Lecture Notes on Ring Theory

Arturo De Faveri

November 2021

> Don't know much about algebra
>
> Sam Cooke, *Wonderful World*

1 Caveats

We assume that the reader possesses elementary notions about rings and modules.

These are notes about r*i*ngs, not about rngs: we tacitly assume that every ring has a unit. Moreover the product $\cdot$ is associative by hypothesis. Normally we don't require that $1 \neq 0$. This trick allows us to treat 0 as a r*i*ng (and a morphism) without being inconsistent.

We won't bother with avoiding sloppy notation: 1 is the unit of every ring as well as the identity function between any two objects; 0 is the zero of every etc.

Throughout our discussion we shall call a left module over a ring R, simply a R-module. The reader may generalize our treatment to the case of right modules.

Alas, lots of important rings, such as local or artinian rings, are relegated to exercises. Our apologies.

Last but not least, these notes are far from being original. They just fill in the details of lectures given by Prof Yu Chen at Torino. For the most it's just been copying and pasting from classic books such as[1]:

- Serge Lang, *Algebra*
- Joseph J. Rotman, *Advanced Modern Algebra*
- Frank W. Anderson & Kent R. Fuller, *Rings and Categories of Modules*

Here we list a couple of important things that don't fit naturally the subsequent topics.

Exercises

Exercise 1.1. If E is an abelian group, the set of endomorphisms $\mathsf{End}(E)$ is a ring with pointwise addition and composition. Let E be an abelian group. Prove that E is a R-module iff there is a ring morphism

$$f : R \to \mathsf{End}(E).$$

[1] However, if you find a typo or a mathematical error – it's more than possible! – you can email me at `arturo dot defaveri at edu dot unito dot it`

Deduce that a R-module is also an S-module whenever there is a ring morphism $g : S \to R$.

Exercise 1.2. Let R be a ring. The ring R^{op} has same carrier and sum as R but the products are reversed. Prove that $R^{\text{op}} \simeq \mathsf{End}_R(R)$. (If E is an R-module – and R is – $\mathsf{End}_R(E)$ is still a ring as above).

2 Free Modules and Exact Sequences

Let R be a ring and M an R-module. For a subset S of M we say that S generates M ($M = \langle S \rangle$) if every $x \in M$ can be written as a linear combination of elements of S. If S is finite M is said to be **finitely generated**. S is called **independent** if there is no nonzero linear combination in S with nonzero coefficients. An independent set of generators is called **basis**.

The category of R-modules has products and coproducts: direct products and sums. Let $\{M_i\}$, $i \in I$, be a family of R-modules. The direct product consists of all sequences (m_i) with each $m_i \in M_i$; the direct sum of all sequences (m_i) with each $m_i \in M_i$ and almost all m_i null. Operations are defined componentwise. Finite products and coproducts coincide in the category of R-modules. Note however that the category of r$i$ngs doesn't have coproducts (i.e. the direct sum of rings with componentwise operations is not necessarily a ring).

A sequence of modules and morphisms is something like

$$M \xrightarrow{f} N \xrightarrow{g} P.$$

It's said to be **exact** if $\operatorname{img} f = \ker g$. If X, Y are R-modules, then $\mathsf{Hom}_R(X, Y)$ is an R-module. We have:

$$\mathsf{Hom}_R(X \oplus Y, Z) \simeq \mathsf{Hom}_R(X, Z) \oplus \mathsf{Hom}_R(Y, Z)$$
$$\mathsf{Hom}_R(X, Y \oplus Z) \simeq \mathsf{Hom}_R(X, Y) \oplus \mathsf{Hom}_R(X, Z)$$

Theorem 2.1. *Let $0 \to M \xrightarrow{f} N \xrightarrow{g} P \to 0$ be an exact sequence of R-modules. Then the following are equivalent:*

- *there is a morphism $\varphi : P \to N$ such that $g\varphi = 1$;*
- *there is a morphism $\psi : N \to M$ such that $\psi f = 1$.*

If one of this condition is met: $N = \operatorname{img} f \oplus \ker \psi = \ker g \oplus \operatorname{img} \varphi \simeq M \oplus P$.

Proof. We just prove that if there is a morphism $\varphi : P \to N$ such that $g\varphi = 1$, then $N = \ker g \oplus \operatorname{img} \varphi$. Let $x \in N$. Then $x - \varphi g(x) \in \ker g$. Hence $N = \ker g + \operatorname{img} \varphi$. We show that $\ker g \cap \operatorname{img} \varphi = 0$. Suppose that $x \in \ker g$ and $x = \varphi(y)$ for some $y \in P$. Then $0 = g(x) = g\varphi(y) = y$ and $x = 0$. □

When these conditions are satisfied the exact sequence is said to **split**.

Corollary 2.2. *Let N, P be R-modules with P free. Let $g : N \to P$ be surjective. There is a free submodule M of N such that $M \simeq P$ and $N = \ker g \oplus M$.*

Proof. If $\{y_i\}_{i \in I}$ is a basis of P, for each y_i let $x_i \in N$ such that $g(x_i) = y_i$. $M := \langle \{x_i\} \rangle$ is free. Extend by linearity the map $y_i \mapsto x_i$ and call it φ. Since $g\varphi = 1$ the sequence $0 \to M \hookrightarrow N \xrightarrow{g} P \to 0$ splits. □

Let M be a free module over R. If $\{x_i\}_{i\in I}$ is a basis of M, $M = \bigoplus Rx_i$. Let $\mathfrak{a}$ be a two-sided ideal of R. $\mathfrak{a}M$ is a submodule of M. Moreover each $\mathfrak{a}x_i$ is a submodule of Rx_i. We have

$$\frac{M}{\mathfrak{a}M} \simeq \bigoplus \frac{Rx_i}{\mathfrak{a}x_i}$$

and each $Rx_i/\mathfrak{a}x_i$ is isomorphic to $R/\mathfrak{a}$ (as R-module).

An R-module E is called **principal** if there is $x \in E$ such that $E = Rx$. The map $R \to Rx$, $a \mapsto ax$ is a linear map whose kernel is a left ideal of R, $\mathfrak{a}$. In particular $E \simeq R/\mathfrak{a}$.

