $u \in M$. If $au \neq 0$, then $Rau = M$ as M is simple, so $u = rau$ for some $r \in R$. But this implies that $(1 - ra)u = 0$, hence since $(1 - ra)$ has a left inverse by assumption, we get that $u = 0$. This contradiction shows that in fact $au = 0$ for all $u \in M$, i.e. $aM = 0$.

(iv) \Rightarrow (iii). This is trivial (take $y = 1$).

(i),(iii) \Rightarrow (iv). For any $y \in R$ and any simple left R -module M , $ayM \subseteq aM = 0$. So ay also satisfies the condition in (i), hence (iii). So for every $x \in R$, $1 - xay$ has a left inverse, $1 - b$ say. The equation $(1 - b)(1 - xay) = 1$ implies $b = (b - 1)xay$. Hence $bM = 0$ for all simple left R -modules M , so b satisfies (i) hence (iii). So, $1 - b$ has a left inverse, $1 - c$, say. Then,

$$1 - c = (1 - c)(1 - b)(1 - xay) = 1 - xay,$$

hence

$$c = xay.$$

Now we have that $1 - b$ is a left inverse to $1 - xay$, and $1 - xay$ is a left inverse to $1 - b$. Hence, $1 - xay$ is a unit with inverse $1 - b$. \square

Now define the *Jacobson radical* $J(R)$ to be

$$J(R) = \{a \in R \mid a \text{ satisfies the equivalent conditions in the theorem}\}.$$

Thus for instance using (i), $J(R)$ is the intersection of the annihilators in R of all the simple left R -modules, or using (ii)

$$J(R) = \bigcap_I I$$

where I runs over all maximal left ideals of R . This implies that $J(R)$ is a left ideal of R , but equally well using (ii)',

$$J(R) = \bigcap_I I$$

where I runs over all maximal right ideals of R so that J is a right ideal of R . Hence, $J(R)$ is a two-sided ideal of R .

The following result is a basic trick in ring theory and maybe gives a first clue as to why the Jacobson radical is so important.

Nakayama's lemma. *Let R be a ring and M be a finitely generated left R -module. If $J(R)M = M$ then $M = 0$.*

Proof. Suppose that M is non-zero and set $J = J(R)$ for short. Let $X = \{m_1, \dots, m_n\}$ be a minimal set of generators of M , so $m_1 \neq 0$. Since $JM = M$, we can write

$$m_1 = j_1 m_1 + \dots + j_n m_n$$

for some $j_i \in J$. So,

$$(1_R - j_1)m_1 = j_2 m_2 + \dots + j_n m_n.$$

But $1_R - j_1$ is a unit by the definition of $J(R)$. So we get that

$$m_1 = (1_R - j_1)^{-1} j_2 m_2 + \dots + (1_R - j_1)^{-1} j_n m_n.$$

This contradicts the minimality of the initial set of generators chosen. \square

We will apply Nakayama's lemma later on, see Corollary 8.2.1. The remainder of the section is concerned with the Jacobson radical in an *Artinian ring*!!! All these results are *false* if the ring is not Artinian...

First characterization of the Jacobson radical for Artinian rings. *Suppose that R is left (or right) Artinian. Then, $J(R)$ is the unique smallest two-sided ideal of R such that $R/J(R)$ is a semisimple algebra.*

Proof. Pick a maximal left ideal I_1 of R . Then (if possible) pick a maximal left ideal I_2 such that $I_2 \not\supseteq I_1$ (hence $I_1 \cap I_2$ is strictly smaller than I_1). Then (if possible) pick a maximal left ideal I_3 such that $I_3 \not\supseteq I_1 \cap I_2$ (hence $I_1 \cap I_2 \cap I_3$ is strictly smaller than $I_1 \cap I_2$). Keep going! The process must terminate after finitely many steps, else you construct an infinite descending chain

$$R \supset I_1 \supset I_1 \cap I_2 \supset I_1 \cap I_2 \cap I_3 \supset \dots$$

of left ideals of R , contradicting the fact that R is left Artinian. We thus obtain finitely many maximal left ideals I_1, I_2, \dots, I_r of R such that $I_1 \cap \dots \cap I_r$ is contained in *every* maximal left ideal of R . In other words,

$$J(R) = I_1 \cap \dots \cap I_r,$$

so the Jacobson radical of an Artinian ring is the intersection of finitely many maximal left ideals.

Consider the map

$$R \rightarrow R/I_1 \oplus \dots \oplus R/I_r, \quad a \mapsto (a + I_1, \dots, a + I_r).$$

It is an R -module map with kernel $I_1 \cap \dots \cap I_r = J(R)$. So it induces an embedding

$$R/J \hookrightarrow R/I_1 \oplus \dots \oplus R/I_r.$$

The right hand side is a semisimple R -module, as it is a direct sum of simples, hence R/J is also a semisimple R -module. This shows that the quotient R/J is a semisimple ring.

Now let K be another two-sided ideal of R such that R/K is a semisimple ring. By the lattice isomorphism theorem, we can write

$$R/K = \bigoplus_{i \in I} B_i/K$$

where B_i is a left ideal of R containing K , $\sum_{i \in I} B_i = R$ and $B_i \cap (\sum_{j \neq i} B_j) = K$ for each i . Set $C_i = \sum_{j \neq i} B_j$ for short. Then,

$$R/C_i = (C_i + B_i)/C_i \cong B_i/(B_i \cap C_i) = B_i/K.$$

This is simple, so C_i is a maximal left ideal of R . Hence, each $C_i \supseteq J(R)$. So $K = \bigcap C_i$ also contains $J(R)$. Thus $J(R)$ is the unique smallest such ideal. \square

Thus you see the first step to understanding the structure of an Artinian ring: understand the semisimple ring $R/J(R)$ in the sense of Wedderburn's structure theorem.

