

Noncommutative algebra

Notes taken by Yeheli Fomberg <yp@campus.technion.ac.il>
Based on lectures by Chen Meiri

Spring 2026

These notes are not endorsed by the lecturers. I have revised them outside lectures to incorporate supplementary explanations, clarifications, and material for fun. While I have strived for accuracy, any errors or misinterpretations are most likely mine.

Contents

1	Introduction	3
1.1	Modules	3
1.2	Simple and semisimple modules	5
1.3	Lattices*	9
2	Wedderburn structure theorem	11
3	Radicals	17
3.1	Jacobson's radical	19
3.2	Radicals in Artinian rings	20

1 Introduction

Remark 1.1. In this course, unless explicitly stated otherwise, the term ring will be preserved to rings with units which are not necessarily commutative. Homomorphisms between rings are required to respect the identity, that means that if $f: R \rightarrow S$ is a ring homomorphism then $f(1_R) = 1_S$.

Definition 1.1 (Opposite ring). For a ring R , we define the opposite ring R^{op} by giving it the additive ring of R , and defining $a *_{R^{\text{op}}} b = b *_R a$.

Example 1.1. Let $n \geq 1$, and let $\mathbb{F}$ be a field. The map $A \mapsto A^T$ is an isomorphism from $M_n(\mathbb{F})$ to $M_n(\mathbb{F})^{\text{op}}$.

1.1 Modules

Definition 1.2 (Module). Let R be a ring. A left R -module is a pair (M, ρ) where M is an abelian group, and ρ is a homomorphism from R to $\text{End}(M)$. Similarly, a right R -module is a pair (M, ρ) where M is an abelian group, and ρ is a homomorphism from R to $\text{End}(M)^{\text{op}}$.

Remark 1.2. If R is commutative, then every left R -module is also a right R -module and vice versa. Thus, when we do commutative algebra, we simply use the term “module”.

Remark 1.3. We sometimes say that M is a left (or right) module, without mentioning the homomorphism ρ when it is possible to infer it from context. If $r \in R$ and $m \in M$ we usually write $r \cdot m$ instead of $\phi(r)(m)$. This terminology is justified by the following exercise.

Exercise 1.1. Let R be a ring and M an abelian group. Prove that there is a bijection between the set of left R -modules with underlying group M and the set of functions $\cdot: R \times M \rightarrow M$ which satisfy the following properties:

- (1) $1_R \cdot m = m$.
- (2) $r \cdot (m + n) = r \cdot m + r \cdot n$.
- (3) $(r + s) \cdot m = r \cdot m + s \cdot m$.
- (4) $(rs) \cdot m = r \cdot (s \cdot m)$.

Example 1.2. A vector space is a module over a field.

Example 1.3. Every abelian group is a module over $\mathbb{Z}$ (note that there is a unique homomorphism from $\mathbb{Z}$ to $\text{End}(M)$).

Example 1.4. Let $n, m \geq 2$ and R be a ring. Then $M_{n,m}(R)$ is a left $M_n(R)$ -module where the action of R on M is by matrix multiplication from the left. Similarly $M_{m,n}(R)$ is a right $M_n(R)$ -module where the action of R on M is by matrix multiplication from the right.

Example 1.5. Let R be a ring. Then R is a left (equivalently, right) R -module where the action of R on R is by left (equivalently, right) multiplication. We usually write ${}_R R$ (equivalently R_R) to indicate that we view ${}_R R$ as a left module (equivalently, right). The left (equivalently, right) ideals of R are the left (equivalently, right) submodules of ${}_R R$ (equivalently, R_R).

Remark 1.4. Many definitions, constructions, and theorems about abelian groups have natural counterparts in the theory of modules.

Definition 1.3. Let R be a ring.

- (1) A R -homomorphism from a left R -module M to a left R -module N is a group homomorphism $\alpha: M \rightarrow N$ such that for every $r \in R$ and every $m \in M$ we have that $\alpha(rm) = r\alpha(m)$.
- (2) A submodule of a left R -module M is a subgroup $L \leq M$ such that for every $r \in R$ and every $m \in L$ we have that $rm \in L$.
- (3) Let L be a submodule of a left R -module M . The quotient group M/L inherits a structure of a left R -module by the rule “for every $r \in R$ and every $m + L \in M/L$ we define $r(m + L) := rm + L$ ”.

Example 1.6.

- (1) Let M be an abelian group and view it as a $\mathbb{Z}$ -module. Every subgroup of M is a submodule.
- (2) Let R be a ring. The submodules of R_R are the right ideals of R .

Exercise 1.2. Let R be a ring and $\alpha: M \rightarrow N$ be a homomorphism of left (right) R -modules. Prove that $\ker \alpha$ and $\operatorname{im} \alpha$ are left (right) submodules of M and N respectively.

Exercise 1.3. State and prove the isomorphism theorems for modules.

Definition 1.4 (Direct product). Let R be a ring. Let $(M_i)_{i \in I}$ be an indexed family of left R -modules. The direct product of $(M_i)_{i \in I}$, denoted by $\prod_{i \in I} M_i$, is the left R -module whose underlying group is the direct product of the underlying groups of each of the M_i s, and the action of R is the pointwise actions. More explicitly:

- (1) The elements of $\prod_{i \in I} M_i$ are functions $f: I \rightarrow \cup_{i \in I} M_i$ such that for every $i \in I$ we have $f(i) \in M_i$.
- (2) For every $f, g \in \prod_{i \in I} M_i$, the sum $f + g$ is defined by the pointwise sum $(f + g)(i) := f(i) + g(i)$.
- (3) For every $r \in R$ and $f \in \prod_{i \in I} M_i$, the product $r \cdot f$ is defined by $(r \cdot f)(i) = r \cdot f(i)$ for every $i \in I$.

Definition 1.5 (Direct sum). Let $(M_i)_{i \in I}$ be an indexed family of left R -modules. The direct sum of the M_i s denoted by $\oplus_{i \in I} M_i$, is the submodule of $\prod_{i \in I} M_i$ consisting of the elements f with finite support, i.e., the elements $f \in \prod_{i \in I} M_i$ for which the set $\{i \in I \mid f(i) \neq 0\}$ is finite.

Remark 1.5. We remind that all of the above (and below) definitions, theorems, and exercises have counterparts with right R -modules.

Exercise 1.4. Let R be a ring and M a left or right R -module. Prove that an intersection of (possibly infinitely many) submodules of M is a submodule of M .

Definition 1.6 (Generated submodule). Let X be a subset of M . The submodule of M generated by X is the intersection of all submodules of M that contain X .

Definition 1.7 (Sum of submodules). Let $\{N_i \mid i \in I\}$ be a set consisting of submodules of M . We denote by $\sum_{i \in I} N_i$ the submodule of M generated by $\cup_{i \in I} N_i$.