Remark 2.3. Let $\{v_i\}$, $i \in I$, be a set of generators for E (at worst we take $I = E$!). For each i let F_i be a free module with basis e_i, so that $F_i \simeq R$ as R-modules. Let $F := \bigoplus F_i$. The map $f : F \to E$ such that $f(e_i) = v_i$ is surjective. Thus every module is a factor module of a free module.

Exercises

Exercise 2.1. Let $M = K + L$ and let $f : M \to N$ be a surjective linear map of R-modules. Prove that if $\ker f = K \cap L$, $N = f(K) \oplus f(L)$.

Exercise 2.2. Complete the details of Theorem 2.1.

3 Modules and Rings Decomposition

Fix a ring R. All modules are going to be (left) R-modules and all linear maps R-linear maps.

An element e of a ring is called **idempotent** if $e^2 = e$. Observe that in this case $1 - e$ is idempotent as well. Two idempotents e_1, e_2 are **orthogonal** if $e_1e_2 = 0 = e_2e_1$. A nonzero idempotent e is **primitive** if whenever $e = e_1 + e_2$ for some idempotents e_1, e_2 then at least one is zero. A set $\{e_1, \dots, e_n\}$ of idempotents is **complete** if $1 = e_1 + \cdots + e_n$.

Let $M_1, \dots, M_n$ be submodules of a module M. We say that they **generate** M if $M_1 + \cdots + M_n = M$ and that they are **independent** if $(M_1 + \cdots + M_i) \cap M_{i+1} = 0$ for each i. Consider the map

$$s : M_1 \times \cdots \times M_n \to M$$

given by $s(x_1, \dots, x_n) = x_1 + \cdots + x_n$. Then s is injective if the submodules are independent, and surjective if they generate M. In case it's a bijection we get

$$M = M_1 \oplus \cdots \oplus M_n.$$

Suppose that it's indeed the case that $M = M_1 \oplus \cdots \oplus M_n$. Let p_i be the projection along the i-th coordinate. Define $e_i \in \mathsf{End}(M)$ as $x \mapsto p_i(x)$. The following trivial remarks are pivotal:

- $e_i^2 = e_i$;
- $e_1 + \cdots + e_n = 1$;
- $M_i = Me_i$.

A nonzero module is **indecomposable** if M and 0 are its only direct summands.

Lemma 3.1. *Let $e \in \operatorname{End} M$ be idempotent. $M = Me \oplus M(1-e)$. In particular M is indecomposable iff $0, 1$ are the only idempotents in $\operatorname{End} M$.*

Proof. For all $x \in M$, $x = xe + x(1-e)$. Moreover if $xe = y(1-e)$, then $xe = xe^2 = (y(1-e))e = 0$. □

Corollary 3.2. *Let M_i be submodules of M. $M = M_1 \oplus \cdots \oplus M_n$ with each M_i indecomposable iff there is complete set $e_1, \dots, e_n$ of pairwise orthogonal, primitive elements in $\operatorname{End} M$ such that $Me_i = M_i$.*

Proof. If $e_1, \dots, e_n$ are as claimed, each $x \in M$ writes uniquely as $x = xe_1 + \cdots + xe_n$. Since e_i is primitive M_i is indecomposable.

Conversely, let e_i defined as the projection along the i-th coordinate. $1 = e_1 + \cdots + e_n$; orthogonality and primitiveness follow. □

We're interested now in decomposing a ring R. The goal is to find a decomposition in terms of two-sided ideal, the case of left ideals being already covered by the paragraphs above.

Assume that R, as left R-module, has a decomposition as a direct sum of two-sided ideals

$$R = R_1 \oplus \cdots \oplus R_n.$$

We know that there is a (unique) set $\{u_1, \dots, u_n\}$ of orthogonal idempotents in R such that $1 = u_1 + \cdots + u_n$ and $R_i = Ru_i$. Since R_i is a two-sided ideal, $u_i R \subseteq R_i$, thus for $i \neq j$ $u_i R u_j \subseteq u_i R \cap Ru_j \subseteq R_i \cap R_j = 0$. If $i = j$

$$u_i r = u_i r(u_1 + \cdots + u_n) = u_i r u_i = (u_1 + \cdots + u_n) r u_i = r u_i$$

implies that each u_i is a central idempotent and $R_i = Ru_i = u_i R = u_i R u_i$ a ring with identity u_i.

Conversely, if $\{u_1, \dots, u_n\}$ is a complete set of nonzero central idempotents then $R_i = Ru_i$ is a two sided ideal and $R = R_1 \oplus \cdots \oplus R_n$ (as a left but also as a right R-module!). We call this a **ring decomposition**[2].

If $R = R_1 \oplus \cdots \oplus R_n$ is a ring decomposition of R and $\{u_1, \dots, u_n\}$ are the associated central idempotents, then the map $r \mapsto (ru_1, \dots, ru_n)$ yields

$$R \simeq R_1 \times \cdots \times R_n.$$

Vice versa, if $R_1, \dots, R_n$ are rings and $i_1, \dots, i_n$ the correspondent injcections into $R_1 \times \cdots \times R_n$,

$$R_1 \times \cdots \times R_n \simeq i_1(R_1) \oplus \cdots \oplus i_n(R_n)$$

and the central idempotents are $i_j(1)$.

Theorem 3.3. *Let $R_1, \dots, R_n$ be nonzero two-sided ideals of R Then*

$$R = R_1 \oplus \cdots \oplus R_n$$

as a ring decomposition iff there is a set of pairwise orthogonal central idempotents $u_1, \dots, u_n \in R$ with $u_1 + \cdots + u_n = 1$ and $R_i = Ru_i$. In particular R is indecomposable as a ring iff 1 is the only nozero central idempotent.

[2] $R = R_1 \oplus \cdots \oplus R_n$ is an abuse of notation. We may also write $R = R_1 + \cdots + R_n$.

In general a ring doesn't have a ring decomposition into *indecomposable* rings. R does have such a decomposition when R (as left R-module) has a decomposition of whose associated idempotents are primitive. This is the method for determining such a decomposition. Assume that $R = Re_1 \oplus \cdots \oplus Re_n$ is *a* decomposition of R and let $\{e_1, \ldots, e_n\}$ be the associated idempotents. Let $e_i \sim e_j$ if there is e_k such that $e_k R e_i \neq 0$ and $e_k R e_j \neq 0$. Let $\approx$ be the transitive closure of $\sim$.

