Ring Theory

Lecturer: Professor Charudatta Hajarnavis

Notes: James Taylor

December 2019

Contents

Introduction

These are lecture notes from the course Ring Theory, given by Professor Charudatta Hajarnavis at the University of Warwick in 2019, written by James Taylor.

If any mistakes are identified, please email me (James Taylor).

Overview

In this course we aim to study non-commutative rings with chain conditions. A commutative integral domain has a (unique) field of fractions. What happens if we drop the commutativity axiom? Do we now obtain a division ring of fractions? If not always then when exactly? Do we need to differentiate between the left hand side and the right hand side of the ring? Also, does the theory extend meaningfully to rings such as rings of matrices which contain zero divisors? We shall give precise answers to all these questions.

Topics covered in pursuit of the above will include prime and semiprime rings, Artinian rings, composition series, the singular submodule, Ore's theorem leading up to Goldie's theorems and their applications.

0 Rings and Modules Preliminaries

A familiarity with the basics of rings and modules is assumed. We list some definitions and facts that we will reference here.

Rings

Generally the rings we consider will not necessarily have an identity or be commutative. We assume knowledge of the notations of subrings and ideals (all ideals are subrings), ring homomorphisms, quotient rings. The kernel of a ring homomorphism is an ideal, and the image generally only a subring. We have the isomorphism theorems similar to those for modules in the next section, and along with internal and external direct sums.

Definition 0.1. A *division ring* is a ring D with 1, $1 \neq 0$, such that for all non-zero elements u, there is $d \in D$ with $ud = du = 1$. When the multiplication in D is commutative we call D a field.
A ring where the product of non-zero elements is non-zero is called a *domain*. If this is commutative, we call this an *integral domain*.

Modules

Definition 0.2. For a ring R, a right R-module is an Abelian group M and ring homomorphism $f : R^{op} \to \mathrm{End}(M)$. We write M_R. A left R-module is an Abelian group M and a ring homomorphism $f : R \to \mathrm{End}(M)$, and we write ${}_RM$. These do not assume that R has an identity, and when R does we call these modules *unital* if additionally $f(1)$ is the identity of M.

All modules we consider if not specified will be assumed to be right modules. This will make life slightly easier - see remark 0. Furthermore, if R has an identity, we will assume that any R-modules we consider are unital - see exercise 7.
We assume a familiarity with submodules, quotient modules, module homomorphisms, kernels, cokernels, and the first isomorphism theorem.

Proposition 0.3. *Let K, L be submodules of M_R. Then*

$$(L + K)/K \cong L/(L \cap K).$$

Furthermore, if $K \subset L$, then L/K is a submodule of M/K, and

$$(M/K)/(L/K) \cong M/L.$$

Given R-modules M_i we can define the external direct product and direct sum. These are the same for finite index sets, but can differ otherwise - the sum requires all but finitely many entries of an element to be 0. Categorically, the direct product is a product, and the direct sum is a coproduct.
Given an R-module M with submodules M_i, we can define their sum to be the set of all finite sums of elements of some finite subset of the M_i. This forms a submodule, and is called the internal sum. We write

$$\sum_i M_i.$$

This sum is said to be direct if every element has a unique representation in this sum. We write

$$\bigoplus_i M_i.$$

We can express this equivalently as: for all j,

$$M_j \cap \left(\sum_{i:i\neq j} M_i \right) = 0.$$

Let M be a R-module, and K, S subsets of M, R respectively. We define their product to be finite sums of ks where $k \in K$, $s \in S$. If K is a non-empty subset of M, and S a right ideal then KS is a submodule of M. In particular this applies when $M = R$. So for $\emptyset \neq S \subset R$ we can define S^2, and inductively S^n for $n \in \mathbb{N}$. If S is a right ideal of R then so is S^n.

Let R be a ring with an ideal I, and let M be a right R-module. Generally M need not be a right R-module. However, if $MI = 0$, then M can be given the structure of a right R/I-module.

Proposition 0.4. *Let R be a ring with an ideal I, and let M be a right R-module with $MI = 0$. Then $m(r + I) := mr$ makes M a well-defined R/I-module, and as the quotient map is surjective, R and R/I submodules of M coincide.*

In particular, $(I^n/I^{n+1})I = 0$, so (I^n/I^{n+1}) is naturally a right (and left) R/I-module. Note that if $MI \neq 0$, then this definition will not be well-defined.

If $M_1 \cong M_2$ as modules, then $\mathrm{End}(M_1) \cong \mathrm{End}(M_2)$ as rings.

Proposition 0.5. *Let R be a ring with identity. Then as rings,*

$$R \cong \mathrm{End}(R_R)$$

Proof. For $x \in R$, let $\rho_x : R \to R$, $\rho_x(r) = xr$. ∎

Remark. If we write our endomorphism composition in the same way, but consider *left* R-modules, then the isomorphism we obtain is

$$R^{op} \cong \mathrm{End}({}_R R).$$

We could remedy this by writing our functions on the right in $\mathrm{End}(M)$, and then work with left modules with the nicer isomorphism.

Let X, Y be R-modules. $\mathrm{Hom}_R(X, Y)$ is easily seen to be an Abelian group.

Lemma 0.6. *Let $V = V_1 \oplus \cdots V_n$, $W = W_1 \oplus \cdots W_m$, for submodules V_i, W_j of R-modules V, W. Then*

1. *As Abelian groups,*

$$\mathrm{Hom}_R(V, W) \cong \begin{bmatrix} \mathrm{Hom}_R(V_1, W_1) & \cdots & \mathrm{Hom}_R(V_n, W_1) \\ \vdots & \ddots & \vdots \\ \mathrm{Hom}_R(V_1, W_m) & \cdots & \mathrm{Hom}_R(V_n, W_m) \end{bmatrix}$$

2. *In particular, for a R module M,*

$$\mathrm{End}_R(M^{(n)}) \cong M_n(\mathrm{End}_R(M))$$

as rings.

1 Chain Conditions

1.1 Finitely Generated Modules

Definition 1.1. Let $T \subset M_R$. Then $\langle T \rangle$ is the intersection of all submodules containing T. By definition $\langle \emptyset \rangle = 0$.

In particular, if $T = \{a\}$, then we have $\langle a \rangle = \{ar + \lambda a \mid r \in R, \lambda \in \mathbb{Z}\}$. When R and M are unital, then $\langle a \rangle = aR = \{ar \mid r \in R\}$.

Note. aR is always a submodule of M, but when M is not unital there is no guarantee that $a \in aR$.

Definition 1.2. M_R is said to be *finitely generated* if $M_R = \langle T \rangle$ for some finite subset T.

If R has 1 and M is unital and finitely generated, then there exists $a_1, ..., a_m \in M$ with $M = a_1 R + a_2 R + ... + a_m R$. We call the a_i generators. If M is generated by one element then M is called cyclic. So a finitely generated module is a finite sum of cyclic modules. Both R_R and ${}_R R$ are cyclic R modules with generator 1. Cyclic submodules of R_R $[{}_R R]$ are called principal right [left] ideals of R.

1.2 Finiteness Assumptions

Definition 1.3. Let $\mathcal{C}$ be a non-empty collection of submodules of M_R. $K \in \mathcal{C}$ is *maximal in $\mathcal{C}$* if there does not exist any $N \in \mathcal{C}$ with $K \subsetneq N$. Similarly $K \in \mathcal{C}$ is *minimal in $\mathcal{C}$* if there does not exist any $N \in \mathcal{C}$ with $N \subsetneq K$.

