Part C
Semisimplicity

MATH 101B: ALGEBRA II
PART C: SEMISIMPLICITY

We have one week to talk about semisimple rings and semisimple modules (Chapter XVII). A *semisimple R-module* is a finite direct sum of simple modules

$$M = S_1 \oplus \cdots \oplus S_n$$

and a *semisimple ring* is a ring R for which all f.g. modules are semisimple. The main reasons that I am choosing this particular topic in noncommutative algebra is for the study of representations of finite groups which we will do after the break.

If G is a finite group then a representation of G over $\mathbb{C}$ is the same as a module over the group ring $\mathbb{C}[G]$ (also written $\mathbb{C}G$). Once we have the basic definitions it will be very easy to see that $\mathbb{C}[G]$ is a semisimple ring. This makes the representation theory of finite groups elementary.

From now on, all rings will be associative rings with $1 \neq 0$ (which may or may not be commutative) and R-module will be understood to be left R-modules.

Contents

1. Simple rings and modules

Although semisimple rings are not defined to be products of simple rings (this being a theorem and not a definition), it still makes sense to talk about simple rings first.

1.1. Simple rings.

Definition 1.1. *A ring R is called* simple *if it has no nonzero two-sided ideals.*

For example, any field is simple. There is also a noncommutative version of a field:

1.1.1. *division rings.*

Definition 1.2. *A* division ring *is a ring R in which every nonzero element has a two-sided inverse. I.e., for all $a \neq 0 \in R$ there is a $b \in R$ so that $ba = ab = 1$.*

Proposition 1.3. *R is a division ring iff every nonzero element has a left inverse.*

Proof. If every $a \neq 0 \in R$ has a left inverse b (so that $ba = 1$) then b also has a left inverse c with $cb = 1$. But then

$$c = c(ba) = (cb)a = a$$

So b is a two-sided inverse for a, making R a division ring. □

Theorem 1.4. *Division rings are simple.*

Proof. Any nonzero two-sided ideal $I \subseteq D$ would have a nonzero element a. So, Da would contain 1 which is a contradiction. □

1.1.2. *matrix rings.*

Definition 1.5. *For any ring R let $Mat_n(R)$ denote the ring of $n \times n$ matrices (a_{ij}) with coefficients a_{ij} in R. Addition is "coordinate-wise" $(a_{ij}) + (b_{ij}) = (c_{ij})$ where $c_{ij} = a_{ij} + b_{ij}$. Multiplication is matrix multiplication: $(a_{ij})(b_{ij}) = (c_{ij})$ where $c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}$. A tedious and unnecessary computation will show that $Mat_n(R)$ is a ring. (There is an easy proof which we will see later.)*

I will assume that everyone knows how matrices work. There is one point that you should be careful about. Since R is noncommutative, the determinant does not behave the way it should. I.e., there is no function $\det : Mat_n(R) \to R$ so that $\det(A)\det(B) = \det(AB)$.

One thing I should have pointed out is that $Mat_n(D)$ is a free R-module with basis given by the matrices x_{ij} which have a 1 in the ij

position and 0 everywhere else. A matrix with coefficients $a_{ij} \in R$ can be written as

$$(a_{ij}) = \sum a_{ij} x_{ij}$$

Theorem 1.6. *If D is a division ring then $Mat_n(D)$ is simple.*

Proof. If I is a nonzero two-sided ideal in $Mat_n(D)$ then I want to show that $I = Mat_n(D)$. Let $A = (a_{ij})$ be a nonzero element of I. Then one of the entries is nonzero: $a_{ij} \neq 0$. Multiplying on the left by x_{ii} and on the right by the matrix $a_{ij}^{-1} x_{jj}$ we see that

$$x_{ij} = x_{ii} A (a_{ij}^{-1} x_{jj}) \in I$$

This implies that every matrix is in I since, for any $b \in D$ and any $k, \ell \leq n$, we have

$$(b x_{ke}) x_{ij} x_{j\ell} = b x_{k\ell} \in I$$

Taking sums we get any element of $Mat_n(D)$. □

Basically, there are no other examples of simple rings.