If u is a nonzero central idempotent and $ue_i \neq 0$, then ue_i and $(1-u)e_i$ are orthogonal idempotents such that $e_i = ue_i + (1-u)e_i$. Since e_i is primitive $ue_i = e_i$. If in addition $e_k R e_i \neq 0$ then $ue_k R e_i = e_k R e_i$ and $ue_k \neq 0$. Thus if $e_j \sim e_i$ (or $e_j \approx e_i$), then $ue_i \neq 0$ iff $ue_j \neq 0$.

Let $u_i := \sum_{E_i} e_j$ where E_i is a $\approx$ equivalence class. u_i is a nonzero idempotent and $\{u_1, \ldots, u_m\}$ is complete and pairwise orthogonal. We summarize all this in the following theorem (which we don't prove).

Theorem 3.4. *Let $\{e_1, \ldots, e_n\}$ be a complete set of pairwise orthogonal and primitive idempotents of R. Let u_i as above. $\{u_1, \ldots, u_m\}$ is a complete set of pairwise orthogonal central idempotents. R decomposes uniquely as*

$$u_1 R u_1 + \cdots + u_m R u_m$$

and each summand $u_i R u_i$ is indecomposable.

Exercises

Exercise 3.1. Let B be a boolean ring (a ring whose all elements are idempotent). Suppose that there is a set $e_1, \ldots, e_n \in B$ of pairwise orthogonal primitive idempotents with $1 = e_1 + \cdots + e_n$. Prove that if $a \in B$ is non-zero, then there exists a unique subset $\{i_1, \ldots, i_m\} \subseteq \{1, \ldots, n\}$ such that $a = e_{i_1} + \ldots + e_{i_m}$.

Deduce the following: *Let $R = R_1 + \cdots + R_n$ be a ring decomposition of R with each $R_1, \ldots, R_n$ indecomposable as a ring. Let $u_1, \ldots, u_n$ be the central idempotents of this decomposition. If $R = S_1 + \cdots + S_m$ is a ring decomposition of R with associated central idempotents $v_1, \cdots, v_m$, then there is a partition $A_1, \ldots, A_m$ of $\{1, \ldots, n\}$ such that $v_i = \sum_{A_i} u_j$. In particular $S_i = \sum_{A_i} R_j$.*

Exercise 3.2. A ring R is said to be **local** if it has a unique two-sided maximal ideal. Call it I. Prove that $I = R \setminus R^*$, where R^* is the set of invertible elements. Let M be a R-module. Deduce that if $\mathsf{End}_R(M)$ is local, then M is indecomposable.

4 Modules over a Principal Ring

By an **entire** ring we mean a commutative ring in which $1 \neq 0$ and without zero-divisors. A **principal ring** is an entire ring whose ideals are principal. Let R be a principal rings. Modules are left R-modules and linear maps are R-linear.

If F is a free module with basis $\{x_i\}_{i \in I}$, the cardinality of I is uniquely determined, and is called the **dimension** of F. Assuming that the dimension of a vector space is a well-defined cardinal number, this is proved by taking a prime element p in R: F/pF is a vector space over the field R/pR and the dimension is the same.

Theorem 4.1. *Let F be a free module and M a submodule. M is free and* $\dim M \leq \dim F$.

Proof. We prove the statement by induction on $n = \dim F$[3]. If $n = 1$, then $F \simeq R$. Thus, M is isomorphic to 0 or R.

Let's prove the inductive step. If $\{x_1, \dots, x_{n+1}\}$ is a basis of F, define $F_n := \langle x_1, ..., x_n \rangle$, and let $M_n := M \cap F_n$. M_n is a free module of dimension $\leq n$. Now

$$\frac{M}{M_n} = \frac{M}{M \cap F_n} \simeq \frac{M + F_n}{F_n} \leq \frac{F}{F_n} \simeq R.$$

By the base step, either M/M_n is isomorphic to 0 or to R. In the first case, $M = M_n$, and we're done. In the second case, by Corollary 2.2 $M = M_n \oplus \langle m \rangle$ for some $m \in M$. Thus M is free of dimension $\leq n+1$. □

Corollary 4.2. *Let E be a finitely generated module and M a submodule. Then M is finitely generated.*

Proof. If $E = \langle v_1, \dots, v_n \rangle$ we consider a free module F with basis $\{x_1, \dots, x_n\}$. The map $x_i \mapsto v_i$ is linear. The preimage of M in F is free and hence finitely generated so that M is finitely generated too. □

A free one-dimensional module is thus isomorphic to R and called **cyclic**.

x in a module M is said to be a **torsion** element if there a nonnull coefficient in R such that $ax = 0$. Let M_{tor} be the submodule of torsion elements. We say that M is a **torsion module** if $M = M_{\text{tor}}$ and that M is **torsion free** if $M_{\text{tor}} = 0$.

Lemma 4.3. *If M is a finitely generated torsion free module, then M is free.*

Proof. Let $M = \langle y_1, \dots, y_m \rangle$ and let $\{v_1, \dots, v_n\}$ be a maximal linearly independent subset of these generators. If y is one of these generator there are $a, b_i \in R$ (not all zero) such that

$$ay + b_1 v_1 + \ldots + b_n v_n = 0.$$

But then $a \neq 0$ and thus $ay \in \langle v_1, \dots, v_n \rangle$. Let $a_j \neq 0$ the correspondent a of each y_j, $j = 1, \dots, m$, such that $a_j y_j \in \langle v_1, \dots, v_n \rangle$. Let $a := a_1 \cdots a_m$ the product of these coefficients. aM is contained in $\langle v_1, \dots, v_n \rangle$ and thus is free. But M is torsion free: the map $x \mapsto ax$ is injective so that $M \simeq aM$. □

Theorem 4.4. *Let E be a finitely generated module. Then E/E_{tor} is free. Moreover, there is a free submodule $M \leq E$ such that $E = E_{\text{tor}} \oplus M$.*

Proof. We prove that E/E_{tor} is torsion free and we apply the lemma (clearly E/E_{tor} is finitely generated). Let $X := x + E_{\text{tor}}$ for some $x \in E$. Let b a nonnull coefficient such that $bX = 0$. Then $bx \in E_{\text{tor}}$ and there is a nonnull $c \in R$ such that $cbx = 0$. Thus $x \in E_{\text{tor}}$ and $X = 0$.