Exercise 1.5. Let R be a ring, and let M be a left or right R -module. Prove that the submodule generated by X consists of the R -linear finite sums of elements of X (where the empty sum is defined to be equal to zero).

Definition 1.8. Let R be a ring, and let M be a left or right R -module. We define $\operatorname{End}_R(M)$ to be the subring of $\operatorname{End}(M)$ consisting of the R -homomorphisms.

Exercise 1.6. Let R be a commutative ring and M an R -module. Prove that for every $r \in R$ and every $f \in \text{End}_R(M)$, the function $rf: M \rightarrow M$ defined by $(rf)(m) := r(f(m))$ belongs to $\text{End}_R(M)$. Deduce that in this case, $\text{End}_R(M)$ carries the structure of an R -module.

Definition 1.9 (Noetherian ring). Let R be a ring, and let M be a left or right module. The module M is called Noetherian (respectively Artinian) if there is no infinite and strictly increasing (respectively, decreasing) chain of submodules of M .

Example 1.7. $\mathbb{Z}_{\mathbb{Z}}$ is a Noetherian $\mathbb{Z}$ -module which is not Artinian.

Example 1.8. Let p be a prime number. Then $\mathbb{Z}[1/p]/\mathbb{Z} = \{a/p^n \mid a \in \mathbb{Z} \text{ and } n \in \mathbb{N}\}/\mathbb{Z}$ is an Artinian $\mathbb{Z}$ -module which is not Noetherian.

Remark 1.6. The group $\mathbb{Z}[1/p]/\mathbb{Z}$ is known as a Prüfer group, and is usually denoted by $\mathbb{Z}(p^\infty)$. It is worth taking the time to understand its structure, and why the claim in Example 1.8 holds.

1.2 Simple and semisimple modules

Definition 1.10 (Simple module). Let R be a ring. A left or right R -module M is called simple if M is not the zero module and the only submodules of M are 0 and M .

Example 1.9. A finite abelian group is a simple module over $\mathbb{Z}$ if and only if it is of a prime order.

Example 1.10. Let $n, m \geq 1$ and $\mathbb{F}$ be a field. Then $M_{n \times m}(\mathbb{F})$ is a simple left $M_n(R)$ -module if and only if $m = 1$.

Example 1.11. Let R be a nonzero ring. Then R_R is a simple right R -module if and only if the right ideals of R are the zero ideal and R itself.

Exercise 1.7 (Characterization of simple modules). Let R be a ring. For a nonzero right R -module M , show that the following conditions are equivalent:

- (1) M is simple.
- (2) $mR = M$ for all nonzero $m \in M$.
- (3) $M \cong R_R/I$ for some maximal right ideal I of R .

Lemma 1.1 (Schur's lemma). Let M and N be right R -modules, and let $\rho: M \rightarrow N$ be a nonzero homomorphism. Then:

- (1) If M is simple, then ρ is injective.
- (2) If N is simple, then ρ is surjective.
- (3) If M and N are simple right R -modules, then either $M \cong N$ or $\text{Hom}_R(M, N) = 0$.
- (4) If M is simple, then $\text{End}_R(M)$ is a division ring.

Remark 1.7. Recall that a division ring is a ring in which division is well defined for nonzero elements. A commutative division ring is a field. As a fun fact, Wedderburn's little theorem asserts that all finite division rings are commutative and therefore finite fields.

Definition 1.11 (Composition series). Let R be a ring and M be a left or right R -module. An increasing chain of submodules $0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_{n-1} \subsetneq M_n = M$ of M is called a composition series of M if for every $0 \leq i < n$, the R -module M_{i+1}/M_i is simple. The factor modules are called the composition modules of M .

Example 1.12. The $\mathbb{Z}$ -module $\mathbb{Z}_{\mathbb{Z}}$ does not have a composition series.

Example 1.13. For every natural number $n \geq 2$ denote $\overline{\mathbb{Z}}_n := \mathbb{Z}/n\mathbb{Z}$. The series $0 \subsetneq 4\overline{\mathbb{Z}}_{12} \subsetneq 2\overline{\mathbb{Z}}_{12} \subsetneq \overline{\mathbb{Z}}_{12}$ and $0 \subsetneq 6\overline{\mathbb{Z}}_{12} \subsetneq 3\overline{\mathbb{Z}}_{12} \subsetneq \overline{\mathbb{Z}}_{12}$ are both composition series for the $\mathbb{Z}$ -module $\overline{\mathbb{Z}}_{12}$. The composition factors of the above two series consist of two simple modules isomorphic to $\overline{\mathbb{Z}}_2$ and one simple module isomorphic to $\overline{\mathbb{Z}}_3$. The fact that the composition factors are identical in both series is not a coincidence.

Exercise 1.8. Prove that M has a composition series if and only if it is Noetherian and also Artinian.

Exercise 1.9. Prove that Jordan–Hölder theorem: If M has a composition series then, up to isomorphism, the composition factors and their multiplicity are the same for each composition series.

Definition 1.12 (Semisimple module). A right or left R -module M is called a semisimple module if it is isomorphic to a direct sum of simple modules.

Example 1.14. Let $p_1, \dots, p_k$ be prime numbers and denote $n := p_1 \cdots p_k$. Then $\mathbb{Z}/n\mathbb{Z}$ is a semisimple $\mathbb{Z}$ -module if and only if $p_1, \dots, p_k$ are distinct.

Definition 1.13 (Internal direct sum). Let R be a ring and M a right or left R -module. Let $(M_i)_{i \in I}$ be an indexed collection of submodules of M . Let $\alpha: \bigoplus_{i \in I} M_i \rightarrow \sum_{i \in I} M_i$ be the R -homomorphism defined by $\alpha(f) := \sum_{i \in I} f(i)$ for every $f \in \bigoplus_{i \in I} M_i$. We say that $\sum_{i \in I} M_i$ is an internal direct sum of the indexes collection $(M_i)_{i \in I}$ if α is an isomorphism onto $\sum_{i \in I} M_i$.

Example 1.15. The Euclidean plane $M = \mathbb{R}^2$ viewed as an R -module is an internal direct sum of the submodules $M_1 = \{(x, 0) \mid x \in \mathbb{R}\}$ and $M_2 = \{(0, y) \mid y \in \mathbb{R}\}$. Indeed, the map $\alpha: M_1 \oplus M_2 \rightarrow \sum_{i=1}^2 M_i$ given by $\alpha((x, 0), (0, y)) = (x, 0) + (0, y) = (x, y)$ is an isomorphism.

Example 1.16. Any polynomial ring $k[x]$ viewed as a module over K is an internal direct sum of the submodules $M_{\text{even}} = \{p \in k[x] \mid p \text{ only contains even powers of } x\}$ and $M_{\text{odd}} = \{p \in k[x] \mid p \text{ only contains odd powers of } x\}$. In that case α is clearly an isomorphism since each polynomial can be uniquely decomposed into the sum of the element of each of these modules.