1.2. **Simple modules.**

Definition 1.7. *A (left) R-module M is called* simple *if $M \neq 0$ and M has no proper nonzero submodules. ($N \subseteq M$ is* proper *if $N \neq M$.)*

I made some trivial observations without proof:

(1) If $N \subset M$ is a maximal proper submodule then M/N is simple.
(2) M is simple iff 0 is a maximal proper submodule.

Theorem 1.8. *${}_R R$ (R considered as a left R-module) is simple iff R is a division algebra.*

Proof. This is obvious both ways. ($\Leftarrow$) A submodule N of ${}_R R$ is the same as a left ideal. If N is nonzero then it has a nonzero element a with inverse b. Then $ba = 1 \in RN$. So, $RN = N$. ($\Rightarrow$) Conversely, suppose that ${}_R R$ is simple and $a \neq 0 \in R$. Then Ra is a nonzero submodule of R. Therefore, $Ra = R$. So, $1 = ba \in Ra$ and b is a left inverse for a. So, R is a division ring. □

One of the most important theorem about simple modules is also trivial:

Lemma 1.9 (Schur's lemma)**.** *If M, N are simple R-modules and $f : M \to N$ is an R-module homomorphism then either $f = 0$ or f is an isomorphism.*

Proof. The kernel of f is a submodule of M. So it is either 0 or M. If $\ker f = M$ then $f = 0$. If $\ker f = 0$ then f is a monomorphism which means that M is isomorphic to the image of f. But the image $\operatorname{im} f = f(M)$ is a submodule of N. So, there are two possibilities. Either $f(M) = 0$ or $f(M) = N$. The first case is not possible since $M \neq 0$. So, $f(M) = N$ which means that f is onto. But f is also monomorphism. So, f is an isomorphism. □

Theorem 1.10. *The endomorphism ring* $\operatorname{End}_R(M)$ *of a simple module* M *is a division ring.*

At this point I decided to review the definition.

Definition 1.11. *The* endomorphism ring $\operatorname{End}_R(M)$ *of an* R*-module* M *is the set of all* R*-module homomorphisms* $f : M \to M$ *with multiplication defined by composition of functions:* $f \cdot g = f \circ g$ *and pointwise addition:* $(f + g)(x) = f(x) + g(x)$.

Proof of the theorem. If M is simple then Schur's lemma tells us that any nonzero element of $\operatorname{End}_R(M)$ is an isomorphism and thus invertible. □

I had time for one more trivial theorem. First a definition.

Definition 1.12. *For any ring* R *the* opposite ring R^{op} *is defined to be the same set* R *with order of multiplication reversed. In other words, the opposite of the ring* $(R, \cdot, +)$ *is the ring* $(R, \cdot^{op}, +)$ *with the same set* R *and the same addition* $+$ *but with a new multiplication* $\cdot^{op}$ *defined by*

$$a \cdot^{op} b = ba$$

R and R^{op} are said to be *anti-isomorphic*. (So, S is *anti-isomorphic* to R iff $S \cong R^{op}$.)

Theorem 1.13. *For any ring* R *we have* $\operatorname{End}_R({}_RR) \cong R^{op}$.

Proof. An anti-isomorphism $\phi : \operatorname{End}_R({}_RR) \to R$ is given by $\phi(f) = f(1)$ with inverse $\rho : R \to \operatorname{End}_R({}_RR)$ sending $a \in R$ to $\rho(a)$ given by right multiplication by a. (So, $\rho(a)(x) = xa$.) It is easy to see that the mappings ϕ and ρ are inverse to each other. The point is that they reverse the order of multiplication:

$$\rho(ab)(x) = xab = \rho(b)\rho(a)(x)$$

So, they induce an isomorphism $\operatorname{End}_R({}_RR) \cong R^{op}$. □

2. Semisimple modules

2.1. **Finiteness conditions.** We will need to assume some finiteness conditions for modules. These work in the same way that they do for modules over commutative rings.

2.1.1. *Noetherian modules.*

Definition 2.1. *An R-module M is called* Noetherian *if it satisfies the ascending chain condition (ACC) for submodules. This is equivalent to saying that every submodule of M is finitely generated. A ring R is called* left-Noetherian *if ${}_RR$ is a Noetherian module.*

Just as in the commutative case we have:

Theorem 2.2.
1. *If M is Noetherian then every submodule and quotient module of M is Noetherian.*
2. *R is left-Noetherian iff every finitely generated R-module is Noetherian.*

Noetherian modules have lots of *maximal submodules*, by which I mean maximal proper submodules.