The map $E \to E/E_{\text{tor}}$ is surjective. We can apply Corollary 2.2 to obtain the second part of the statement. □

As a corollary we get that the dimension of such submodule M is uniquely determined ($M \simeq E/E_{\text{tor}}$). This number is called the **rank** of E.

Recall that the **annihilator** of a subset $S \subseteq E$ is the ideal $\mathsf{Ann}_R S$ of R given by those coefficients that zero all the elements of S. In particular we have: $\mathsf{Ann}_R x = \langle a \rangle$ and $\mathsf{Ann}_R E = \langle b \rangle$. We say that a is a **period**

[3] If the dimension of F is not finite then one enumerates the basis and employs transfinite induction.

of x (and b of E). A period is determined up to multiplication by a unit (whence we shall mostly say *the* period). The period of a torsion module E is positive, and it's not 1 if $E \neq 0$.

$c \in R$, $c \neq 0$, is called **exponent** for x (for E) if $cx = 0$ ($cE = 0$). Let E_c be the submodule of elements with exponent c. Let p being prime we denote by $E(p)$ the submodule of elements with exponent a power of p.

Theorem 4.5. *Let E be a finitely generated nonzero torsion module with period $a = p_1^{r_1} \cdots p_n^{r_n}$. Then*

$$E = E(p_1) \oplus \cdots \oplus E(p_n).$$

Proof. We argue inductivey: let $a = bc$ with b, c coprime. Let $x, y \in R$ such that $1 = xb + yc$. We show that $E = E_b \oplus E_c$. Let $z \in E_b \cap E_c$. Then $z = z(xb + yc) = 0$. Moreover, let $z = xbz + ycz$. $xbz \in E_c$ because $cxbz = axz = 0$; $ycz \in E_b$. □

$y_1, \dots, y_m \in E$ are **independent** if whenever the expression $a_1 y_1 + \cdots + a_m y_m$ with coefficient in R is zero then $a_i y_i = 0$ for all i. This is equivalent to require that the module $\langle y_1, \dots, y_m \rangle$ has decomposition

$$\langle y_1, \dots, y_m \rangle = \langle y_1 \rangle \oplus \cdots \oplus \langle y_m \rangle.$$

Lemma 4.6. *Let E be a torsion module with exponent p^r and $x \in E$ an element with period p^r. Let $Y_1, \dots, Y_m$ independent elements of $E/\langle x \rangle$. There is a representative y_i of Y_i with same period such that $x, y_1, \dots, y_m$ are independent.*

Proof. Let Y have period p^n and y be a representative. Since $p^n Y = 0$, then $p^n y \in \langle x \rangle$: $p^n y = p^s cx$ with p and c coprime and $s \leq r$. If $s = r$ we are done. If $s < r$, then $p^s cx$ has period p^{r-s} and y has period p^{n+r-s}. Since p^r is an exponent of E, $n + r - s \leq r$. Thus $n \leq s$; $y - p^{s-n} cx$ is a representative of Y with same period. As to the last statement, suppose that

$$ax + a_1 y_1 + \cdots + a_m y_m = 0.$$

Then $a_1 Y_1 + \cdots a_m Y_m = 0$. By hypothesis $a_i Y_i = 0$. If p^{r_i} is the period of Y_i, then p^{r_i} divides a_i. Then $a_i y_i = 0$ and finally $ax = 0$. □

Each $E(p)$ can be written as a direct sum

$$E(p) = \frac{R}{\langle p^{r_1} \rangle} \oplus \cdots \oplus \frac{R}{\langle p^{r_s} \rangle}$$

with $1 \geq r_1 \geq \cdots \geq r_s$. Observe that $E(p) =: E$ is finitely generated. Let $x_1 \in E$ with period p^{r_1} for some prime p and maximal r_1. Consider $E/\langle x_1 \rangle$. $(E/\langle x_1 \rangle)_p$ is a vector space over R/pR, whose dimension is strictly less than the dimension of E_p. If $Y_1, \dots, Y_m$ are linearly independent elements of $(E/\langle x_1 \rangle)_p$ then lemma above implies that $\dim E_p \geq m + 1$: we can always find an element of $\langle x_1 \rangle$ with period p independent of $y_1, \dots, y_m$. Then we go on by induction: there are $X_2, \dots, X_s$ with periods $p^{r_2}, \dots, p^{r_s}$ such that $r_2 \geq \ldots \geq r_s$. By lemma above there are representatives $x_2, \dots, x_s$ with period p^{r_i} and such that $x_1, \dots, x_s$ are independent. Since r_1 is maximal, $r_1 \geq r_2$.

The decomposition is essentially unique, as the following result (which we don't prove) illustrates.

Theorem 4.7. *Let E be a finitely generated nonzero torsion module. Then*

$$E \simeq \frac{R}{\langle q_1 \rangle} \oplus \cdots \oplus \frac{R}{\langle q_r \rangle}$$

where each q_i is a nonzero element of the ring. Moreover $q_1 \mid q_2 \mid \cdots \mid q_r$ and the sequence of ideals $\langle q_1 \rangle, \dots, \langle q_r \rangle$ is uniquely determined.

The ideals $\langle q_1 \rangle, \dots, \langle q_r \rangle$ are called **invariants** of E.

Exercises

Exercise 4.1. Deduce the structure theorem for finite abelian groups: every finite abelian group can be expressed as the direct sum of cyclic subgroups of prime-power order. (Hint: a group is a $\mathbb{Z}$-module).

5 Simple Modules and Rings

A **division ring** is a ring in which $1 \neq 0$ and such that every nonnull element has an inverse. A commutative division ring is a field. A module over a division ring is also called **vector space**.

We say that an R-module is **simple** if it's nonzero and if it has no other submodule than 0 and itself.