Example 1.17. The matrix algebra $M_n(\mathbb{R})$ viewed as an $\mathbb{R}$ -module is an internal direct sum of the submodules M_{sym} and M_{skew} of symmetric and skew-symmetric matrices by the famous decomposition result we have seen in linear algebra.

Remark 1.8. If $\sum_{i \in I} M_i$ is an internal direct sum, we may use the notation $\bigoplus_{i \in I}^{\text{int}} M_i = \sum_{i \in I} M_i$, or write $\sum_{i \in I} M_i \cong \bigoplus_{i \in I}^{\text{int}} M_i$.

Lemma 1.2. Let R be a ring, let M be a left or right R -module. Let N and L be submodules of M . Then:

- (1) $L + N \cong \bigoplus_{i \in I}^{\text{int}} L \oplus N$ if and only if $L \cap N = 0$.
- (2) If L is simple then $L + N \cong \bigoplus_{i \in I}^{\text{int}} L \oplus N$ if and only if L is not contained in N .

Proof.

- (1) Let $\rho: L \oplus N \rightarrow L + N$ be the R -homomorphism defined by $\rho((\ell, n)) = \ell + n$. The R -homomorphism ρ is always onto, so we only have to check when it is injective. For every $(\ell, n) \in L \oplus N$, we have that $(\ell, n) \in \ker \rho$ if and only if $\ell + n = 0$ or equivalently $\ell = -n \in L \cap N$. It follows that $\ker \rho = 0$ if and only if $L \cap N = 0$.

- (2) Since L is simple and $L \cap N$ is a submodule of L , by definition of the simple module either $L \cap N = 0$ or $L \cap N = L$. By (1), the former holds if and only if $L + N \cong^{\text{int}} L \oplus N$. The latter possibility holds if and only if $L \subseteq N$. This completes the proof. $\square$

Remark 1.9. Part (1) of Theorem 1.2 holds even in the case of an infinite sums.

Definition 1.14 (Complemented module). Let R be a ring and M a left or right R -module. Then M is called complemented if for every submodule N of M there exists a submodule L such that $M = N \oplus^{\text{int}} L$.

Proposition 1.3 (Properties of complemented modules). *Let R be a ring and M a left or right complemented R -module. Then:*

- (1) *Every submodule of M is complemented.*
- (2) *If $M \neq 0$ then M contains a simple submodule.*
- (3) *M is generated by its simple submodules.*

Proof.

- (1) Let N be a submodule of M and L a submodule of N . We have to show that there exists a submodule K of N such that $N = L \oplus^{\text{int}} K$. Since M is complemented, there exists a submodule E of M such that $M = N \oplus^{\text{int}} E$. It follows by Theorem 1.2 that $L + E = L \oplus^{\text{int}} E$, which is a submodule of M . Since M is complemented, there exists a submodule D of M such that $M = D \oplus^{\text{int}} (L \oplus^{\text{int}} E)$. Since $L \subseteq N$, we get that:

$$N = N \cap M = N \cap (D \oplus^{\text{int}} (L \oplus^{\text{int}} E)) = N \cap (L \oplus^{\text{int}} (D \oplus^{\text{int}} E)) = L \oplus^{\text{int}} (N \cap (D \oplus^{\text{int}} E)),$$

where the second to last transition is commutativity of the direct sum, and the last transition is the modular property of the lattice of submodules (see Section 1.3). Hence, we can take $K := N \cap (D \oplus^{\text{int}} E)$, which completes the proof.

- (2) Assume that $M \neq 0$ and choose some nonzero $m \in M$. By Zorn's lemma, there exists a submodule N of M which is maximal with respect to the property that it does not contain m . Since $m \notin N$, we get that $M \neq N$. Since M is complemented, there exists a submodule L of M such that $M = L \oplus^{\text{int}} N$. We claim that L is simple. Assume, by way of contradiction, that L is not simple. Since L is complemented (by (1)), there exist nonzero submodules L_1 and L_2 of L such that $L = L_1 \oplus^{\text{int}} L_2$. It follows that:

$$(L_1 \oplus^{\text{int}} N) \cap (L_2 \oplus^{\text{int}} N) = N,$$

so $m \notin (L_1 \oplus^{\text{int}} N) \cap (L_2 \oplus^{\text{int}} N)$. Thus, either $m \notin (L_1 \oplus^{\text{int}} N)$ or $m \notin (L_2 \oplus^{\text{int}} N)$. Since L_1 and L_2 are nonzero, we get a contradiction to the maximality of N with respect to the property of not containing m .

- (3) If $M = 0$ then M is semisimple (this completes the proof). Assume that $M \neq 0$. Let N be the submodule of M which is generated by all simple submodules of M . Assume, by way of contradiction, that $M \neq N$. Since M is complemented, there exists a nonzero submodule L of M such that $M = L \oplus^{\text{int}} N$. By (1) we get that L is complemented, and by (2) we get that L contains a simple submodule K . By the definition of N , we must have $K \subseteq N \cap L = 0$, which is a contradiction (recall a simple submodule is nonzero).

□

Remark 1.10. Note that the zero module is a semisimple but not simple.

Theorem 1.4 (Characterization of semisimple modules). *Let R be a ring and M a left or right R -module. Then the following conditions are equivalent:*

- (1) M is semisimple.
- (2) M is an internal direct sum of some simple submodules of it.
- (3) $M = \sum_{i \in I} M_i$ where $\{M_i \mid i \in I\}$ is the set of simple submodules of M .
- (4) M is complemented.

Proof. We can assume that $M \neq 0$ (because in that case the statement is trivial). The implications (1) $\implies$ (2) $\implies$ (3) are clear. We will now show (3) $\implies$ (4). Let N be a submodule of M . Define: $T := \{J \subseteq I \mid N + \sum_{i \in J} M_i \stackrel{\text{int}}{\cong} N \oplus (\oplus_{i \in J} M_i)\}$. T is not empty since $\emptyset \in T$. Moreover, T is closed to the union of ascending chains of sets in T . Thus we can apply Zorn's lemma and get that there exists a maximal element $J \in T$ with respect to inclusion. It is now enough to show that $M = N \oplus (\oplus_{i \in I} M_i)$, since then M is complemented which completes the proof. Assume otherwise. By (3), there exists $j \in I$ such that N_j is not contained in $N \oplus (\oplus_{i \in J} M_i)$, in particular, $j \notin J$. Theorem 1.2 implies that:

$$N = \sum_{i \in J \cup \{j\}} M_i = (N \oplus (\oplus_{i \in J \cup \{j\}} M_i)) \stackrel{\text{int}}{\oplus} N_j = N \oplus (\oplus_{i \in J \cup \{j\}} M_i),$$

in contradiction to the maximality of J . This contradiction completes the proof of the implication (3) $\implies$ (4). Note that in the proof of (3) $\implies$ (4), if we choose $N = 0$, then we have shown that $M = \oplus_{i \in I} M_i$, which means that M is semisimple hence the implication (3) $\implies$ (1) is now proved. We now have the implications (1) $\iff$ (2) $\iff$ (3) $\implies$ (4), but the implication (4) $\implies$ (3) follows from Theorem 1.3. □

Corollary 1.5. *A submodule of a semisimple module is semisimple.*

Proof. This follows immediately from the characterization of semisimple modules as complemented modules. Since any submodule of a complemented module is itself complemented, the proof is complete. □

Exercise 1.10. Let M be a semisimple module. Then the following are equivalent:

- (1) M is Artinian.
- (2) M is Noetherian.
- (3) M is isomorphic to a finite direct sum of simple modules.