M_R has the *ACC for submodules in $\mathcal{C}$*, if every chain

$$A_1 \subset A_2 \subset ...$$

stabilises: $\exists k \in \mathbb{N}$ with $A_k = A_{k+1} = ...$. M_R has the *maximum condition on submodules in $\mathcal{C}$*, if every non-empty collection of submodules in $\mathcal{C}$ has a maximal submodule. We similarly define the *DCC* and minimum condition on submodules in $\mathcal{C}$.

Proposition 1.4. *Let $\mathcal{C}$ be a non-empty collection of submodules of M_R. Then TFAE:*

(a) M_R has ACC [DCC] on submodules in $\mathcal{C}$.

(b) M_R has maximum [minimum] condition on submodules in $\mathcal{C}$.

Proof. We will do the ACC case, with the DCC case being symmetric. Suppose that M_R has ACC on submodules in $\mathcal{C}$, and let $\mathcal{B}$ be non-empty set of submodules of $\mathcal{C}$. Suppose that this $\mathcal{B}$ has no maximal submodule. So taking any $N_1 \in \mathcal{B}$, we can construct a chain inductively, for $N_i \in \mathcal{B}$ not maximal in $\mathcal{B}$ implies that there is some $N_{i+1} \in \mathcal{B}$ with $N_i \subsetneq N_{i+1}$. But this chain contradicts the ACC. Conversely, given any chain, we take $\mathcal{B} \subset \mathcal{C}$ as the collection of all submodules in the chain, and a maximal element in the chain implies this chain stabilises. ∎

Definition 1.5. We say M_R has ACC, if M_R has ACC for submodules in the collection of all submodules of M_R.

We say M_R has maximal condition, if M_R has maximal condition on submodules in the collection of all submodules of M_R.

Proposition 1.6. *TFAE for any M_R:*

(a) M has ACC.

(b) M has maximal condition.

*(c) **Every** submodule of M is finitely generated.*

Remark. M being finitely generated does not imply that all submodules are! See exercise 11.

Proof. All that is left to show is that (c) is equivalent to either (a) or (b).
(a) $\Rightarrow$ (c): Take any submodule S. If S is not finitely generated, then we can find a sequence of elements $a_1, a_2, ..$ from S such that $a_i \notin \langle a_1, ..., a_{i-1} \rangle$ for each i. But then this contradicts ACC.
(c) $\Rightarrow$ (b): Suppose that there is some non empty collection $\mathcal{C}$ of submodules which do not have a maximal element. So we can construct a sequence $M_1 \subsetneq M_2 \subsetneq ...$ of elements of $\mathcal{C}$. Let N be their union. If N was finitely generated then it's generators must all be in M_k for some k, and so this would contradict that $M_k \neq M_{k+1}$. So N is not finitely generated. ∎

Example 1.7. Any PID has all ideals finitely generated, so as right modules over themselves have ACC. Therefore, $\mathbb{Z}_\mathbb{Z}$ has ACC. Note that with $\mathbb{Z}$ we can construct arbitrarily long chains, so there is no universal bound of the length of strict chains. We will see later though when we look at composition series, that if we require ACC and DCC, then we can actually get universal bounds.

Lemma 1.8 (Dedekind Modular Law)**.** *Let A, B, C be submodules of M_R, with $A \supset B$. Then:*

$$A \cap (B + C) = B + A \cap C \; (= A \cap B + A \cap C)$$

"If $A \supset B$, then the distributive law holds."

Proof. If $x = b + c \in A \cap B + A \cap C$, then $b + c \in A$, so $x \in A \cap (B + C)$. If $x = b + c \in A \cap (B + C)$, then $c = x - b \in A$, as $B \subset A$, so $x \in A \cap B + A \cap C$. ∎

Proposition 1.9. *Let K be a submodule of M_R. Then M_R has ACC [DCC] $\Leftrightarrow$ Both K and M/K have ACC [DCC].*

Proof. Here is the ACC case. The DCC case is similar.
"$\Rightarrow$": Every submodule of M is finitely generated, so all submodules of K must be too, so K has ACC. Any submodule of M/K is the image of a submodule of M under the quotient map, so must be finitely generated, thus M/K has ACC.
"$\Leftarrow$": Let $M_1 \subset M_2 \subset ...$ be an ascending chain. Then both

$$K \cap M_1 \subset K \cap M_2 \subset ...$$
$$M_1 + K \subset M_2 + K \subset ..$$

stabilise after some $N \in \mathbb{N}$. The first because K has ACC, and the second via the quotient subgroup correspondence, because the chain

$$(M_1 + K)/K \subset (M_2 + K)/K \subset ..$$

must stabilise. Therefore for any $i \geq 0$,

$$\begin{aligned} M_{N+i} &= M_{N+i} \cap (M_{N+i} + K) \\ &= M_{N+i} \cap (M_N + K) \\ &= M_{N+i} + (M_{N+i} \cap K) \\ &= M_N + (M_N \cap K) \\ &= M_N \end{aligned}$$

■

This proposition has many useful consequences, which we shall now explore.

Corollary 1.10. *Let $M_1, M_2, ..., M_n$ be submodules of M_R. If each M_i has ACC [DCC] then so does $M_1 + ... + M_n$.*

Proof. By induction on n. Let $L = M_1 + ... + M_{n-1}$ have ACC. Let $K = L + M_n$. Then $K/L = (L + M_n)/L \cong M_n/(M_n \cap L)$, which has ACC as a quotient of M_n. So as L has ACC, so does K. ■

Corollary 1.11. *Let R have 1, with ACC [DCC] on right ideals of R (submodules of R_R). Let M_R be a unital finitely generated module. Then M_R has ACC [DCC].*

Proof. For ACC: As M_R is unital and finitely generated, there exist $m_i \in M$ such that $M = m_1R+...+m_kR$. Therefore, it is sufficient to show that m_iR has ACC on submodules. Indeed, let $\psi_i : R \to m_iR$, $\psi_i(r) = m_ir$, a surjective homomorphism of modules. So $m_iR \cong R/\ker(\psi_i)$ has ACC. ■

Remark. What if R does not have 1? Here the ACC and DCC cases are not symmetric. For ACC the result is still true, but for DCC is not. This is due to the fact that for a general R,

$$\langle m \rangle = mR + m\mathbb{Z}$$

and $\mathbb{Z}$ has ACC but not DCC. Find an example where the theorem doesn't hold for DCC.

Corollary 1.12. *If R has ACC [DCC] on right ideals, then so does $M_n(R)$.*

Proof. Consider $M_n(R)$ as a right R module. Let $T_{ij} \cong R$ be the R submodule of the (i, j)th position. Each T_{ij} has ACC [DCC], and so $M_n(R) = \sum T_{ij}$ has ACC [DCC] as a right R module. Then the result follows, as right ideals of $M_n(R)$ are also R submodules (we have actually proven something slightly stronger). ■

Definition 1.13. A module with ACC on submodules is called *Noetherian*, and with DCC on submodules is called *Artinian*. A ring is right Noetherian if it has ACC on right ideals. A ring is right Artinian, if it has 1 and has DCC on right ideals. A ring is Noetherian if both right and left Noetherian, and Artinian if both right and left Artinian.