Theorem 5.1 (Schur's Lemma)**.** *Let E, F be simple R-modules. Every nonzero map between E and F is an isomorphism. In particular $\mathsf{End}_R(E)$ is a division ring.*

Proof. Let f be such a map. Its kernel is trivial and its image is F. □

Lemma 5.2. *Let E be an R-module whose submodules F admit a complement: $E = F \oplus G$. Then every nonzero submodule of E has a simple submodule.*

Proof. Let $v \in E, v \neq 0$. Rv is a principal submodule of E. Consider the kernel L of the map $R \to Rv$. L is contained in a maximal left ideal M. M/L is maximal submodule of R/L, hence Mv is a maximal submodule of Rv. By hypothesis $E = Mv \oplus G$, whence $Rv = Mv \oplus (G \cap Rv)$, because every element $x \in Rv$ can be written uniquely as $x = mv + g$ with $m \in M$, $g \in G$ and $g = x - mv \in Mv$. Since Mv is maximal in Rv, $G \cap Rv$ is simple. □

Theorem 5.3. *The following conditions on a R-module E are equivalent.*

1. *E is the sum of simple submodules.*
2. *E is the direct sum of simple submodules.*
3. *Every submodule F of E admits a complement: $E = F \oplus G$.*

Proof. Let's prove that the first item implies the second. Let $E = \sum E_i$, $i \in I$, be a sum of simple submodules. We show that there is $J \subseteq I$ such that $E = \bigoplus E_j$, $j \in J$. The subsets S of I such that the sum $\sum E_s$ ($s \in S$) is direct, ordered by inclusion, satisfy the assumptions of Zorn's Lemma. Define J to be a maximal subset given by Zorn. Each E_i is contained in the sum over $j \in J$: $\sum E_j \cap E_i$ is a submodule of E_i; it's equal to E_i: if the intersection were zero J wouldn't be maximal.

Let F be a submodule of $E = \bigoplus E_i$, $i \in I$. Let J be a maximal subset of I such that $F + \bigoplus E_j$ $(j \in J)$ is direct. Argue as before.

The third item implies the first. Let F be the submodule of E which is sum of all simple submodules of E. By way of contradiction, if $F \neq E$, then $E = H \oplus G$, with $G \neq 0$. Then, by lemma above, G contains a simple submodule, contradicting the definition of F. □

An R-module satisfying one of these equivalent conditions is called **semisimple**. A ring is semisimple if $1 \neq 0$ and it's semisimple as a left R-module.

Theorem 5.4. *Let E be a nonzero R-module and $K := \mathsf{End}_R(E)$. Then $\mathsf{End}_R(E^n) \simeq \mathsf{M}_n(K)$.*

Proof. Consider a map $f : E^n \to E^n$. Let f_i be the restriction of f to the i-th factor of E^n and π_j be the projection along the j-th component. Every x has a unique expression as $x = x_1 + \cdots + x_n$. Identify x with the column

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

and f with the matrix

$$\begin{pmatrix} \pi_1 f_1 & \cdots & \pi_1 f_n \\ \vdots & & \vdots \\ \pi_n f_1 & \cdots & \pi_n f_n \end{pmatrix}$$

The effect of f on x is described by matrix multiplication. Conversely, given a matrix (f_{ij}) with elements in $\mathsf{End}_R(E)$ we define an endomorphism of E^n by means of this matrix. □

Here there's something tricky going on. Let $E = R$ as R-module in the preceding theorem. If R is a field then $\mathsf{End}_R(R^n) \simeq \mathsf{M}_n(R)$ as usual. However, if R is not commutative, $\mathsf{End}_R(R)$ is not isomorphic to R but to R^{op}! Therefore $\mathsf{End}_R(R)$ is isomorphic to $\mathsf{M}_n(R^{\mathrm{op}})$ (or to $\mathsf{M}_n(R)^{\mathrm{op}}$ which is the same).

Theorem 5.5. *Let $E = E_1^{n_1} \oplus \cdots \oplus E_r^{n_r}$ be a direct sum of simple nonisomorphic modules E_i. Then each E_i and each i is uniquely determined.*

Proof. Suppose that we have an isomorphism

$$E_1^{n_1} \oplus \cdots \oplus E_r^{n_r} \simeq F_1^{m_1} \oplus \cdots \oplus F_s^{m_s}.$$

By Schur's Lemma each E_i is isomorphic to some F_j and vice versa. It follows that $r = s$ and (up to a permutation of the indices) $E_i \simeq F_i$. But then the claim follows from the remark that if E is simple and $E^n \simeq E^m$, then $n = m$. $\mathsf{End}_R(E^n) \simeq \mathsf{M}_n(K)$ as above is a K-vector space with dimension n^2, so that n is uniquely determined. □

We shall call $n_1 + \cdots + n_r$ the **length** of E.

Lemma 5.6. *If R is semisimple, every R-module is semisimple.*

Proof. Let E be an R-module. By Remark 2.3 E is a factor module of the free module $\bigoplus Rx_i$ where $\{x_i\}_{i\in I}$ is a set of generators. But $Rx_i \simeq R$ is semisimple adn quotients preserve semisimplicity (see Exercise 5.2 below). □

A ring is **simple** if it's nonzero an has no two-sided ideal besides zero and itself.

Theorem 5.7. *Let R be a semisimple ring. Then*

$$R = L_1^{n_1} \oplus \cdots \oplus L_s^{n_s} = R_1 \oplus \cdots \oplus R_s$$

where each R_i is a simple ring.

Proof. Since R is semisimple, $R = \bigoplus L_i$, $i \in I$, where each L_i is a simple left ideal of R. Thus the unit element can be written as $1 = \sum e_i$, with almost all $e_i = 0$: $1 = e_1 + \cdots + e_s$. Now let $x = \sum x_i \in R$; for any $j = 1,\dots,s$, $e_j x = e_j x_j$ and

$$x_j = e_1 x_j + \cdots + e_s x_j = e_j x_j.$$

Also $x = e_1 x + \cdots + e_s x$. This proves that the set I is finite with s elements, and also that each x writes uniquely as $x = e_1 x + \cdots + e_s x$. Define R_i to be the sum of all simple left ideals isomorphic to L_i. □

Corollary 5.8. *If R is a semisimple ring, every simple R-module E is isomorphic to a left ideal L_i of R.*

Proof. Consider the map

$$f : L_1^{n_1} \oplus \cdots \oplus L_s^{n_s} \to E$$

that sends $1 = e_1 + \cdots + e_s$ into $x \neq 0$. The image of L_i can't be zero for every i. Thus for at least one i, $L_i \simeq E$. □

It's easy to see that for each two-sided ideal I of R, $\mathsf{M}_n(I)$ is a two-sided ideal of $\mathsf{M}_n(R)$. Conversely *each* ideal J of $\mathsf{M}_n(R)$ arises in this way: $J = \mathsf{M}_n(I)$ for some two-sided ideal I of R. Let I be the set of $a \in R$ that appear in some entry of a matrix of J. This is an ideal of R. Now, let E_{ij} the matrix with 1 in the entry ij and zero elsewhere. Pre- and post-composing matrices in J by E_{ij} moves entries to any desired place.