Proposition 2.3. *Every proper submodule of a Noetherian module is contained in a maximal submodule.*

Proof. Otherwise, we would get a sequence of larger and larger submodules, contradicting the ACC. □

Sometimes it is enough just to assume that M is finitely generated.

Lemma 2.4 (finite sum lemma). *If a f.g. module M is a sum of submodules $M = \sum_{\alpha \in I} N_\alpha$, then there is a finite subset J of the index set I so that $M = \sum_{\beta \in J} N_\beta$.*

Proof. To say that M is the sum of the submodules N_α is the same as saying that the inclusion maps $N_\alpha \hookrightarrow M$ give an epimorphism

$$\bigoplus_{\alpha \in I} N_\alpha \twoheadrightarrow M$$

Suppose that $x_1, \cdots, x_n$ generate M and, for each i, choose $y_i \in \bigoplus_{\alpha \in I} N_\alpha$ which maps onto x_i. Then each y_i has only finitely many nonzero coordinates. Let $J \subseteq I$ be the set of all $\beta \in I$ so that some y_i has a nonzero β coordinate. Then $M = \sum_{\beta \in J} N_\beta$. □

2.1.2. *Artinian modules.*

Definition 2.5. *An R-module M is called* Artinian *if it satisfies the descending chain condition (DCC) for submodules. A ring R is called* left-Artinian *if ${}_RR$ is an Artinian module.*

Analogous to the corresponding statements for Noetherian modules and with analogous proofs we have the following.

Theorem 2.6.
(1) *Every submodule and quotient module of an Artinian module is Artinian.*
(2) *R is left Artinian iff every f.g. R-module is Artinian.*
(3) *Every nonzero submodule of an Artinian module contains a simple submodule.*

A statement which is dual to the finite sum lemma for Noetherian modules is the following.

Lemma 2.7 (finite intersection lemma). *Suppose that M is an Artinian module and $N = \bigcap_{\alpha \in I} N_\alpha$ is an intersection of submodules. Then there is a finite subset J of the index set I so that $N = \bigcap_{\beta \in J} N_\beta$.*

Proof. Finite intersections form a descending sequence of submodules which stops when it is equal to the infinite intersection. □

Example 2.8. *(1) $\mathbb{Z}$ is a Noetherian $\mathbb{Z}$-module but it is not Artinian. (2) Take the ring*

$$\mathbb{Z}[\tfrac{1}{p}] = \{a/p^n \mid a \in \mathbb{Z}, n \geq 0\}$$

$\mathbb{Z} \subset \mathbb{Z}[1/p]$ is a subring (not an ideal). So the quotient $\mathbb{Z}[1/p]/\mathbb{Z}$ is a $\mathbb{Z}$-module (not a ring). This module is Artinian but not Noetherian (but there is a theorem that says that all Artinian rings are Noetherian).

2.2. Definition of semisimple.

Definition 2.9. *A f.g. R-module M is called* semisimple *if it satisfies one of the following equivalent definitions.*
(1) *M is a direct sum of simple modules.*
(2) *M is a sum of simple submodules.*
(3) *Every submodule of M is a direct summand.*

First I need a trivial lemma.

Lemma 2.10. *Suppose that N, S are submodules of any module M where S is simple. Then $N + S$ is either equal to N or to $N \oplus S$. In both cases, N is a direct summand of $N + S$.*

Proof. $N \cap S$ is a submodule of S. So, it is either 0 or S. In the first case, $N + S = N \oplus S$. In the second case, $N + S = N$. □

Proof of equivalence of definitions. Clearly, (1) implies (2). Also, by the finite sum lemma (2.4), (2) implies

(2′) M is a finite sum of simple submodules.

Since every simple module is generated by one element (any nonzero element), condition (2′) includes the assumption that M is finitely generated.