Remark. Why do we add the condition that Artinian rings must have identity? We will see in 3.20 that "most" rings with DCC have an identity automatically, and rings with DCC but not identity are quite peculiar, see Baer's example in exercise 15.

Example 1.14. $M_n(\mathbb{Z})$ is Noetherian, and $M_n(k)$ for any field k is both Artinian and Noetherian.
By applying the reasoning used in the proof, one can show both

$$\begin{bmatrix} \mathbb{Z} & 2\mathbb{Z} \\ \mathbb{Z} & \mathbb{Z} \end{bmatrix} \text{ and } \begin{bmatrix} \mathbb{Z} & \mathbb{Z} \\ 0 & \mathbb{Z} \end{bmatrix}$$

are Noetherian (see exercise 17).

We will use the following without proof:

Theorem 1.15 (Hilbert Basis Theorem)**.** *If R is a unital right (resp. left) Noetherian ring, then $R[x]$ is a unital right (resp. left) Noetherian ring.*

1.3 Composition Series

We will see in this section, that together ACC and DCC together can be used to give certain invariants of a module.

Definition 1.16. M_R is said to have *finite length* if there exists a chain of submodules

$$M = M_0 \supsetneq M_1 \supsetneq ... \supsetneq M_{k-1} \supsetneq M_k = 0$$

such that no submodule can be properly inserted between any two.

If R and M are unital, then this means that each quotient M_i/M_{i+1} is irreducible.

Definition 1.17. We call such a series a *composition series* for M, and each quotient M_i/M_{i+1} a factor of the series. We call k the length of the series. Given two series

$$M = M_0 \supsetneq M_1 \supsetneq ... \supsetneq M_{s-1} \supsetneq M_s = 0$$
$$M = K_0 \supsetneq K_1 \supsetneq ... \supsetneq K_{t-1} \supsetneq K_t = 0$$

these are *equivalent*, if $s = t$ and there exists $\sigma \in S_t$ with

$$M_i/M_{i+1} \cong K_{\sigma(i)}/K_{\sigma(i)+1}$$

for all i.

Example 1.18. One pair of equivalent composition series are

$$\mathbb{Z}/6\mathbb{Z} \supsetneq 2\mathbb{Z}/6\mathbb{Z} \supsetneq 0$$
$$\mathbb{Z}/6\mathbb{Z} \supsetneq 3\mathbb{Z}/6\mathbb{Z} \supsetneq 0$$

Lemma 1.19. *M_R has a composition series if and only if M_R has both ACC and DCC.*

Proof. "$\Leftarrow$": By ACC we can choose M_1 maximal such that $M = M_0 \supsetneq M_1$. Continue this process to choose M_2, M_3 etc. Then by DCC this process must terminate.
"$\Rightarrow$": Induction on k, the least length of a composition series for M. If $k = 1$, then M is simple. Now assume true for M_R with composition series of least length smaller than k. Take a composition series

$$M = M_0 \supsetneq M_1 \supsetneq ... \supsetneq M_k = 0$$

which is a shortest composition series for M. Then

$$M_1 \supsetneq \dots \supsetneq M_k = 0$$

is a shortest composition series for M_1. By the induction hypothesis, M_1 has ACC and DCC, and M/M_1 has a composition series of length 1 so has ACC and DCC. Then by 1.9, M has both ACC and DCC. ■

Lemma 1.20. *Let M_R be a module admitting a composition series. Then any series of submodules can be* refined *to a composition series, by inserting extra terms as needed.*

Proof. Let

$$M = A_0 \supsetneq A_1 \supsetneq \dots \supsetneq A_k = 0$$

be a series of submodules in M. By the above, M_R has both ACC and DCC. Choose a submodule B_1 with

$$A_0 \supsetneq B_1 \supsetneq A_1$$

where B_1 is minimal containing A_1. This can be chosen by DCC. Then choose B_2 such that

$$A_0 \supsetneq B_2 \supsetneq B_1 \supsetneq A_1$$

where B_2 is minimal containing B_1, again using DCC. This process must terminate, by ACC. ■

Now we show that the concept of length of a module is well defined. The proof here for modules is much simpler than the proof of the corresponding theorem for groups.

Theorem 1.21 (Jordan Hölder)**.** *Any two composition series for a module are equivalent.*

Proof. Let M_R admit a composition series. Let $\lambda(M)$ be the length of a shortest composition series for M. We use induction on $\lambda(M)$. If $\lambda(M) = 1$, then M is irreducible. Suppose that the result holds for all modules X_R with $\lambda(X) \leq s - 1$. Let M_R have $\lambda(M) = s$, so there exists a shortest composition series

$$M = M_0 \supsetneq M_1 \supsetneq \dots \supsetneq M_s = 0 \tag{A}$$

Consider another composition series

$$M = K_0 \supsetneq K_1 \supsetneq \dots \supsetneq K_n = 0 \tag{B}$$

Now as both M_{s-1} and K_{n-1} are simple, we must have that either $M_{s-1} = K_{n-1}$, or $M_{s-1} \cap K_{n-1} = 0$ (a classic strategy when dealing with simple modules).
Case 1: $M_{s-1} = K_{n-1}$. Divide both series by M_{s-1}:

$$M = M_0/M_{s-1} \supsetneq M_1/M_{s-1} \supsetneq \dots \supsetneq M_{s-1}/M_{s-1} = 0 \tag{C}$$
$$M = K_0/M_{s-1} \supsetneq K_1/M_{s-1} \supsetneq \dots \supsetneq K_{n-1}/M_{s-1} = 0 \tag{D}$$

which are two composition series for M/M_{s-1}, and $\lambda(M/M_{s-1}) = s-1$. So by induction, $s - 1 = n - 1$, hence $s = n$ and (C) and (D) are equivalent by the module isomorphism theorems.
Case 2: $M_{s-1} \cap K_{n-1} = 0$. Then $M_{s-1} + K_{n-1}$ is a direct sum. Then by 1.20 we can construct a compostion series for M:

$$M = Q_0 \supsetneq Q_1 \supsetneq \dots \supsetneq Q_{t-3} \supsetneq M_{s-1} \oplus K_{n-1} \supsetneq M_{s-1} \supsetneq M_s = 0 \tag{E}$$

By case 1, $s = t$, and (E) is equivalent to (A). Now we need to do the work that doesn't just use the induction hypothesis: Consider

$$M = Q_0 \supsetneq Q_1 \supsetneq \ldots \supsetneq Q_{t-3} \supsetneq M_{s-1} \oplus K_{n-1} \supsetneq K_{n-1} \supsetneq K_n = 0 \tag{F}$$

a composition series equivalent to (E), with just the last two composition factors swapped. (F) has length s, and the last non zero term is K_{n-1}, so (F) is equivalent to (B) as in case 1. Therefore, as equivalence is transitive, (A) is equivalent to (B). ■

Definition 1.22. For a module M_R of finite length, let $|M|$ denote the length.

Corollary 1.23. *Let M_R be a module of finite length, and K a submodule. Then*

$$|M| = |K| + |M/K|$$

Proof. Exercise 42. ■

2 Basic Concepts in Non-Commutative Rings

2.1 Prime Ideals

Definition 2.1. An ideal $I \lhd R$ is *prime* if $P \neq R$, $A, B \lhd R$ and $AB \subset P \Rightarrow A \subset P$ or $B \subset P$.