Remark 1.11. From now on we mainly use the term “semisimple module” and not the term “complemented module”, since they are the same thing.

1.3 Lattices*

This subsection is outside the scope of the course, but since we have use the modular property of the lattice of submodules in Theorem 1.3, we might as well learn about it.

Definition 1.15 (Lattice, as a poset). A partially order set $(L, \leq)$ is called a lattice if any pair of elements $\{a, b\}$ has a unique join (least upper bound) and a unique meet (greatest lower bound).

Remark 1.12. The join of a and b is denoted by $a \vee b$ and $a \wedge b$. We will soon show an example of a lattice, think why both the names, and the notations make sense (think what are the meet and the join in the lattice of subsets of $\mathbb{R}$ with respect to set inclusion).

Example 1.18. Consider the set of natural numbers where the order $a \leq b$ is defined by $a \mid b$ (a divides b). In this case, the join would be $a \vee b = \text{lcm}(a, b)$ and the meet would be $a \wedge b = \text{gcd}(a, b)$.

Example 1.19 (Lattice of subgroups). The subgroups of a group G ordered by inclusion form a lattice, in which case we have $H \wedge K = H \cap K$ and $H \vee K = \langle H \cup K \rangle$, for any two subgroups $H, K \leq G$.

Example 1.20 (Lattice of submodules). The submodules of a module M ordered by inclusion form a lattice, in which case we have $N \wedge K = N \cap K$ and $N \vee K = N + K$, for any two submodules N, K of M .

Example 1.21 (Lattice of ideals). Let $\mathcal{I}(R)$ be the set of all ideals of the ring R . Under the partial order of set inclusion the bottom element (denoted by $\perp$) is the zero ideal $\{0\}$, and the top elements (denoted by $\top$) is the ring itself R . The join of ideals is $I \vee J = I + J$, and the meet of ideals is $I \wedge J = I \cap J$.

Remark 1.13. We can also view lattices as algebraic structures.

Definition 1.16 (Lattice). A lattice is an algebraic structure $(L, \vee, \wedge)$, consisting of a set L , and two binary, commutative and associative operations $\vee$ and $\wedge$ on L which satisfy the following axioms (sometimes called absorption laws):

$$a \vee (a \wedge b) = a \quad a \wedge (a \vee b) = a$$

Remark 1.14. From the axioms of the lattice follow the two “idempotent laws”:

$$a \vee a = a \quad a \wedge a = a$$

It also follows that both $(L, \vee)$ and $(L, \wedge)$ are semilattices (semilattices are defined by the structure induced on these structures by the bigger structure $(L, \vee, \wedge)$).

Exercise 1.11. Think why Definition 1.15 and Definition 1.16 are equivalent definitions.

Remark 1.15 (Bounded lattice). A bounded lattice is a lattice which has a top element, denoted by 1 or $\top$, and a bottom element, denoted by 0 or $\perp$. This makes $\mathcal{I}(R)$ (defined in Example 1.21) a bounded lattice. Note that in bounded lattices the 0 element is the identity element of the join operation, and the 1 element is the identity for the meet operation. It can be shown that a partially ordered set is a bounded lattice if and only if every finite set of elements (including the empty set) has a join and a meet.

Remark 1.16 (Complete lattice). A poset is called a complete lattice if all its subsets have both a join and a meet. Hence every complete lattice is a bounded lattice.

Definition 1.17 (Distributive lattice). A lattice $(L, \wedge, \vee)$ is said to be a distributive lattice if it satisfies the following distributive axioms:

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c) \quad a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$$

Remark 1.17. It turns out that each distributive law in Definition 1.17 implies the other.

Definition 1.18 (Modular lattice). A modular lattice is a lattice $(L, \wedge, \vee)$ which satisfies the modular law:

$$a \leq b \implies a \vee (x \wedge b) = (a \vee x) \wedge b,$$

where x, a, b are arbitrary elements in the lattice, $\leq$ is the partial order (see Exercise 1.11).

Remark 1.18. It turns out that the lattice of submodules of a module M with respect to set inclusion is a modular lattice that is not distributive. In this case the modular property becomes:

$$L \subseteq N \implies L + (K \cap N) = (L + K) \cap N,$$

where L, N, K are clearly submodules of M . By commutativity we get that:

$$L \subseteq N \implies L + (N \cap K) = N \cap (L + K),$$

which is exactly what we used in Theorem 1.3.

2 Wedderburn structure theorem

Definition 2.1 (The α map setting). Let $n \geq 2$, let R be a ring, and let $M_1, \dots, M_n$ be right R -modules. Let $M = \bigoplus_{i=1}^n M_i$, and let $\rho_i: M_i \rightarrow M$ be the inclusions, and $\pi_i: M \rightarrow M_i$ be the projections. Moreover, denote $\alpha_{i,j} := \pi_i \circ \alpha \circ \rho_j \in \text{Hom}_R(M_j, M_i)$. For $\alpha \in \text{End}_R(M)$ and $\bar{m} \in M$ denote:

$$\alpha(\bar{m}) := (\alpha_{i,j})_{1 \leq i,j \leq n} \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} := \begin{pmatrix} \sum_{j=1}^n \alpha_{1,j}(m_j) \\ \vdots \\ \sum_{j=1}^n \alpha_{n,j}(m_j) \end{pmatrix}$$

Note the analogy with ordinary matrix-vector multiplication, where the entries $\alpha_{i,j}$ are maps applied to the components m_j . For $\alpha, \beta \in \text{End}_R(M)$ denote:

$$(\alpha \circ \beta)_{1 \leq i,j \leq n} := \sum_{k=1}^n \alpha_{i,k} \circ \beta_{k,j},$$

which is analogous to matrix multiplication. Conversely, for every $1 \leq i, j \leq n$ let $\gamma_{i,j} \in \text{Hom}_R(M_j, M_i)$. We can then define a map $\alpha: M \rightarrow M$ by: for every $\bar{m} = (m_1, \dots, m_n)^T \in M$,

$$\alpha(\bar{m}) := \begin{pmatrix} \sum_{j=1}^n \gamma_{1,j}(m_j) \\ \vdots \\ \sum_{j=1}^n \gamma_{n,j}(m_j) \end{pmatrix}.$$