(2′) ⇒ (3) Suppose that $N \subseteq M$ and $M = \sum_{i=1}^{n} S_i$. For each $k \leq n$ let

$$N_k = N + S_1 + \cdots + S_k$$

Lemma 2.10 says that N_k is a direct summand of $N_{k+1} = N_k + S_{k+1}$ for every k. Therefore, N is a direct summand of $N_n = M$.

(3) ⇒ (1). Since any submodule $N \subseteq M$ is a summand: $M = N \oplus K$, $N \cong M/K$ is also a quotient of M. Therefore, every submodule of M is f.g. making M Noetherian. If $M = M/0$ is not a direct sum of simple modules then, by the ACC, there is a maximal submodule K so that M/K is not a direct sum of simple modules. But then $M = N \oplus K$ by assumption. So, $N \cong M/K$ is not a direct sum of simple modules. In particular, N is not simple. So, it has a nonzero proper submodule N_1. But then we must have

$$N = N_1 \oplus N_2$$

($M = N_1 \oplus L$ and we can take $N_2 = L \cap N$). Since $K \subset K \oplus N_1$, the quotient $M/(K \oplus N_1) \cong N_2$ is a direct sum of simple modules by maximality of K. Similarly, N_1 is a direct sum of simple modules. So, $N = N_1 \oplus N_2 \cong M/K$ is a direct sum of simple modules and we have a contradiction which shows that (1) must hold. □

2.3. Unique decomposition.

Theorem 2.11. *The simple summands of a semisimple R-module are uniquely determined up to isomorphism. In other words, if*

$$M = S_1 \oplus \cdots \oplus S_n = T_1 \oplus \cdots \oplus T_m$$

where S_i, T_j are simple submodules of M, then $n = m$ and $S_i \cong T_{\sigma(i)}$ for some permutation σ of n.

Proof. For each j let

$$N_j = T_1 \oplus \cdots \oplus \widehat{T_j} \oplus \cdots \oplus T_m$$

This is a maximal submodule of M since $M/N_j \cong T_j$ is simple. Also, $\bigcap N_j = 0$. So, there is some j so that $S_n \not\subseteq N_j$. Since S_n is simple, this implies that $S_n \cap N_j = 0$. Since N_j is maximal we conclude that $M = S_n \oplus N_j$ and therefore,

$$M/S_n \cong S_1 \oplus \cdots \oplus S_{n-1} \cong N_j = T_1 \oplus \cdots \oplus \widehat{T_j} \oplus \cdots \oplus T_m$$

The theorem follows by induction on n. □

Definition 2.12. *Define the* length $\ell(M)$ *of a semisimple module M to be the number of simple summands in any decomposition $M = \bigoplus S_i$.*

Corollary 2.13. *Submodules and quotient modules of semisimple modules are semisimple. Furthermore, $\ell(N) + \ell(M/N) = \ell(M)$ for any submodule N of a semisimple module M.*

Proof. By (3), $M = N \oplus K$ for some submodule $K \cong M/N$. Each a quotient of M and therefore a sum of finitely many simple modules. So, they are both semisimple. Decomposing N, K into direct sums of n, m simple modules, we get a decomposition of $M = N \oplus K$ into $n+m$ simple modules. So,

$$\ell(M) = n + m = \ell(N) + \ell(M/N)$$

□

Corollary 2.14. *Semisimple modules are both Noetherian and Artinian.*

Proof. For any increasing or decreasing sequence of submodules the lengths increase or decrease. □

2.4. **Jacobson radical.** An Artinian module M is semisimple iff its Jacobson radical is zero.

Definition 2.15. *The* Jacobson radical rM *of any R-module M is defined to be the intersection of all maximal (proper) submodules of M.*

Proposition 2.16 (Naturality of rM)**.** *If $f : M \to N$ is a homomorphism of R-modules, then $f(rM) \subseteq rN$.*

Proof. For any maximal submodule $L_\alpha \subseteq N$, $f^{-1}(L_\alpha)$ is either equal to M or to a maximal submodule of M. Therefore,

$$f^{-1} \bigcap L_\alpha = \bigcap f^{-1}(L_\alpha)$$

contains rM which is what we wanted to show. □

Theorem 2.17. *Suppose that M is an Artinian R-module. Then*

(1) *M/rM is semisimple.*
(2) *M is semisimple iff $rM = 0$.*

Proof. By the finite intersection lemma (2.7), the Jacobson radical of M is a finite intersection of maximal submodules: $rM = \bigcap N_i$. Thus we have an exact sequence:

$$0 \to rM \to M \to \bigoplus M/N_i$$

Since each N_i is maximal, M/N_i is simple. So, M/rM is also semisimple, being isomorphic to a submodule of $\bigoplus M/N_i$.