Example 2.2. In a unital ring, maximal ideals are prime: Suppose that P is maximal, but not prime, so there is some A, B ideals with $AB \subset P$, but $A \not\subset P$, $B \not\subset P$. Let $a \in A \setminus P$, $b \in B \setminus P$. Then $ab \in P$. Let C be the ideal generated by P and a, which as P is maximal must equal R, and as $1 = x + ar$ for some $x \in P$, $r \in R$. But then $b = bx + bar \in P$.

We will see later that every unital ring contains a maximal ideal, and so a prime ideal.

Theorem 2.3. *Let $P \lhd R$, $P \neq R$. Then TFAE:*

(a) P is prime.

(b) If $A, B \lhd_r R$, then $AB \subset P \Rightarrow A \subset P$ or $B \subset P$

(c) If $A, B \lhd_l R$, then $AB \subset P \Rightarrow A \subset P$ or $B \subset P$

(d) $aRb \subset P$ and $a, b \in R \Rightarrow a \in P$ or $b \in P$.

Proof. For (b) $\Rightarrow$ (a) $\Rightarrow$ (d) $\Rightarrow$ (b): The first is trivial. Let $aRb \subset P$ and $a, b \in R$. Then $(RaR), (RbR) \lhd R$, and $(RaR)(RbR) \subset R(aRb)R \subset RPR \subset P$. Then either $RaR \subset P$ or $RbR \subset P$. (If R is unital we are done here) Then suppose that $RaR \subset P$. Define

$$\langle a \rangle := \left\{ \lambda a + ra + as + \sum_i r_i a s_i \mid \lambda \in \mathbb{Z}, r, s, r_i, s_i \in R \right\}$$

Then this is an ideal. We have that $RaR \subset \langle a \rangle^3 \subset P$, so $\langle a \rangle \subset P$, so $a \in P$.
For $(d) \Rightarrow (b)$, Let $AB \subset P$, where these are right R modules. Suppose that $A \not\subset P$. Then fix some $a \in P \setminus A$. Then for any $b \in B$, $aRb \subset P$, so $b \in P$.
Similarly for (c) $\Rightarrow$ (a) $\Rightarrow$ (d) $\Rightarrow$ (c). ■

Corollary 2.4. *Let P be a proper ideal of a commutative ring R. Then P is a prime ideal if and only if P is completely prime ($ab \in P \Rightarrow a \in P$ or $b \in P$), if and only if R/P is an integral domain.*

Proof. If P is prime then $ab \in P$ means that $aRb = abR \subset P$, so $a \in P$ or $b \in P$ by the final equivalent condition. Conversely, if P is not prime, then there are ideals $AB \subset P$ with $A \not\subset P$, $B \not\subset P$, so there is $ab \in P$ with $a \notin P$, $B \notin P$. ∎

Definition 2.5. R is called a *prime ring* if 0 is a prime ideal.

Example 2.6. Directly from the definition, domains are prime rings, and by the above this is equivalent for commutative rings. $M_2(\mathbb{Z})$ is not an integral domain, so 0 is not completely prime. But 0 is a prime ideal ($AB = 0 \Rightarrow A = 0$ or $B = 0$), and so $M_2(\mathbb{Z})$ is a prime ring.

2.2 Ideals in Matrix Rings

Let R be a unital ring, and (a_{ij}) an $n \times n$ matrix with $a_{ij} \in R$. Let E_{ij} be the matrix with a single 1 in the (i, j) th place. Then $(a_{ij}) = \sum_i \sum_j a_{ij} E_{ij}$ uniquely. Also $E_{ij} E_{kl} = \delta_{jk} E_{il}$.

Theorem 2.7. *Let R be a unital ring. Then*

1. $I \lhd R \Rightarrow M_n(I) \lhd M_n(R)$
2. *(Converse) Every ideal of $M_n(R)$ is of the form $M_n(I)$ for some $I \lhd R$.*

Proof. Let $X \lhd M_n(R)$. Let $A = (a_{ij}) \in X$. Consider a fixed $1 \leq \alpha, \beta \leq n$. We have that

$$E_{1\alpha} \left(\sum_{i,j} a_{ij} E_{ij} \right) E_{\beta 1} \in X$$

So $a_{\alpha\beta} E_{11} \in X$. Letting I be all elements that occur in the top left hand corner of some matrix of X, then $I \lhd R$, and $X = M_n(I)$. ∎

What is a characterisation of right/left ideals? See this stackexchange answer.

Example 2.8. Not true for right ideals. Take

$$\begin{bmatrix} 2\mathbb{Z} & 2\mathbb{Z} \\ 0 & 0 \end{bmatrix} \lhd_r M_2(\mathbb{Z})$$

which is not of the form above.

Corollary 2.9. *If R is a unital ring and R is prime, then so is $M_n(R)$.*

Example 2.10. $M_n(\mathbb{Z})$ is an example of a non-commutative prime noetherian ring.

Definition 2.11. An *domain* is a ring R with $ab = 0 \Rightarrow a = 0$ or $b = 0$.

Example 2.12. Division Ring $\Rightarrow$ Domain $\Rightarrow$ Prime ring. A matrix ring over an domain is prime. Thus $M_n(\mathbb{Z})$ is a typical example of a prime ring.

2.3 Simple Rings

Definition 2.13. R is said to be *simple* if 0 and R are the only ideals of R. A field is a commutative simple ring with 1.

Let R be a simple ring, and consider R^2, an ideal of R. Then $R^2 = 0$ or $R^2 = R$. Consider the case $R^2 = 0$. So $xy = 0$ for all $x, y \in R$. So any additive subgroup of R is automatically an ideal of R. So the additive group has no subgroups other than 0 and R, hence the additive group of R is cyclic of prime order. Therefore, the structure of such simple rings is completely determined, with trivial multiplication. Therefore, *we will always assume that* simple rings have $R^2 = R$. Therefore, a simple ring is prime. This condition is always the case when R has an identity.

Example 2.14. Let D be a division ring. Then for $n \geq 1$, $M_n(D)$ is a simple Artinian ring.

Proof. D has no right or left ideals other than 0 or D. So by 2.7, $M_n(D)$ is a simple ring. Similarly, if the base ring is right Artinian, then so is the matrix ring, by 1.12. ■

We will see later that the Artin-Wedderburn Theorem gives that all simple Artinian rings are of this form.

2.4 Nil and Nilpotent Subsets

Definition 2.15. Let $S \subset R$, non-empty. S is *nil* if for any $s \in S$, there exists a $k \geq 1$ (dependant on s) such that $s^k = 0$. S is *nilpotent* if there exists a $k \geq 1$ such that $S^k = 0$ / $s_1 \cdots s_k = 0$ for any $s_i \in S$. Clearly nilpotent implies nil. If S is just a single element, then these coincide, and we say the element is nilpotent.

Example 2.16. In $\mathbb{Z}/4\mathbb{Z}$, the ideal $2\mathbb{Z}/4\mathbb{Z}$ is nilpotent.

Lemma 2.17. *Let R be a ring.*

(a) If I, K are nilpotent right ideals of R, then so are $I + K$ and RI.

(b) Any nilpotent right ideal lies inside a nilpotent ideal.

Note that RI is a two sided ideal.