The map α is an R -endomorphism of M and for every $1 \leq i, j \leq n$ we have $\alpha_{i,j} = \gamma_{i,j}$. Let E be the set of $n \times n$ matrices X such that for every $1 \leq i, j \leq n$, we have:

$$X_{i,j} \in \text{Hom}(M_j, M_i).$$

Let $\psi: \text{End}_R(M) \rightarrow E$ be the map defined by: for every $\alpha \in \text{End}_R(M)$, we have:

$$\psi(\alpha) := (\alpha_{i,j})_{1 \leq i,j \leq n}.$$

The map ψ is an isomorphism of rings, where E is endowed with matrix-like operations:

- Addition is defined as follows: for every $1 \leq i, j \leq n$ and all elements $\alpha = (\alpha_{i,j})_{1 \leq i,j \leq n}$ and $\beta = (\beta_{i,j})_{1 \leq i,j \leq n}$ of E , then:

$$(\alpha + \beta)_{i,j} := \alpha_{i,j} + \beta_{i,j}.$$

- Multiplication is defined as follows: for every $1 \leq i, j \leq n$ and all elements $\alpha = (\alpha_{i,j})_{1 \leq i,j \leq n}$ and $\beta = (\beta_{i,j})_{1 \leq i,j \leq n}$ of E , then:

$$(\alpha\beta)_{i,j} := \sum_{k=1}^n \alpha_{i,k} \circ \beta_{k,j}.$$

Corollary 2.1. *Let M be an Artinian semisimple right R -module. Then:*

$$\text{End}_R(M) \cong M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k).$$

Proof. Since M is semisimple and Artinian:

$$M \cong \bigoplus_{i=1}^k M_i^{n_i},$$

with simple and pairwise nonisomorphic modules (if the sum were infinite we could show M is not Artinian by considering less and less coordinates). By Schur's lemma, $D_i := \text{End}_R(M_i)$ is a division algebra, and for every $1 \leq i \neq j \leq n$, we have $\text{Hom}_R(M_j, M_i) = 0$. Using the matrix description, we get that:

$$\text{End}_R(M) \cong M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k).$$

□

Definition 2.2 (Simple ring). A nonzero ring R is called simple if R and 0 are the only two-sided ideals.

Example 2.1. A division ring is a simple ring.

Example 2.2. We claim that if R is a simple ring then $M_n(R)$ is a simple ring.

- (1) We have to show that for every nonzero $X \in M_n(R)$, the two-sided ideal generated by X is equal to $M_n(R)$.
- (2) Let $X \in M_n(R)$ be a nonzero element and fix $1 \leq k, j \leq n$ such that $x := X_{k,l} \neq 0$.
- (3) For every $1 \leq i, j \leq n$ and every $t \in R$, let $e_{i,j}(t)$ be the matrix with t on the (i, j) th entry and 0 elsewhere.
- (4) In order to finish the proof, it is enough to show that for every $1 \leq i, j \leq n$, we have that $e_{i,j}(1)$ belongs to the two sided ideal generated by X .
- (5) Since R is a simple ring there exist $r_1, s_1, \dots, r_m, s_m \in R$ such that:

$$1 = r_1 x s_1 + \cdots + r_m x s_m \implies e_{i,j}(1) = e_{i,k}(r_1) X e_{l,j}(s_1) + \cdots + e_{i,k}(r_m) X e_{l,j}(s_m),$$

and this completes the proof.

Exercise 2.1. Let D be a field and V an $\aleph_0$ -dimensional D -module. Prove that:

- (1) The set $I := \{\alpha \in \text{End}_D(V) \mid \dim(\text{im } \alpha) < \infty\}$ is a nonzero proper two sided ideal of the space $E := \text{End}_D(V)$.
- (2) $R := E/I$ is a simple ring.
- (3) R_R does not contain a simple R -module.

Proof.

- (1) Note that a modules over a field is a vector space. Let $\alpha \in \text{End}_D(V)$ be an endomorphism which projects onto a 1 dimensional subspace of V . Since $\dim \text{im } \alpha = 1 < \infty$ we have $\alpha \in I$ hence $I \neq \emptyset$.

Let $\alpha \in I$ and $\beta, \gamma \in E$. We have that $\text{im}(\alpha \circ \beta) \subseteq \text{im}(\alpha)$ hence $\dim(\alpha \circ \beta) < \infty$ and so $\alpha \circ \beta \in I$. We also have that $\text{im}(\gamma \circ \alpha) = \gamma(\text{im } \alpha)$, and since $\dim(\text{im } \alpha) < \infty$, and γ is a linear map, we get that $\dim(\gamma \circ \alpha) < \infty$ and hence $\gamma \circ \alpha \in I$.

Additionally, I is additively closed since $\text{im}(\alpha + \beta) \subseteq \text{im } \alpha + \text{im } \beta$.

The ideal I is proper since $\dim(\text{id}_V) = \aleph_0$ hence $\text{id}_V \notin I$.

- (2) By the correspondence theorem we must show that any ideal $J \supsetneq I$ in E must be equal to E . Let $\alpha \in J \setminus I$, then $\dim \operatorname{im} \alpha = \aleph_0$, hence there exists some subspace $U \subseteq V$ such that the restriction $\alpha|_U: U \rightarrow \operatorname{im} \alpha$ is an isomorphism, hence $\dim U = \aleph_0$. Note that by the above claims, we have that there exist isomorphisms $\phi: V \rightarrow U$ and $\psi: \operatorname{im} \alpha \rightarrow V$. Note that we have that:

$$(\psi \circ P) \circ \alpha \circ \phi = \operatorname{id}_V,$$

where $P: V \rightarrow \operatorname{im} \alpha$ is the projection map. Since both $\psi \circ P$ and ϕ are elements in E , we get that $\operatorname{id}_V \in \langle \alpha \rangle \subseteq J$, hence $J = E$, which completes the proof.

- (3) A simple submodule of R_R corresponds to a minimal right ideal of R . We know from (2) that R has no nontrivial two sided ideals, but since it tells us nothing about the existence of right ideals, we have to do the work.

Let $0 \neq \alpha \in R = E/I$ meaning $\operatorname{im} \alpha = \aleph_0$. Let $\operatorname{im} \alpha = W_1 \oplus W_2$ so that $\dim W_1 = \dim W_2 = \aleph_0$. Let β be the projection of α onto W_1 , so that $\dim \operatorname{im} \beta = \dim W_1 = \aleph_0$ hence $0 \neq \beta \in R$. The inclusion $\beta R \subseteq \alpha R$ is obvious, and the inclusion is strict since $\alpha \notin \beta R$ (because by construction we would get $\dim W_2 < \aleph_0$). This implies that there is not minimal right ideal in R , hence R_R has no simple submodules.

□

Exercise 2.2. Let $n \geq 1$ and D be a division ring. View the elements of D^n as rows of elements in R . Prove that:

- (1) D^n is a simple right $M_n(D)$ -module.
- (2) $\operatorname{End}_{M_n(D)}(D^n) \cong D$.
- (3) $\dim_{\operatorname{End}_{M_n(D)}(D^n)}(D^n) = n$.