This shows that $rM = 0$ implies M is semisimple. Conversely, suppose $M = \bigoplus S_i$. Then the kernel of each projection $M \twoheadrightarrow S_i$ is a maximal submodule N_i and $rM \subseteq \bigcap N_i = 0$. □

3. Semisimple rings

3.1. **Jacobson radical of a ring.** The theorem is that an Artinian ring is semisimple if and only if its Jacobson radical is zero. But we need to define the terms.

Definition 3.1. *The* Jacobson radical *rR of a ring R is defined to be the intersection of all maximal left ideals. (This is the same as the Jacobson radical of $_RR$.)*

As a special case of the previous theorem we have the following.

Corollary 3.2. *If R is a left Artinian ring then $_RR$ is semisimple iff $rR = 0$.*

Definition 3.3. *A ring R is called* semisimple *if every f.g. R-module is semisimple.*

By what we know, it is clear that all f.g. modules are semisimple if and only if $_RR$ itself is semisimple. This gives the following.

Corollary 3.4. *A ring is semisimple iff it is left-Artinian (and Noetherian) and its Jacobson radical is zero.*

Proof. ($\Leftarrow$) This follows from the previous corollary.

($\Rightarrow$) If R is a semisimple ring, $_RR$ is a semisimple module which implies that it is Artinian and Noetherian and its radical is zero. □

Theorem 3.5. *The Jacobson radical of R is a two-sided ideal.*

Proof. rR is clearly a left ideal. So, let $a \in R$. Then right multiplication by a is an R-module homomorphism $\rho(a) : {}_RR \to {}_RR$. By naturality of r (2.16) this implies that $(rR)a \subseteq rR$. So, rR is also a right ideal. □

Corollary 3.6. *Simple Artinian rings are semisimple.*

Corollary 3.7. *Division rings and matrix rings over division rings are semisimple.*

Proof. Division rings are clearly Artinian. So, they they are semisimple. The matrix ring $Mat_n(D)$ is finitely generated as a D-module and therefore is Artinian (since all left ideals are also D-submodules). So, it is also semisimple by the previous corollary. □

3.2. **Wedderburn structure theorem.**

Theorem 3.8 (Wedderburn structure theorem)**.** *A ring R is semisimple if and only if it is a finite product of matrix rings over division rings:*

$$R \cong \prod Mat_{n_i}(D_i)$$

To show that these products are semisimple we need the following lemma.

Lemma 3.9. *If R, S are semisimple rings then their product $R \times S$ is semisimple.*

Proof. The unit $1 = (1, 1)$ of the ring $R \times S$ can be written as a sum:

$$1 = (1, 0) + (0, 1) = e_1 + e_2$$

where e_i are central, orthogonal idempotents. (*Central* means $e_i x = x e_i$ for all x, *orthogonal* means $e_1 e_2 = 0$ and *idempotent* means $e_i^2 = e_i$.) If M is any $R \times S$ module then any $x \in M$ can be written as $x = 1x = e_1 x + x_2 x$. Thus

$$M = e_1 M \oplus e_2 M.$$

Since $e_1 S = S e_1 = 0$, the action of S on $e_1 M$ is zero. So, the action of $R \times S$ on $e_1 M$ factors through $(R \times S)/S \cong R$ and the action of $R \times S$ on $e_2 M$ factors through S. If M is f.g. then $e_1 M, e_2 M$ are finitely generated modules over R, S respectively. So they are semisimple. This makes M semisimple. □

This lemma, together with Corollary 3.7, proves that the rings named in the structure theorem are all semisimple.