Proof. Suppose that $I^m = K^n = 0$ for $m, n \geq 1$. Consider $(I + K)^{m+n-1}$. A typical term in the expansion is of the form $X_1X_2...X_{m+n-1}$ where each X_i is I or K. There are at least m I's in the term or else at least n K's. $IK \subset I$, $KI \subset K$. So any term is either a subset of I^m or K^n, so is zero. Also $(RI)^m = R(IR)^{m-1}I \subset RI^m = 0$.
For the (b), even if R doesn't have an identity this holds, as $I \subset RI + I$, and $RI + I$ is a two sided ideal. ■

By symmetry the corresponding result holds for nilpotent lefts ideals.

Definition 2.18. The sum of all nilpotent ideals of R is called the *Nilpotent Radical* of R or the *Nil-Radical*. This is usually denoted by $N(R)$.

Note that this is the sum of two sided ideals. However, it follows from 2.17 that $N(R)$ is also equal to the sum of all nilpotent right ideals, and by symmetry is also equal to the sum of all nilpotent left ideals.

Clearly $N(R)$ is a nil ideal, because any element is contained inside a finite sum of ideals. In general however it is *not nilpotent.* For example the ring $\oplus_n \mathbb{Z}/n\mathbb{Z}$ has $N(R) = R$, but no power of $N(R)$ is zero. This shows that just because we have proven the sum of finitely many nilpotent ideals is nilpotent, the general sum need not be. Additionally, $N(R) \subset P$ for all prime ideals P, as any nilpotent ideal to some power is in P, so it is in P.

Example 2.19. If n is a nilpotent element in a commutative ring R, then the ideal generated by n, RnR, is nilpotent.

Example 2.20 (Zassenhaus's Example)**.** Let F be a field, I the open interval $(0, 1)$, and R the vector space with basis $\{x_i \mid i \in I\}$. Define multiplication on R by extending the following product of basis elements:

$$x_i x_j = \begin{cases} x_{i+j} & \text{if } i + j < 1 \\ 0 & \text{if } i + j \geq 1 \end{cases}$$

Every element of R can be written uniquely as $\sum_i a_i x_i$ for $a_i \in F$, all a_i zero except for a finite number. Then R is nil but not nilpotent. For any N, let $i < N^{-1}$. Then $x_i^N \neq 0$. In fact $N(R) = R$.

Remark. For commutative rings we have the binomial theorem, but in general we don't, so that is why in this section there is a lot of divergence between the commutative and non-commutative theories.

Proposition 2.21. *Let R be a commutative ring. Then $N(R)$ equals the set of all nilpotent elements of R.*

Proof. Let X be the set of all nilpotent elements. Then $X \triangleleft R$, and every element of X lies in a nilpotent ideal of R (by 2.19). ∎

Remark. Doesn't hold if R is non-commutative: Let $R = M_2(F)$ for some field F. Then R is a simple ring, so $N(R) = 0$. But

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = 0$$

2.5 Semiprime Ideals

Definition 2.22. Let $K \triangleleft R$. We say K is a semiprime ideal if $[A \triangleleft R,\ A^n \subset K$, for some $n \geq 1] \Rightarrow A \subset K$.

A prime ideal is semiprime. More generally, any intersection of prime ideals is semiprime. R is called *semiprime* if 0 is a semiprime ideal. So R is a semiprime if and only if R has no non-zero nilpotent prime ideals.

Lemma 2.23. *For $K \triangleleft R$, K is semiprime if and only if R/K is a prime ring.*

Proposition 2.24. *R is semiprime $\Leftrightarrow$ $N(R) = 0$ $\Leftrightarrow$ R contains no non-zero nilpotent right ideals $\Leftrightarrow$ R contains no non-zero nilpotent ideals.*

The proof of the following is similar to the proof for the analogous theorem for prime ideals.

Proposition 2.25. *The following are equivalent for $K \lhd R$:*

(a) *K is a semiprime ideal*

(b) *$A^n \subset K$, $A \lhd_r R$, $n \geq 1 \Rightarrow A \subset K$*

(c) *$A^n \subset K$, $A \lhd_l R$, $n \geq 1 \Rightarrow A \subset K$*

(d) *$aRa \subset K$, $a \in R \Rightarrow a \in K$*

2.6 Minimal Prime Ideals in Rings with ACC on Ideals

The following has a very interesting proof.

Proposition 2.26. *Let R be a ring with ACC on ideals. Then every ideal of R contains a product of prime ideals.*

Proof. Suppose not, and let S be the non-empty set of all ideals which don't contain a product of prime ideals. By ACC then S has a maximal element A. By assumption A cannot be prime. So there exist B, C ideals with $BC \subset A$, but neither is a subset of A. So $B + A$ and $C + A$ strictly contain A. By maximality of A in S, both $B + A$ and $C + A$ contain a product of prime ideals. Therefore $(B + A)(C + A)$ does too. But $(B + A)(C + A) \subset BC + A \subset A$. Hence A contains a product of primes, which is a contradiction. ∎

Definition 2.27. A prime ideal P of R is a *minimal prime* if it does not properly contain any other prime ideal.

Theorem 2.28. *Let R be a ring with ACC on ideals. Then*

(a) *Every prime ideal of R contains a minimal prime and R contains only finitely many minimal primes.*

(b) *If $P_1, ..., P_k$ are the minimal primes of R then*

$$N(R) = P_1 \cap ... \cap P_k$$

(c) *$N(R)$ is nilpotent*

At first this looks surprising, as the ACC talks about maximality, but here this gives us minimality. The proof uses the previous result heavily.

Proof. (a) By 2.26, there exists prime ideals $T_1, ..., T_n$ such that $T_1 \cdots T_n = 0$. Let $P_1, ..., P_k$ be minimal in the set $\{T_i\}_i$, so each T_j contains one of the P_q's. Then for any prime ideal $P \supset 0 = T_1 \cdots T_n$, so $P \supset T_i \supset P_j$ for some i, j. Thus $P_1, ..., P_k$ are precisely the minimal primes of R.

(b) Now $P_1 \cap ... \cap P_k \subset T_j$ for all j, $1 \leq j \leq k$. Hence $(P_1 \cap ... \cap P_k)^n = 0$. Thus $P_1 \cap ... \cap P_k \subset N(R)$. But clearly $N(R) \subset P$ for all primes P. So $N(R) = P_1 \cap ... \cap P_k$.

(c) We have shown that $P_1 \cap ... \cap P_k$ is nilpotent.

∎

2.7 Annihilators

Definition 2.29. Let S be a non empty subset of M_R. The *right annihilator* of S is

$$r(S) = \{r \in R \mid Sr = 0\}.$$

Clearly $r(S)$ is a right ideal. When S is a submodule of M_R, then actually $r(S) \lhd R$. Similarly $l(S)$ is defined for a left R-module, is a left ideal, and when S is a submodule then $l(S) \lhd R$. In most applications S is a subset of R, or even both a left and right ideal, so we can consider both the left and right annihilators. A right ideal I is called an *annihilator right ideal* or a *right annihilator* if $I = r(S)$ for some subset $S \subset R$. Similarly for left ideals. Clearly $S \subset rl(S)$, $S \subset lr(S)$, and using this, we have that $rlr(S) = r(S)$, $lrl(S) = l(S)$, see exercise 23c. It follows that *ACC on right annihilators is the same as DCC on left annihilators.*

2.8 Nil Implies Nilpotent Theorems

We often want objects such as $N(R)$ to be nilpotent. In the presence of ACC or DCC fortunately the problem of $N(R)$ typically being only Nil goes away.