Proof.

- (1) Let $0 \neq v \in D^n$. We must show that $v \cdot M_n(D) = D^n$. Since D is a division ring, the conclusion is trivial.
- (2)
- (3)

□

Lemma 2.2. Let R be a simple ring. If R_R contains a simple right submodule M (equivalently, left), then all the simple submodules of R_R are isomorphic to M and R_R (equivalently, ${}_R R$) is semisimple.

Proof. For every $r \in R$ we know that rM is a submodule of R_R . If $rM \neq 0$, then the map $x \mapsto rx$ is a nonzero R -homomorphism from the simple right R -module M onto the right R -module rM so it must be an isomorphism. Since $\sum_{r \in R} rM$ is a nonzero two sided ideal of the simple ring R , it must be equal to R . Thus, R_R is an inner direct sum of the simple submodules isomorphic to M . In particular, R is semisimple and every simple submodule of R_R is isomorphic to M . □

Definition 2.3 (ρ -isomorphism). Let $\rho: R \rightarrow S$ be an isomorphism of rings. Let M be a right R -module and N a right S -module.

- (1) A bijective map $\psi: M \rightarrow N$ is called a ρ -isomorphism if for every $r \in R$ and $m \in M$, we have that $\psi(mr) = \psi(m)\rho(r)$.

(2) We say that M and N are ρ -isomorphic if there exists a ρ -isomorphism between them.

Remark 2.1. Let $\rho: R \rightarrow S$ be an isomorphism of rings, and $\psi: M \rightarrow N$ a ρ -isomorphism of right modules. The map $\bar{\psi}: \text{End}_R(M) \rightarrow \text{End}_S(N)$ defined by $\bar{\psi}(\alpha) := \psi \circ \alpha \circ \psi^{-1}$ for every $\alpha \in \text{End}_R(M)$, is an isomorphism of rings. Moreover, ψ is a $\bar{\psi}$ -isomorphism from the left $\text{End}_R(M)$ -module M to the left $\text{End}_S(N)$ module N . Indeed, for every $\alpha \in \text{End}_R(M)$ and every $m \in M$, we have:

$$\psi(\alpha(r)) = \psi \circ \alpha \circ \psi^{-1}(\psi(m)) = \bar{\psi}(\alpha)(\psi(m)).$$

Lemma 2.3. Let $n_1, n_2 \geq 2$ and D_1 and D_2 be division algebras. If $M_{n_1}(D_1) \cong M_{n_2}(D_2)$ then $D_1 \cong D_2$ and $n_1 = n_2$.

Proof. Let $\rho: M_{n_1}(D_1) \rightarrow M_{n_2}(D_2)$ be an isomorphism. For every $1 \leq r \leq 2$, we have that M_{n_r} is a simple ring so:

$$L_r := \{X \in M_{n_r}(D_r) \mid (\forall 2 \leq i \leq n_r \text{ and } \forall 1 \leq j \leq n_r) X_{i,j} = 0\}$$

is a minimal right ideal of $M_{n_r}(D_r)$. Since $M_{n_r}(D_r)$ is simple, every minimal right ideal of $M_{n_r}(D_r)$ is isomorphic to L_r as an $M_{n_r}(D_r)$ -module. Since ψ sends a minimal right ideal of $M_{n_1}(D_1)$ to a minimal right ideal of $M_{n_2}(D_2)$, we get that L_1 and L_2 are ρ -isomorphic, and:

$$D_1 \cong \text{End}_{M_{n_1}(D_1)}(L_1) \cong \text{End}_{M_{n_2}(D_2)}(L_2) \cong D_2.$$

Let $\bar{\psi}: \text{End}_{M_{n_1}(D_1)}(L_1) \rightarrow \text{End}_{M_{n_2}(D_2)}(L_2)$ be the isomorphism induced by ψ . Since L_1 and L_2 are also $\bar{\psi}$ -isomorphic:

$$n_1 = \dim_{\text{End}_{M_{n_1}(D_1)}(L_1)}(L_1) = \dim_{\text{End}_{M_{n_2}(D_2)}(L_2)}(L_2) = n_2,$$

which completes the proof. $\square$

Example 2.3. Theorem 2.3 is false over general rings. For example, $M_4(\mathbb{F}) \cong M_2(M_2(\mathbb{F}))$.

Lemma 2.4. Let $R_1, \dots, R_m$ and $S_1, \dots, S_n$ be simple rings and denote $R := R_1 \times \dots \times R_m$ and $S := S_1 \times \dots \times S_n$, and suppose that $R \cong S$. Then $m = n$ and there exists a permutation $\sigma \in \text{Sym}(n)$ such that for every $1 \leq i \leq m$, the map ψ induces an isomorphism of rings $\bar{\psi}_i: R_i \rightarrow S_{\sigma(i)}$.

Proof. We can view R (respectively, S) as an inner direct product of the R_i s (respectively, of the S_j s). In particular, we identify each R_i (respectively, each S_j) as a two sided ideal of R (respectively, S). Since each R_i (respectively, each S_j) is a simple ring, the sets $X := \{R_i \mid 1 \leq i \leq m\}$ and $Y := \{S_j \mid 1 \leq j \leq n\}$ are the sets of minimal two sided ideals of R and S respectively. Moreover, $|X| = m$ and $|Y| = n$. Since ψ is an isomorphism of rings, $m = n$ and there exists $\sigma \in \text{Sym}(m)$ such that for every $1 \leq i \leq m$, we have $R_i = S_{\sigma(i)}$. Let $1 \leq i \leq m$ and let $\bar{\psi}_i: R_i \rightarrow S_{\sigma(i)}$ be the map induced by ψ . Since ψ is a homomorphism of rings, $\bar{\psi}$ preserves addition and multiplication. It is left to show that for every $1 \leq i \leq m$, we have $\beta_i(1_{R_i}) = 1_{S_{\sigma(i)}}$. Since the β_i respect multiplication and are surjective, $\beta_i(1_{R_i})$ is an element of the ring $S_{\sigma(i)}$ such that for every $s \in S_{\sigma(i)}$ we have $s\beta_i(1_{R_i}) = s$. In particular, by taking $s := 1_{S_{\sigma(i)}}$ we get that:

$$\beta_i(1_R) = 1_{S_{\sigma(i)}}\beta_i(1_{R_i}) = 1_{S_{\sigma(i)}},$$

which completes the proof. $\square$

Corollary 2.5. *Let $m_1, \dots, m_r$ and $n_1, \dots, n_s$ be positive integers, and let $D_1, \dots, D_r$ and $E_1, \dots, E_s$ be division algebras such that:*

$$M_{m_1}(D_1) \times \cdots \times M_{m_r}(D_r) \cong M_{n_1}(E_1) \times \cdots \times M_{n_s}(E_s).$$

Then $r = s$ and there exists a permutation $\sigma \in \text{Sym}(r)$ such that for every $1 \leq i \leq r$ we have $n_{\sigma(i)}$ and $D_i \cong E_{\sigma(i)}$.