In particular $\mathsf{M}_n(R)$ is simple iff R is simple[4].

Theorem 5.9 (Wedderburn-Artin)**.** *A ring R s semisimple iff there are $D_1,\dots,D_s$ division rings such that*

$$R \simeq \mathsf{M}_{n_1}(D_1) \oplus \cdots \oplus \mathsf{M}_{n_s}(D_s).$$

Proof. One direction is clear: by what we've just remarked $M_{n_i}(D_i)$ is simple.

Conversely,

$$\begin{aligned}\mathsf{End}_R(R) &\simeq \mathsf{End}_R(L_1^{n_1} \oplus \cdots \oplus L_s^{n_s})\\ &\simeq \mathsf{End}_R(L_1^{n_1}) \oplus \cdots \oplus \mathsf{End}_R(L_s^{n_s})\\ &\simeq \mathsf{M}_{n_1}(B_1) \oplus \cdots \oplus \mathsf{M}_{n_s}(B_s)\end{aligned}$$

where each B_i is a division ring; but now observe that $\mathsf{End}_R R \simeq R^{\mathrm{op}}$ and that the opposite of a division ring is still a division ring. □

[4] This fact is an instance of a more deep, general phenomenon: the rings R and $\mathsf{M}_n(R)$ are **Morita equivalent**.

Now, let E be an R-module and let $S := \mathsf{End}_R(E)$. E is a S-module with scalar multiplication given by $(f,x) \mapsto f(x)$. Each $a \in R$ induces a linear map $f_a : E \to E$ by $f_a(x) = ax$. The function $a \mapsto f_a$ is a morphism of rings between R and $\mathsf{End}_S(E)$, so that we can view R as a subring of $\mathsf{End}_S(E)$. If $a \in R$ and $s \in \mathsf{End}_R(E)$, $f_a(sx) = a(sx) = s(ax) = sf_a(x)$.

Definition 5.10. A subring T of $\mathsf{End}_R(E)$ is said to be **dense** in $\mathsf{End}_R(E)$ if for every $f \in \mathsf{End}_R(E)$ and every $x_1,\dots,x_m \in E$ there is $t \in T$ such that $f(x_i) = tx_i$.

Lemma 5.11. *Let E be a semisimple R-module and let $S := \mathsf{End}_R(E)$. Let $f \in \mathsf{End}_S(E)$. For every $x \in E$ there is $a \in R$ such that $f(x) = ax$.*

Proof. By semisimplicity $E = Rx \oplus F$ for some F. $\pi : E \to Rx$ is an element of S and hence $f(x) = f(\pi x) = \pi f(x)$, so that $f(x) \in Rx$. □

Theorem 5.12 (Jacobson's Density Theorem)**.** *Let E be a semisimple R-module and let $S := \mathsf{End}_R(E)$. R is dense in $\mathsf{End}_S(E)$.*

Proof. First, we deal with the case E simple. Let $f \in \mathsf{End}_S(E)$. Extend f to a function $E^n \to E^n$ by letting $f^n(y_1,\dots,y_n) = (f(y_1),\dots,f(y_n))$. Let $S_n := \mathsf{End}_R(E^n)$; it's easy to see that $f^n \in \mathsf{End}_{S_n}(E^n)$. By lemma above there is $a \in R$ such that

$$(ax_1,\dots,ax_n) = (f(x_1),\dots,f(x_n)).$$

If E is not simple, it's nonetheless of type $E_1^{n_1} \oplus \cdots \oplus E_r^{n_r}$ with each summand simple. $\mathsf{End}_R(E)$ is a ring of matrices splitting in blocks determined by the simple components. Then the argument carries on as before. □

An R-module E is called **faithful** if $\mathsf{Ann}_R E = 0$[5]. A ring with a faithful simple module is called **primitive**. Observe that a simple ring R is primitve: by Zorn R has a maximal left ideal I; R/I is simple and $\mathsf{Ann}_R(R/I)$ can't be R [6].

Corollary 5.13. *A ring R is primitive iff there is a division ring D and a D-vector space E such that R is dense in $\mathsf{End}_D(E)$.*

Proof. Suppose that R is primitive, and let E be its faithful simple R-moudule. E is a vector space over $D := \mathsf{End}_R(E)$. By Jacobson's Density Theorem R is dense in $\mathsf{End}_D(E)$.

Conversely, let E be a vector space over a division ring D and let R be dense in $\mathsf{End}_D(E)$. E is an R-module. Let $x \in E$. For every $y \in E$ there is $f \in \mathsf{End}_D(E)$ such that $f(x) = y$, and consequently there is $a \in R$ such that $f(x) = ax$. Whence $E = Rx$, for *every* $x \in E$; this implies that E is simple. Finally, since $R \subseteq \mathsf{End}_D(E)$, $\mathsf{Ann}_R(E) \subseteq \mathsf{Ann}_{\mathsf{End}_D(E)}(E) = 0$ and E is faithful. □

[5] That is to say, if the action of R on E is faithful.

[6] However, a primitive ring needn't be simple: if k is a field and E an infinite-dimensional k-space, $\mathsf{End}_k(E)$ is primitive but not simple.

Exercises

Let R be a ring.

Exercise 5.1. Let E be an R-module. Prove that E is simple iff it's isomorphic to R/I for some maximal left ideal I of R.

Exercise 5.2. Prove that every submodule and every factor module of a semisimple module is semisimple.

Exercise 5.3. Let E be an R-module. E is **artinian** if it satisfies the descending chain condition: there is no infinite descending chain of submodules of E. Prove that

- every nonempty family of submodules of E has a minimal element (hint: Zorn);
- a simple artinian ring is semisimple.