3.2.1. *endomorphisms.* Suppose that M is a semisimple R-module. Then we want to show that the endomorphism ring $\text{End}_R(M)$ is the opposite of one of the rings in the Wedderburn structure theorem. This will prove the structure theorem because of the observation (Theorem 1.13) that $\text{End}_R({}_RR) \cong R^{op}$: If R is semisimple then ${}_RR$ is a semisimple R-module. This will imply that $\text{End}_R({}_RR)$ is the opposite of one of the rings in the structure theorem and therefore R is one of those rings.

In the decomposition $M = \bigoplus S_i$, some of the simples S_i may be isomorphic to each other. We use the notation nS_i to denote a direct sum of n copies of the simple module S_i. Then we can write:

$$M \cong \bigoplus_{i=1}^{m} n_i S_i$$

where the S_i are nonisomorphic.

By Schur's lemma, there are no homomorphisms from S_i to S_j for $i \neq j$. Therefore,

$$\text{End}_R(M) \cong \prod_{i=1}^{m} \text{End}_R(n_i S_i)$$

So, it suffices to show the following lemma.

Lemma 3.10. (1) *If S is a simple R-module then*

$$\text{End}_R(nS) \cong Mat_n(D)$$

where $D = \text{End}_R(S)$.

(2) *If D is a division algebra then D^{op} is also a division algebra.*

(3) $Mat_n(D)^{op} \cong Mat_n(D^{op})$.

Proof. (1) An isomorphism $\phi : \text{End}_R(nS) \to Mat_n(D)$ is given as follows. For any $f : nS \to nS$ let $\phi(f) \in Mat_n(D)$ be the matrix with ij-coordinate (in $D = \text{End}_R(S)$) given by the composition

$$p_i \circ f \circ t_j : S \xrightarrow{t_j} nS \xrightarrow{f} nS \xrightarrow{p_i} S$$

where $t_j : S \to nS$ is the inclusion of the jth summand and $p_i : nS \to S$ is the projection to the ith summand.

This is a homomorphism since

$$\phi(f \circ g) = (p_i \circ f \circ g \circ t_j) = (p_i \circ f \circ \sum t_k \circ p_k \circ g \circ t_j)$$

$$= (p_i \circ f \circ t_k)(p_k \circ g \circ t_j) = \phi(f)\phi(g)$$

This uses the equation $\sum t_k \circ p_k = id$ which should be familiar from your very first assignment.

To show that ϕ is an isomorphism, we give the inverse: $\phi^{-1}(f_{ij}) = \sum t_i \circ f_{ij} \circ p_j$

(2) is obvious. To show (3), an anti-isomorphism

$$\tau : Mat_n(D) \xrightarrow{\approx} Mat_n(D^{op})$$

is given by transpose: $\tau(f) = f^t$ is the matrix with ij-coordinate equal to f_{ji}. □

3.2.2. *algebraically closed fields.* We want to talk about algebras over algebraically closed fields.

Definition 3.11. *An* algebra *over a field K is defined to be a ring A which contains the field K in its center. (The* center *of A is the set of elements which commute with all other elements of A. This is a subring but not an ideal.)*

Since the center of A acts on all A-modules, every module over a K-algebra will be a vector space over K. If a K-algebra A is finite dimensional as a vector space over K, then it is clearly Artinian.

Theorem 3.12. *The only finite dimensional division algebra over an algebraically closed field K is K itself.*

Proof. Suppose that D is an n dimensional division algebra over an algebraically closed field K. Take any $a \in D$. Right multiplication by a gives a K-linear endomorphism of the n-dimensional vector space D:

$$\rho(a) : D \cong K^n \to D \cong K^n$$

Since K is algebraically closed, it contains all of the eigenvalues (roots of the characteristic polynomial) of this endomorphism. Let $\lambda \in K$ be one of these eigenvalues. Then right multiplication by $a - \lambda$ is singular, i.e., there is an $x \neq 0 \in D$ (the eigenvector) so that $x(a - \lambda) = 0$. But D is a division algebra. So, this implies that $a = \lambda \in K$. Since $a \in D$ was arbitrary, this implies that $D = K$. □

Corollary 3.13. *The only semisimple algebras over $\mathbb{C}$ are finite products of matrix algebras:*

$$\prod Mat_{n_i}(\mathbb{C}).$$