Proof. Immediate by Theorem 2.3 and Theorem 2.4. □

Definition 2.4. A ring R is called a right (equivalently, left) Artinian/Noetherian/semisimple ring if R is Artinian/Noetherian/semisimple as a right (equivalently, left) R -module.

Example 2.4. Here are some claims based on the previous definition:

- (1) The ring $\mathbb{Z}$ is not semisimple.
- (2) The ring $R := \mathbb{Z}/6\mathbb{Z}$ is not simple. It is semisimple since $R_R \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$.
- (3) In Exercise 2.1, we constructed a simple ring that does not contain a minimal ideal. It follows that this ring is not semisimple.
- (4) For every $n \geq 1$ and any division ring D , we have that $M_n(D)$ is right semisimple. Indeed, as a right module it is isomorphic to a direct sum of n copies of D^n where the elements of D^n are viewed as rows and $M_n(D)$ act by multiplication from the right.
- (5) Similarly, for every $n \geq 1$ and any division ring D we have that $M_n(D)$ is right semisimple.
- (6) If $R_1, \dots, R_n$ are semisimple rings, so is $R_1 \times \cdots \times R_n$.

Lemma 2.6.

- (1) *A right semisimple ring is right Artinian.*
- (2) *A left semisimple ring is left Artinian.*
- (3) *A simple ring is right (equivalently, left) semisimple if and only if it is right (equivalently, left) Artinian.*

Proof.

- (1) The module R_R is generated by its simple submodules. In particular, there are finitely many simple submodules $M_1, \dots, M_k$ such that $1_R \in \sum_{i=1}^k M_k$. It follows that $R = \{1_R r \mid r \in R\} \subseteq \sum_{i=1}^k M_k$. Since R_R is generated by finitely many simple submodules, R is right Artinian.
- (2) Analogous to (1).
- (3) By (1), if R is semisimple it is Artinian. Assume that R is simple and Artinian. Since R is Artinian, R_R contains a minimal submodule M . This claim follows from Theorem 2.2. □

Theorem 2.7 (Wedderburn structure theorem). *Let R be a ring. The following properties are equivalent:*

- (1) *R is a right semisimple ring.*
- (2) *R is a left semisimple ring.*

(3) There exist positive integers $n_1, \dots, n_k$ and division algebras $D_1, \dots, D_k$ such that $R \cong M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k)$.

Moreover, if (3) holds, then $n_1, \dots, n_k$ are unique and $D_1, \dots, D_k$ are unique up to isomorphism.

Proof. □

Corollary 2.8. *An Artinian simple ring is isomorphic to $M_n(D)$ for unique $n \geq 2$ and unique (up to isomorphism) division algebra D .*

Corollary 2.9. *There exists a simple ring which is not semisimple.*

Proof. The ring $R = E/I$ defined in Exercise 2.1 is simple (as shown in part (2) of the exercise), but since it is shown in part (3) that it is not Artinian, it cannot satisfy condition (3) in the Wedderburn structure theorem, hence it cannot be semisimple. □

3 Radicals

Definition 3.1 (Radical of a module). Let R be a ring and M be a left (or right) R -module. The radical of M is defined to be the intersection of all maximal modules of M . If none exist, then we define it to be M .

Remark 3.1. We denote the radical of M by $\text{Rad } M$.

Example 3.1. We have the following radicals:

- (1) $\text{Rad } \mathbb{Q}_{\mathbb{Q}} = 0$.
- (2) $\text{Rad } \mathbb{Q}_{\mathbb{Z}} = \mathbb{Q}$.
- (3) $\text{Rad}(\mathbb{Z}/6\mathbb{Z}) = 2\mathbb{Z}/6\mathbb{Z} \cap 3\mathbb{Z}/6\mathbb{Z} = 0$.
- (4) $\text{Rad } \mathbb{Z}/18\mathbb{Z} = 2\mathbb{Z}/18\mathbb{Z} \cap 3\mathbb{Z}/18\mathbb{Z} = 6\mathbb{Z}/18\mathbb{Z}$.

Exercise 3.1. Let $n \geq 1$, and let D be a division ring. Denote by $R = M_n(D)$. Show that $\text{Rad}_R R = \text{Rad } R_R = 0$.

Lemma 3.1. Let R be a ring and $\alpha: M \rightarrow N$ an R -homomorphism. Then $\alpha(\text{Rad } M) \subseteq \text{Rad } N$.

Proof. We have that:

$$\alpha^{-1}(\text{Rad } N) = \bigcap_{L \text{ maximal in } N} \alpha^{-1}L,$$

and thus we simply need to show that if L is a maximal module of N , then $\alpha^{-1}(L)$ contains $\text{Rad } M$. Let L be a maximal submodule of N . α induces an injective R -homomorphism:

$$\bar{\alpha}: M/\alpha^{-1}(L) \rightarrow N/L,$$

where N/L is a simple ideal, hence there are only two possibilities:

- (1) $\text{im } \bar{\alpha} = 0$ and then $\alpha^{-1}(L) = M$.
- (2) $\bar{\alpha}$ is an isomorphism, and hence $P := \alpha^{-1}(L)$ is a maximal submodule of M and so $\text{Rad } M \subseteq P = \alpha^{-1}(L)$.

This completes the proof. □

Corollary 3.2. Let R be a ring. Then $\text{Rad } R_R$ and $\text{Rad}_R R$ are two-sided ideals.

Proof. Without loss of generality we will only prove the case for $\text{Rad } R_R$. It is clear that $\text{Rad } R_R$ is a right ideal. Thus it suffices to show that for every $r \in R$,

$$r \text{Rad } R_R \subseteq \text{Rad } R_R.$$

This follows from Theorem 3.1 since the map $R_R \rightarrow R_R$ which sends $x \mapsto rx$ is an R -homomorphism. □

Lemma 3.3. Let R be a ring and M be an R -module. Then for every $m \in M$ the following conditions are equivalent:

- (1) $m \in \text{Rad } M$.
- (2) For every $N \leq M$, if M is generated by $N \cup \{m\}$ then $N = M$.

Proof.