Definition 2.30. Let $0 \neq M \lhd_r R$ $[0 \neq M \lhd R]$. Then M is said to be a minimal right ideal [ideal] if $M' \subsetneq M$ and $M' \lhd_r R$ $[M' \lhd R] \Rightarrow M' = 0$. (Minimal with respect to non-zero right ideals [ideals])

Let K be a nil ideal of R, and M a minimal right ideal. Exercise 25 gives that $MK = 0$. In particular, $l(K) \neq 0$ in this case. $(*)$

Theorem 2.31 (Hopkins)**.** *Let R be a ring with DCC on right ideals. Then nil ideals of R are nilpotent.*

Note. We are not assuming the ring is right Artinian, where the identity is assumed.

Proof. Let K be a nil ideal of R. The chain

$$K \supsetneq K^2 \supsetneq K^3$$

stabilises, so for some n, $K^n = K^{n+1}$. Therefore, $l(K^n) = l(K^{n+1})$. Let $\bar{R} = R/l(K^n)$, letting bars denote images. We want to show that $\bar{R} = 0$. Suppose that $\bar{R} \neq 0$. By DCC in $\bar{R}$, $\bar{R}$ contains a minimal right ideal. Also $\bar{K}$ is a nil ideal. By $(*)$, there exists $\bar{x} \in \bar{R} \backslash 0$, such that $\bar{x}\bar{K} = 0$. So in R, $xK \subset l(K^n)$ hence $xK^{n+1} = 0$ and $x \in l(K^{n+1}) = l(K^n)$. Therefore, $\bar{x} = 0$ so $\bar{R} = 0$ and hence $R \subset l(K^n)$. Then $RK^n = 0$, and $K^{n+1} = 0$. ■

Corollary 2.32. *$N(R)$ is a nilpotent ideal in a ring with DCC on right ideals.*

(This gives that Jacobson radical is a nilpotent ideal)

Remark. The idea of this proof comes from a paper by Herstein and Small. In fact we can show that nil one sided ideals are nilpotent in this ring (perhaps later when we do semisimple artinian rings). It is possible to do this right here using the Jacobson radical. (take K as the Jacobson Radical and the proof works).

Lemma 2.33 (Utumi 1963)**.** *Let R be a ring with ACC on right annihilators. If R has a non-zero nil one-sided ideal, then R has a non-zero nilpotent right ideal.*

The proof is very interesting, and only works if you do the left hand side first.

Proof. Suppose that R has a non-zero nil left ideal A. Let $r(a)$ be maximal in the set $\{r(y) \mid y \in A \setminus 0\}$. Claim: $aRa = 0$. Let $t \in R$. If $ta = 0$ then we're done. Otherwise, there is some $k > 1$ such that $(ta)^k = 0$, $(ta)^{k-1} \neq 0$, as $ta \in A$ which is nil. So $ta \in r((ta)^{k-1}) \supset r(a)$. We chose $r(a)$ to be maximal, so $r((ta)^{k-1}) = r(a)$. So $ta \in r(a)$, so $ata = 0$ always. So $aRa = 0$. This gives us $(a)^3 = 0$, where (a) is the right ideal generated by $a \neq 0$.
Now suppose that we have $0 \neq B$ a right ideal of R with B nil. If $B^2 = 0$ then B is a non-zero nilpotent right ideal. Otherwise, there exists $b \in B$, with $Bb \neq 0$. So $Rb \neq 0$. Take $A = Rb$. This is a non-zero nil left ideal, and thus by the first part with this as A, we're done. ■

Lemma 2.34. *Let R be a ring with ACC on ideals. Then R contains a unique maximal nilpotent ideal N and N contains all nilpotent one-sided ideals of R.*

Proof. By 2.28 we have that $N(R)$ is nilpotent. Therefore the set S of nilpotent ideals containing $N(R)$ is non-empty, and so by ACC contains a maximal element N. For any one-sided nilpotent ideal, this is contained in a nilpotent ideal and so in $N(R)$ and thus in N. Furthermore, this is clearly unique. ■

Theorem 2.35 (Lentzki)**.** *Let R be a right Noetherian ring. Then nil one-sided ideals of R are nilpotent.*

Remark. Compare this with Hopkins Theorem.

Proof. By 2.34, R has a unique maximal nilpotent ideal N. Suppose that R has a nil one sided ideal X such that $X \not\subset N$. Then $(X + N)/N$ is a non-zero nil one-sided ideal of the right Noetherian ring R/N. By 2.33, R/N contains a non-zero nilpotent right ideal. Hence R contains a nilpotent right ideal which does not lie inside N[1]. Contradiction to 2.34. Thus $X \subset N$. ■

2.9 Idempotent Elements

Definition 2.36. An element $e \in R$ is *idempotent* if $e = e^2$.

Example 2.37. 0 and 1 are idempotent. In an integral domain with 1, these are the only idempotents. In $\mathbb{Z}/6\mathbb{Z}$, we have that 3 and 4 are idempotent. In $M_2(\mathbb{Z})$,

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \qquad \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

are idempotent.

These are important, as they allow us to split our ring into a direct sum of right ideals.

Lemma 2.38. *Let e be an idempotent in R. Then $R = eR \oplus K$, where $K = \{x - ex \mid x \in R\}$.*

Proof. K is a right ideal. Any $x = (x - ex) + ex$. Also $z \in eR \cap K$, so $z = ea = b - eb$ for some $a, b \in R$. Then $e^2 a = eb - e^2 b = 0$, so $z = ea = 0$. ■

[1] and so doesn't lie in $N(R) \subset N$

Corollary 2.39 (Peirce Decomposition)**.** *Let R be a ring with 1 and e an idempotent in R. Then $R = eR \oplus (1-e)R$.*

Proof. $K = (1-e)R$, for K as above. ■

Proposition 2.40. *Let R be a ring with 1. Suppose that $R = I_1 \oplus ... \oplus I_n$ a direct sum of right ideals. Then we can write $1 = e_1 + e_2 + ... + e_n$ uniquely for $e_i \in I_i$. Then the e_j have the following properties:*

1. *$e_i^2 = e_i$ for all $1 \leq i \leq n$.*
2. *$e_i e_j = 0$ for $i \neq j$*
3. *$I_j = e_j R$*
4. *$R = Re_1 \oplus ... \oplus Re_n$ is a direct sum of left ideals.*

Proof. For each j we have

$$e_j = 1e_j = e_1 e_j + ... + e_j^2 + ... + e_n e_j$$

$$e_j - e_j^2 = e_1 e_j + ... + e_{j-1}e_j + e_{j+1}e_j + ... + e_n e_j \in I_j \cap \left(\sum_{s \neq j} I_s \right) = 0$$

So $e_j = e_j^2$. As the sum is direct, $e_i e_j = 0$ for $i \neq j$. Clearly $e_j R \subset I_j$, and if $a \in I_j$, $a = 1a = e_1 a + ... + e_n a$, and so $a - e_j a = e_1 a + ... + e_n a \in I_j \cap \left(\sum_{s \neq j} I_s \right) = 0$, so $a = e_j a \in e_j R$. Finally, the sum of the left ideals is clearly R, and is direct, as given $r_i e_i = \sum_{j \neq i} r_j e_j$, then multiplying on the right by e_j gives that $r_i e_i = r_i e_i^2 = 0$. ■

Example 2.41. In $M_n(\mathbb{Z})$, let $e_j := \text{diag}(0, ..., 1, ..., 0)$. Remember left ideals are columns, and right are rows.