Exercise 5.4. Prove (original) Wedderburn's Theorem:

Let E be a faithful simple R-module. Let $D := \mathsf{End}_R(E)$, and suppose E is finite dimensional as a D-vector space. Then $R \simeq \mathsf{End}_D(E)$.

6 The Radical

The **(Jacobson) radical** of a ring R is defined to be the left ideal $\mathsf{J}(R)$ given by the intersection of all maximal left ideals of R.

Lemma 6.1. *If E is a simple R-module, then $\mathsf{J}(R)E = 0$.*

Proof. Since E is simple $E \simeq R/I$ for some maximal left ideal I of R. Note that $\mathsf{J}(R) \subseteq I$. If $a \in \mathsf{J}(R)$ and $x \in R$ then $a(x+I) = ax + I \in I$. □

Theorem 6.2 (Nakayama's Lemma)**.** *Let E be a finitely generated R-module. If $\mathsf{J}(R)E = E$, $E = 0$.*

Proof. By induction on the number of generators of E. Let $x_1, \ldots, x_s$ be such generators. By assumption there are $a_1, \ldots, a_s \in \mathsf{J}(R)$ such that

$$x_s = a_1 x_1 + \cdots + a_s x_s.$$

Therefore there is $a \in \mathsf{J}(R)$ such that $(1+a)x_s$ lies in the module generated by the first $s-1$ generators. Moreover $1+a$ is a unit in R, otherwise $1+a$ is contained in some maximal ideal (every non-unit is contained in a maximal ideal) but then 1 belongs to this maximal ideal, since $a \in \mathsf{J}(R)$. Absurd. Hence x_s lies in the module generated by $x_1, \ldots, x_{s-1}$ and by induction $E = 0$. □

Corollary 6.3. *Let E be an R-module and F a submodule. If $\mathsf{J}(R)E + F = E$, then $F = E$.*

Proof. Apply Nakayama's Lemma to E/F[7]. □

The radical has two important characterizations.

[7] It's possible to prove this result directly applying Zorn's Lemma. Of course Zorn's Lemma is needed in the proof of theorem above too.

Theorem 6.4. $\mathsf{J}(R)$ *is equal to the following:*

1. *the intersection of all annihilators of simple R-modules;*
2. *the set of elements $x \in R$ such that every element of the form $1 + Rx$ is a unit.*

Proof. Recall that an R-module E is simple iff it's isomorphic to R/I for some maximal left ideal I of R. Then $\mathsf{Ann}_R E \simeq \mathsf{Ann}_R R/I$. But $\mathsf{Ann}_R R/I \simeq I$. This proves the first statement.

Let $x \in \mathsf{J}(R)$ and $a \in R$. Define $y := 1 + ax \in R$. Then $R = \mathsf{J}(R)R + Ry$ and, by Corollary 6.3, $R = Ry$. Now, use the analogue for right R-modules of Corollary 6.3 to get $R = yR$. This shows that $1 + ax$ is invertible. Conversely, assume $1 + ax$ is invertible for all $a \in R$ but $x \notin J$ for some maximal left ideal J. $x + J$ is invertible in R/J, so that $1 + ax \in J$ for some a. But then $1 \in J$, absurd. □

A ring R is called **semiprimitive** if R has a faithful semisimple left module.

Theorem 6.5. *A ring R is semiprimitive iff* $\mathsf{J}(R) = 0$.

Proof. Let E be a faithful semisimple R-module. $E = \bigoplus E_i$ where each E_i is simple. By the first above characterization of $\mathsf{J}(R)$, $\mathsf{J}(R)E = 0$. Therefore $\mathsf{J}(R) \subseteq \mathsf{Ann}_R E = 0$ and $\mathsf{J}(R) = 0$.

Conversely, assume that $\mathsf{J}(R) = 0$. Let $\{E_i\}$ be a family of pairwise nonisomorphic R-modules such that each isomorphism class of simple R-modules is represented. Let $E := \bigoplus E_i$. E is semisimple and

$$\mathsf{Ann}_R E = \bigcap \mathsf{Ann}_R E_i = \mathsf{J}(R) = 0.$$

□

In particular, since $\mathsf{J}(R/\mathsf{J}(R)) = 0$, $R/\mathsf{J}(R)$ is always semiprimitve.

Exercises

Exercise 6.1. Let R be artinian. Show that its radical is 0 iff R is semisimple.

Exercise 6.2. Prove that if R is artinian, then its radical is nilpotent. (Hint: Nakayama's Lemma).

A Jordan Normal Form

Module theory provides a neat way to prove that every square matrix with coefficients in an algebraically closed field is similar to a Jordan matrix.

Theorem A.1. *Let k be an algebraically closed field, and let E be a k-vector space of dimension $n > 0$. Let $A \in \mathsf{End}_k(E)$. There is a basis of E over k such that with respect to this basis A is in normal form.*

Proof. E is a $k[A]$-module, and, thanks to the map $k[x] \to k[A]$ that sends x into A, a $k[x]$-module as well. Note that $k[x]$ is a principal ring. The above map is surjective and has nontrivial kernel generated by a polynomial $q(x)$ (called **minimal polynomial** of A). Since $0 = q(A)E = q(x)E$, q is the period of E. q has a factorization $p_1^{r_1} \cdots p_s^{r_s}$ into distinct prime powers. Hence $E = E(p_1) \oplus \cdots \oplus E(p_s)$.

Each $E(p)$ can be written as a direct sum of submodules isomorphic to $k[x]/\langle p^r\rangle$ for some irreducible polinomial $p(x) = (x-\alpha)$ and some $r \geq 1$. We investigate the structure of the submodule $k[x]/\langle p^r\rangle$. Let $v \in E$ with period p^r. We show that the elements

$$\{v, (x-\alpha)v, \ldots, (x-\alpha)^{r-1}v\}$$

(or better

$$\{v, (A-\alpha)v, \ldots, (A-\alpha)^{r-1}v\})$$

are a basis. They are linearly independent over k, because the dependence between

$$v, (A-\alpha)v, \ldots, (A-\alpha)^{r-1}v$$

implies that of $v, Av, \ldots, A^{r-1}v$. But then there is a polynomial $g(x)$ with degree less than r such that $g(A) = 0$. Since $\dim_k(k[x]/\langle p^r\rangle) = r$ the set is a basis (and is the basis by which A is in the required form). □

B The Tensor Product

Fix a pair of R-modules E_1, E_2. If F is an R-module, the set $\mathsf{Bil}(E_1, E_2; F)$ of bilinear maps from $E_1 \times E_2$ to F forms an R-module.