- (1) $\implies$ (2) Let N be a submodule of M such that $N \cup \{m\}$ generates M . Assume, by way of contradiction, that $M = N$. Since $N \cup \{m\}$ generates M , we conclude that $m \notin N$, hence $M \neq N$. Denote:

$$X := \{L \leq M \mid N \subseteq L \text{ and } m \notin L\}.$$

The set X is nonempty since $N \in L$ and it is closed under unions of increasing chains, and hence by Zorn's lemma there exists a maximal element P . We know that $M \notin X$ and hence $P \neq M$. P is a maximal submodule with respect to the property of containing N and not containing m . We will now show that P is a maximal submodule of M in contradiction to:

$$P \supseteq \text{Rad } M \text{ and } m \notin P \text{ and } m \notin \text{Rad } M,$$

where the first inclusion follows from P being a maximal submodule. Assume that exists $P \leq Q \leq M$ with $P \neq Q$. Then since P is maximal in X , we get that $Q \notin X$, but $N \subseteq P \subseteq Q$ and so $m \in Q$. This implies that $Q = M$ since M is generated by $N \cup \{m\}$.

- (2) $\implies$ (1) Let $m \in M$ be an element that satisfies the property in (2). Let L be a maximal submodule of M . We need to show that $m \in L$. Assume, by way of contradiction, that $m \notin L$. Then, by maximality of L , the submodule generated by $L \cup \{m\}$ is M . By assumption on m , we get $M = L$. This contradiction completes the proof. □

Lemma 3.4 (Nakayama's lemma). *Let R be a ring, let M be an R -module, and let $P \leq M$. Then:*

- (1) *Assume that for every $N \leq M$, if $P + N = M$ then $N = M$. Then $P \subseteq \text{Rad } M$.*
- (2) *If $P \subseteq \text{Rad } M$ and M or P are finitely generated as modules over R , then for every submodule $N \leq M$, if $M = P + N$ then $M = N$.*

Proof.

- (1) We need to show that if N is a maximal submodule of M , then $P \leq N$. Since $N \neq M$ (by definition) the assumption of (1) shows that $P + N \neq M$. From maximality of N , we get $N = P + N$, which means that $P \leq N$.
- (2) If P is finitely generated as a module over R , then we get the claim from induction over the minimal number of generators of P and the previous lemma. Next assume that M is finitely generated and that $N \leq M$ such that $M = P + N$. Denote the generators of M by $x_1, \dots, x_k$. Since $M = P + N$ we get that for any $1 \leq i \leq k$ there exists $y_i \in P$ and $z_i \in N$ such that $x_i = y_i + z_i$. Denote by Q the submodules of M generated by $y_1, \dots, y_k$. Then:

- (1) $Q \subseteq P \subseteq \text{Rad } M$.
- (2) Q is finitely generated.
- (3) $M = Q + N$.

From the previous case we get that $M = N$, which completes the proof. □

Example 3.2. We have that $P = \text{Rad } \mathbb{Q}_{\mathbb{Z}} = \mathbb{Q}$. We have $0 \neq \mathbb{Q}$ and $0 + P = \mathbb{Q}$. This shows that the assumption of being finitely generated is necessary.

3.1 Jacobson's radical

Lemma 3.5 (Nakayama's lemma). *Let $R \neq 0$ be a ring with maximal $P \triangleleft R$. Then the following conditions are equivalent:*

- (1) $P \subseteq \text{Rad } R_R$.
- (2) *If M is a finitely generated right R -module and $N \leq M$ satisfies $M = N + MP$, then $N = M$.*
- (3) $\{1 + x \mid x \in P\} \in R^\times$.

Proof.

- (1) $\implies$ (2) Let M be a finitely generated module over R . For every $m \in M$ the map $\alpha_m: R_R \rightarrow M$ given by $x \mapsto mx$ is an R -homomorphism. Thus, by the lemma from the beginning of the section:

$$MP = \sum_{m \in M} mP = \sum_{m \in M} \alpha_m(P) \subseteq \text{Rad } M.$$

The rest follows from Nakayama's lemma for modules.

- (2) $\implies$ (3) Denote $G := \{1 + x \mid x \in P\}$. Since P is a right ideal, G is closed under multiplication and contains 1. We will show that every element in G has a right inverse in R . First, Assume by way of contradiction, that $x \in P$ and that $1 + x$ does not have a right inverse in R . Then $I := (1 + x)R \neq R$ is a right ideal and hence contained in a maximal right ideal J . Since $1 + x \in J$ then $x \notin J$. Hence, since J is maximal $R_R = J + xR$. From (2) it follows that $J = R_R$, which is a contradiction.

We finished showing that for any $g \in G$ there exists a right inverse in R . Now we will prove that any $g \in G$ has a right inverse in G . Let $g \in G$. There exist $x \in P$ and $y \in R$ such that $g = 1 + x$ and $1 = xy$. Denote $z := y - 1$, and then:

$$1 = (1 + x)(1 + z) = 1 + x + z + xz,$$

and $z = -x - xz \in P$. Thus, $y = 1 + z \in G$. We will now show that for any $g \in G$ there is a left inverse in G which completes this part of the proof. Let $g \in G$, there exists $h \in G$ inverse to g

(3)

□

Corollary 3.6. *Let R be a ring. Then $\text{Rad}_R R = \text{Rad } R_R$.*

Proof. By the left version of Nakayama's lemma for rings (specifically (3) implies (1)), we get that $\{1 + x \mid x \in \text{Rad}_R R\} \subseteq R^\times$. We have seen before that $\text{Rad}_R R$ is a two sided ideal, and in particular a right ideal. By (3) implies (1) (in the right versino of Nakayama's lemma) we get that $\text{Rad}_R R \subseteq \text{Rad } R_R$. From symmetry, we get that other direction of containment, hence they are equal. □

Definition 3.2 (Jacobson radical). Let R be a ring. The Jacobson radical of R is defined by:

$$J(R) := \text{Rad}_R R = \text{Rad } R_R.$$

Exercise 3.2. Show that if R is an Artinian ring, then $R/J(R)$ is a semisimple ring.

Exercise 3.3. Let R be a ring. Let I be a right (or left ideal), such that all of its elements are nilpotent. Show that $I \in J(R)$.

3.2 Radicals in Artinian rings

Proposition 3.7. *Let R be an Artinian ring. Then there exists $k \geq 1$ such that $J(R)^k = 0$.*

Proof. We know that:

$$\cdots \subseteq J(R)^3 \subseteq J(R)^2 \subseteq J(R).$$

Since R is Artinian, there exists $k \geq 1$ such that $J(R)^k = J(R)^{k+m}$ for every $m \in \mathbb{N}$. In particular, $J(R)^k = J(R)^{2k}$. We claim that $J(R)^k = 0$. Denote:

$$X := \left\{ 0 \neq I \triangleleft R_R \mid IJ(R)^k = I \right\}.$$

The set X is nonempty since $J(R)^k \in X$. Since X is Artinian, there exists a minimal element L in X . Since $L \neq 0$, there exists $0 \neq \ell \in L$. Note that:

$$L \supseteq \ell J(R)^k \in X,$$

so by minimality of L ,

$$L = \ell J(R)^k \subseteq \ell R \subseteq L,$$

and so L is finitely generated as an ideal. Moreover, $L = 0 + L = 0 + LJ(R)^k$. By Nakayama's lemma for rings we get that $L = 0$, which is a contradiction. $\square$