2.10 Ideals and Idempotents

Definition 2.42. For a ring R, let the centre of R be

$$C(R) = \{x \in R \mid xr = rx \; \forall r \in R\}.$$

This is a subring of R, but in general not an ideal.

Example 2.43. In $R = M_n(S)$, where S is a commutative ring, $C(R)$ is the set of diagonal matrices.

Lemma 2.44. *Let $I \lhd R$, with $I = eR = Rf$ where e, f are idempotent. Then*

1. *$e = f$*
2. *e is the identity of the ring I*
3. *$e \in C(R)$*

Proof. 1. $e = e^2 \in I$. $e = af$, so $e = af = af^2 = af(f) = ef$. Similarly, $f = e(eb) = ef$. So $e = f$.

2. For $x \in I$, so $x = ea = be$, so $ex = x = xe$ for all $x \in I$.

3. For $x \in R$, $ex, xe \in I$, so as e is the identity, $ex = exe = xe$, so $e \in C(R)$.

■

By both the above we have the following.

Lemma 2.45. *Let R be a ring with 1. Suppose that $R = A_1 \oplus ... \oplus A_k$ a direct sum of* ideals*. Let $1 = e_1 + ... + e_k$. Then*

1. *$e_j \in C(R)$,*

2. *$e_j e_i = e_j \delta_{ij}$,*

3. *$A_j = e_j R = Re_j$,*

4. *e_j is the identity of the ring A_j.*

Note that in the above, viewing A_j as a ring with identity in its own right, we can also consider $R = A_1 \oplus ... \oplus A_k$ as a direct sum of rings with identity.

Example 2.46. Let R be a ring with 1, $A \triangleleft R$ and $e = e^2 \in A$. This does *not* imply that $A = Re$. Take

$$R = \begin{bmatrix} \mathbb{Z} & \mathbb{Z} \\ 0 & \mathbb{Z} \end{bmatrix}, \; A = \begin{bmatrix} \mathbb{Z} & \mathbb{Z} \\ 0 & 0 \end{bmatrix}, \text{ and } e = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

Then $A = eR \triangleleft R$, $e = e^2$ but $Re \subsetneq eR = A$.

However, in an important case for us, it does work.

Proposition 2.47. *Let A be an ideal of a semiprime ring R, with $A = eR$, $e = e^2 \in A$. Then $A = Re$.*

Proof. Let $K = \{x - xe \mid x \in A\}$. Then K is a left ideal of R, since A is. We have $Ke = 0$, so $KeR = 0$. Hence $K^2 = 0$, as $K \subset eR = A$. Therefore, $K = 0$, as R is semiprime. Thus, $x = xe$ for all $x \in A$, so $A \subset Re$. Also $Re \subset A$ since $e \in A$ and $A \triangleleft_l R$, so $A = eR = Re$. ■

Lemma 2.48. *Let A be an ideal of a ring R such that $A = eR = Re$ with $e = e^2 \in A$. Viewing A as a ring in it's own right, then $K \triangleleft_r A \, [K \triangleleft_l A] \Rightarrow K \triangleleft_r R \, [K \triangleleft_l R]$*

And so this is also true for two sided ideals. The conclusion of the lemma is definitely not the case in general.

Proof. Let $k \in K$ and $r \in R$. We have to use e to show that $rk \in K$. Now $kr = (ke)r$ since e is the identity of the ring A. $(ke)r = k(er) \in K$, as $er \in A$, and $K \triangleleft_r A$. Similarly on the left. ■

Corollary 2.49. *Let A be an ideal of a ring R such that $A = eR = Re$ with $e = e^2 \in A$. Then:*

1. *R is a right Artinian ring $\Rightarrow$ A is a right Artinian ring.*

2. *A is a minimal ideal of $R \Rightarrow A$ is a simple ring.*

3 Artinian Rings

We will use Zorn's lemma several times, which is equivalent to the axiom of choice.

Definition 3.1. A partially ordered set is $(S, \leq)$, where S is a non empty set, and $\leq$ is a binary operation defined for certain pairs of elements, satisfying:

1. $a \leq a$
2. $a \leq b, b \leq c \Rightarrow a \leq c$
3. $a \leq b, b \leq a \Rightarrow a = b$

Let S be a partially ordered set. A non-empty subset T is said to be totally ordered if for every pair $a, b \in T$, either $a \leq b$ or $b \leq a$. An element $x \in S$ is called *maximal* if $x \leq y \Rightarrow x = y$. Let T be a totally ordered subset of S. T has an upper bound (in S) if there exists $c \in S$ such that $x \leq c$ for all $x \in T$.

Theorem 3.2 (Zorn's Lemma)**.** *Let S be a partially ordered set such that every totally ordered subset of S has an upper bound in S. Then S contains a maximal element.*

This maximal element need not be unique.

Definition 3.3. Let M be a proper right ideal of R. Then M is a *maximal right ideal* if it is maximal among all proper right ideals.

Similarly we define maximality for left and two-sided ideals.

Proposition 3.4. *Let R be a ring with 1. Let $I \triangleleft_r R$ $[I \triangleleft R]$ such that $I \neq R$. Then there exists a maximal right ideal [ideal] M of R such that $I \subset M$.*

Note that the identity assumption is crucial here.

Proof for right ideals. Let S be the set of proper right ideals of R containing I, partially ordered by inclusion. $S \neq \emptyset$ as $I \in S$. Let $\{T_\alpha\}_\alpha$ be a totally ordered subset of S. Let $T := \cup_\alpha T_\alpha$. Then T is a right ideal of R (the union is not typically a right ideal). Additionally, $T \supset I$. We just need to check that $T \neq R$. This is not the case, as $T = R \Rightarrow 1 \in T \Rightarrow 1 \in T_\alpha$ for some α. T is our required maximal right ideal. ■

Remark. This is false if R does not have 1: take any Abelian group without maximal subgroups, such as $(\mathbb{Q}, +)$, with trivial multiplication ($xy = 0$ for all $x, y \in R$).

Corollary 3.5. *Any ring with* 1 *contains a maximal right ideal [ideal].*

Proof. Let $I = 0$ in above. ■

3.1 Irreducible Modules

Definition 3.6. A right R module M is said to be *irreducible* if $MR \neq 0$ and M contains no submodules other than 0 and M.

Note. Some use *simple* for this term, but we reserve this for simple rings.
If R has 1, then the first condition is the $M \neq 0$, and minimal right ideals of R are exactly the irreducible submodules of R_R.

Example 3.7. (a) If p is prime, then $\mathbb{Z}/p\mathbb{Z}$ is an irreducible $\mathbb{Z}$ module (and these are all irreducible $\mathbb{Z}$ modules).

(b) Every ring with 1 has an irreducible module, as R contains a maximal right ideal M. So R/M is an irreducible right R module.

(c) Let V be a vector space. Then irreducible submodules are exactly 1-dimensional subspaces. Additionally, V is the direct sum of irreducible submodules, as any V has a basis, see exercise 26.