Now, let C be the category whose objects are bilinear maps $f : E_1 \times E_2 \to F$. We define an arrow from $f : E_1 \times E_2 \to F$ to $g : E_1 \times E_2 \to G$ to be a R-linear map $h : F \to G$ such that the following diagram commute:

$$\begin{tikzcd}
 & F \arrow[dd, "h"] \\
E_1 \times E_2 \arrow[ur, "f"] \arrow[dr, "g"'] & \\
 & G
\end{tikzcd}$$

The **tensor product** of E_1 and E_2 is a universal object in the category C, i.e. it comprises an R-module $E_1 \otimes E_2$ and a bilinear map $\varphi : E_1 \times E_2 \to E_1 \otimes E_2$ such that for every object of C $g : E_1 \times E_2 \to G$ there is a unique $g_\star : E_1 \otimes E_1 \to G$ making the following diagram commute

$$\begin{tikzcd}
 & E_1 \otimes E_2 \arrow[dd, "g_\star"] \\
E_1 \times E_2 \arrow[ur, "\varphi"] \arrow[dr, "g"'] & \\
 & G
\end{tikzcd}$$

We now show that such an object exists. Uniqueness is clear by universality.

Theorem B.1. C *admits a universal object.*

Proof. Let M be the free R-module generated by the pairs $(e_1, e_2) \in E_1 \times E_2$ and let $M/\sim$ be the quotient of M modulo the following relations:

$$(e_1 + e_1', e_2) \sim (e_1, e_2) + (e_1', e_2) \quad (e_1, e_2 + e_2') \sim (e_1, e_2) + (e_1, e_2') \quad (ae_1, e_2) \sim (e_1, ae_2) \sim a(e_1, e_2)$$

for every $a \in R$. Define $E_1 \otimes E_2 := M/\sim$ and φ to be the composition of the inclusion $E_1 \times E_2 \hookrightarrow M$ with the canonical map $M \to M/\sim$. Now, consider the diagram (where $\bar{g}$ is induced by g by linearity):

$$\begin{tikzcd}
E_1 \times E_2 \arrow[r, hook] \arrow[dr, "g"'] & M \arrow[r] \arrow[d, "\bar{g}"] & E_1 \otimes E_2 \arrow[dl, dashed, "g_\star"] \\
& G &
\end{tikzcd}$$

Since $\bar{g}$ takes the value 0 on the submodule generated by $\sim$, the universal property of factor modules assures that there is a unique $g_\star$ that gets the job done. □

C Solutions to Selected Exercises

2.1. Taken $n \in N$, by surjectivity there are $k \in K$, $l \in L$ such that $n = f(k+l) = f(k) + f(l)$. Hence $N = f(K) + f(L)$. We show that $f(K) \cap f(L) = 0$. Let $x \in f(K) \cap f(L)$; in particular $x = f(k) = f(l)$ for some $k \in K$, $l \in L$.

$$0 = x - x = f(l) - f(k) = f(l-k)$$

implies that $l - k \in \ker f = K \cap L$. $l \in L$ and $(l-k)+k \in K$ hence $f(l) = 0$ and $x = 0$.

3.1 Since $e_1, \dots, e_n$ are idempotent, orthogonal $R \simeq Re_1 \oplus \cdots \oplus Re_n$. But since $\{e_1, \dots, e_n\}$ are primitive then each Re_i is isomorphic to $\mathbb{Z}_2$. Suppose not, then there is $x \in Re_i$ such that $x \neq 0, 1$. But a subring of a boolean ring is a boolean ring, hence $x^2 = x$. This implies that $Re_i \simeq Rx \oplus R(1-x)$ and e_i is not primitive. Therefore $R \simeq \mathbb{Z}_2 \oplus \cdots \oplus \mathbb{Z}_2$. Now, let $a \in R$ as above. $a = a_1 e_1 + \cdots a_n e_n$ with each a_i equal to 0 or to 1. This proves our statement.

5.3 The family of simple R-modules is nonempty (R itself belongs to it). Therefore there is a minimal simple R-module E. For every $a \in R$, aE is still a R-module. By simplicity either $aE \simeq E$ or $aE = 0$. In any case the sum $I := \sum_{a \in R} aE$ is a sum of simple modules. I is a two-sided ideal of R. Since R is simple, $R \simeq I$.

5.4 Let $\{x_1, \dots, x_n\}$ be a basis of E as a D-space. Let $f \in \mathsf{End}_D(E)$. Jacobson's Density Theorem there is $a \in R$ such that $ax_i = f(x_i)$. Then the assignment $R \to \mathsf{End}_D(E)$ is surjcetive. By faithfulness is injective.

6.1 By definition the radical of R is the intersection of all maximal left ideals. Since R is artinian this intersection is finite: $\mathsf{J}(R) := I_1 \cap \cdots \cap I_k$ (otherwise there'd be an infinite descending sequence of ideals). If $\mathsf{J}(R) = 0$, the map

$$R \to \bigoplus_i R/I_i$$

is injective. Since R/I_i is simple R is a submodule of a semisimple module, whence semisimple. Conversely, if R is semisimple, then $R \simeq \bigoplus_i R/I_i$ where each I_i is a maximal left ideal. Since this map is injective its kernel $\bigcap_i I_i$ is zero. This implies that $\mathsf{J}(R) = 0$.

6.2 Let $N := \mathsf{J}(R)$. $N \supset N^2 \supset \cdots$ is a descending sequence of left ideals. Let N^∞ be its limit. We prove that $N^\infty = 0$. There is r such that $N^\infty = N^r$. Suppose that $N^r \neq 0$. The set S of ideals $L \subset N^\infty$ such that $N^\infty L \neq 0$ is nonempty: $N^r N = N^{r+1} \neq 0$. Let L be a minimal such ideal. By minimality L is finitely generated. By Nakayama's Lemma $N(N^r L) = N^r L = 0$, contradiction.