5.4.1. Corollary. *Let R be a left Artinian ring and M be a left R -module. Then, M is semisimple if and only if $J(R)M = 0$.*

Proof. If M is semisimple, it is a direct sum of simples. Now, $J(R)$ annihilates all simple left R -modules by definition, hence $J(R)$ annihilates M . Conversely, if $J(R)$ annihilates M , then we can view M as an $R/J(R)$ -module by defining $(a + J(R))m = am$ for all $a \in R, m \in M$ (one needs $J(R)$ to annihilate M for this to be well-defined!). Since $R/J(R)$ is semisimple by the previous theorem, M is a semisimple $R/J(R)$ -module. But the R -module structure on M is just obtained by lifting the $R/J(R)$ -module structure, so this means that M is semisimple as an R -module too. \square

Second characterization of the Jacobson radical for Artinian rings. *Let R be a left (or right) Artinian ring. Then, $J(R)$ is a nilpotent ideal of R (i.e. $J(R)^n = 0$ for some $n > 0$) and is equal to the sum of all nilpotent ideals of R .*

Proof. Suppose $x \in R$ is nilpotent, say $x^n = 0$. Then, $(1 - x)$ is a unit, indeed,

$$(1 - x)(1 + x + x^2 + \cdots + x^{n-1}) = 1.$$

So if I is a nilpotent ideal of R , then every $x \in I$ satisfies condition (iv) of the Jacobson radical theorem. This shows every nilpotent ideal of R is contained in $J(R)$. It therefore just remains to prove that $J(R)$ is itself a nilpotent ideal.

Set $J = J(R)$. Consider the chain

$$J \supseteq J^2 \supseteq J^3 \supseteq \cdots$$

of two-sided ideals of R . Since R is left Artinian, the chain stabilizes, so $J^k = J^{k+1} = \cdots$ for some k . Set $I = J^k$, so $I^2 = I$. We need to prove that $I = 0$.

Well, suppose for a contradiction that $I \neq 0$. Choose a left ideal K of R minimal such that $IK \neq 0$ (use the fact that R is left Artinian). Take any $a \in K$ with $Ia \neq 0$. Then, $I^2a = Ia \neq 0$, so the left ideal Ia of R coincides with K by the minimality of K . Hence, $a \in K$ lies in Ia , so we can write $a = xa$ for some $x \in I$. So, $(1 - x)a = 0$. But $x \in J$, so $1 - x$ is a unit, hence $a = 0$, which is a contradiction. \square

5.4.2. Corollary. *In particular, a left (or right) Artinian ring R is semisimple if and only if it has no non-zero nilpotent ideals.*

The corollary can be applied in particular to commutative rings. In that case, if $x \in R$ is a nilpotent element, the ideal (x) it generates is a nilpotent ideal. So, a *commutative Artinian ring is semisimple if and only if it has no non-zero nilpotent elements*. Now let $G = C_p$, the cyclic group of order p . Maschke's theorem shows that if F is any field of characteristic different from p , then FG is a semisimple. Conversely, suppose F is a field of characteristic p . The group algebra FG is finite dimensional, hence is a commutative Artinian ring. Consider the element

$$1 + x + \cdots + x^{p-1} \in FG$$

where x is a generator of G . We have that

$$(1 + x + \cdots + x^{p-1})^p = 1 + x^p + \cdots + x^{(p-1)p} = 1 + 1 + \cdots + 1 = p = 0.$$

Hence, it is a non-zero nilpotent element. Thus, FG is *not* semisimple in this case.

We end with an important application:

Hopkin's theorem. *Let R be a left Artinian ring and M be a left R -module. The following are equivalent:*

- (i) M is Artinian;
- (ii) M is Noetherian;
- (iii) M has a composition series;
- (iv) M is finitely generated.

Proof. (i) \Rightarrow (iii) and (ii) \Rightarrow (iii). Let $J = J(R)$. Then, J is nilpotent by the second characterization of the Jacobson radical. So, $J^n = 0$ for some n . Consider

$$M \supseteq JM \supseteq J^2M \supseteq \cdots \supseteq J^nM = 0.$$

It is a descending chain of R -submodules of M . Set $F_i = J^iM/J^{i+1}M$. Then, F_i is annihilated by J , hence is a semisimple left R -module. Now, if M is Artinian (resp. Noetherian), so is each F_i , so each F_i is in fact a direct sum of *finitely many* simple R -modules. Thus, each F_i obviously has a composition series, so M does too by the lattice isomorphism theorem.

(iii) \Rightarrow (iv). Let $M = M_1 \supset \cdots \supset M_n = 0$ be a composition series of M . Pick $m_i \in M_i - M_{i+1}$ for each $i = 1, \dots, n-1$. Then, the image of m_i in M_i/M_{i+1} generates M_i/M_{i+1} as it is a simple R -module. It follows that the m_i generate M . Hence, M is finitely generated.

(iv) \Rightarrow (i) is Theorem 5.2.2.

(iii) \Rightarrow (ii) and (iii) \Rightarrow (i). These both follow immediately from the Jordan-Hölder theorem (actually, the Schreier refinement lemma using that any refinement of a composition series is trivial). \square

Now we can show that "Artinian implies Noetherian":

5.4.3. Corollary. *If R is left (resp. right) Artinian, then R is left (resp. right) Noetherian.*

Proof. Apply Hopkin's theorem to the Artinian R -module ${}_R R$. \square