(d) This is not true in general, $\mathbb{Z}/4\mathbb{Z}$ is not even the sum of it's subgroups, as only proper non-trivial subgroup is $2\mathbb{Z}/4\mathbb{Z}$. $\mathbb{Z}/6\mathbb{Z}$ is however, and furthermore the sum is direct.

Lemma 3.8. *Let M, K be right R modules, and $\theta : M \to K$ a non-zero R module homomorphism.*

1. *M irreducible $\Rightarrow \theta$ is a monomorphism.*
2. *K irreducible $\Rightarrow \theta$ is a epimorphism.*
3. *Both M,K irreducible $\Rightarrow \theta$ is a isomorphism.*

If $\theta : M \to M$ is an isomorphism, then the inverse $\theta^{-1} : M \to M$ is an isomorphism, and $\theta\theta^{-1} = \mathbb{1}_M = \theta^{-1}\theta$.

Lemma 3.9 (Schur's Lemma)**.** *If M is irreducible, then* $\mathrm{End}_R(M)$ *is a division ring.*

We now investigate irreducible modules.

Definition 3.10. A module M_R is *completely reducible* (CR) if M is expressible as a sum (not necessarily direct) of irreducible submodules.

Note. Again, some use *semisimple* for this term, but we reserve this for semisimple rings. We will show we can always throw away redundant submodules to make this direct!

Example 3.11. $\mathbb{Z}/6\mathbb{Z}$ is CR as a $\mathbb{Z}$ module.

Lemma 3.12. *Let M be a right R-module such that*

$$M = \sum_{\lambda \in \Lambda} M_\lambda$$

where each λ is a irreducible submodule. Let K be a submodule of M. Then there exists a subset $\Omega \subset \Lambda$ such that

$$M = K \oplus \left(\bigoplus_{\omega \in \Omega} M_\omega \right)$$

This heavily uses Zorn's Lemma.

Proof. Consider S, the set of submodules $K + \sum_{\alpha \in \mathcal{A}} M_\alpha$ such that this sum is direct, where $\mathcal{A}$ is a subset of Λ. Now for any chain of elements of S, $Y_i \subset Y_{i+1}$, $Y_i = K \oplus \bigoplus_{\alpha \in \mathcal{A}_i} M_\alpha$. We claim an upper bound for this chain is $Y := K + \sum_{\alpha \in \mathcal{A}} M_\alpha$, where $\mathcal{A} = \cup_i \mathcal{A}_i$. To see this, note that as $Y_i \subset Y_{i+1}$, then $\sum_{\alpha \in \mathcal{A}_i} M_\alpha \subset \sum_{\alpha \in \mathcal{A}_{i+1}} M_\alpha$, and so $\mathcal{A}_i \subset \mathcal{A}_{i+1}$, because any M_β for $\beta \in \mathcal{A}_i$, has an inclusion homomorphism into $\sum_{\alpha \in \mathcal{A}_{i+1}} M_\alpha$, and so by Schur's lemma is isomorphic to one of the summands. Using this, it is easily shown that the sum for Y is direct and so $Y \in S$. Therefore, by Zorn's Lemma we obtain a maximal element in S, $X = K \oplus \left(\bigoplus_{\omega\in\Omega} M_\omega\right)$. We claim $X = M$. Let $\lambda \in \Lambda$, we now use the classic trick. Either $X \cap M_\lambda = 0$, or $X \cap M_\lambda = M_\lambda$. The first possibility cannot happen, as we get a direct sum $X \oplus M_\lambda$ contradicting maximality. Then as $M = \sum_{\lambda\in\Lambda} M_\lambda$, $X = M$. ■

Theorem 3.13. *Let $M_R \neq 0$. TFAE:*

(i) M_R is completely reducible

(ii) M_R is a direct sum of irreducible submodules

(iii) $mR = 0, m \in M \Rightarrow m = 0$, and every submodule of M is a direct summand of M.

Proof. $(i) \Rightarrow (ii)$: Take $K = 0$ in above.
$(ii) \Rightarrow (iii)$: Suppose that $mR = 0$ for $m \in M$. Let $M = \oplus M_\lambda$, with each irreducible. Write $m = m_1 + ... + m_k$, with each $m_j \in M_{\lambda_j}$. For all $r \in R$, $0 = mr = m_1 r + ... + m_k r$, so as a direct sum, $m_j r = 0$ for all j. Define $K_j = \{x \in M_{\lambda_j} \mid xR = 0\}$, a submodule of M_{λ_j}. M_{λ_j} is irreducible, so $K_j = 0$ or $K_j = M_{\lambda_j}$. But $M_{\lambda_j} R \neq 0$, so $K_j = 0$, as $M_{\lambda_j} \neq K_j$. Additionally all submodules of M must be a direct summand, as if they contain any non-zero element of some M_λ, then they contain M_λ.
$(iii) \Rightarrow (i)$: Note that for any non-zero submodule N of M, the hypothesis is still true: if $nR = 0$, $n \in N$, then $n = 0$, and every submodule of N is a direct summand of N, because by the Dedekind/Modular law, if N' is a submodule of N, then $M = N' \oplus K$ for some K, so $N = N \cap (N' \oplus K) = N' \oplus N \cap K$. First we show that M contains an irreducible submodule.
Let $0 \neq y \in M$. Let $S = \{K \subset M \text{ submodule} \mid y \notin K\}$. Partially ordering this set by inclusion, by Zorn's lemma there is a maximal element A, with $A \neq M$. There is a submodule $B \neq 0$, such that $M = A \oplus B$. We claim that B is irreducible. Suppose that B contains a submodule B_1 such that $0 \subsetneq B_1 \subsetneq B$. Then as the hypothesis is still true for B, $B = B_1 \oplus B_2$. Now $y \in A \oplus B_1$, so $y \in A \oplus B_2$ by maximality of A, thus $y \in (A \oplus B_1) \cap (A \oplus B_2) = A$, but this is a contradiction. So B is irreducible. Let K be the sum of all irreducible submodules of M, which exists as this sum is non-empty. If $K \neq M$, then there exists some non-zero submodule L such that $M = K \oplus L$. As above, L contains an irreducible submodule, contradiction. (K contains all irreducible submodules of M, and $K \cap L = 0$). So $M = K$. ■

Remark. The first hypothesis of (iii) $(mR = 0 \Rightarrow m = 0)$ holds automatically if R is unital and M_R is a unital module.

3.2 Minimal Right ideals and Idempotents

Lemma 3.14. *Let M be a minimal right ideal of a ring R. Then either:*

1. *$M^2 = 0$, or*
2. *$M = eR$ where $e = e^2 \in M \setminus 0$.*

Proof. Suppose the $M^2 \neq 0$. Then there exists $a \in M$ such that $aM \neq 0$. Now $aM \lhd_r R$ (as $M \lhd_r R$) and $aM \subset M$ since $a \in M$. Then, $M = aM$. Since $a \in M$, there exists some $e \in M$ with $a = ae$. In particular, $a \neq 0 \Rightarrow e \neq 0$. Also, $a = ae = ae(e) = ae^2$

$\Rightarrow a(e - e^2) = 0 \Rightarrow e - e^2 \in M \cap r(a)$. Now $M \cap r(a) \triangleleft_r R$, and $M \cap r(a) \subset M$ implies $M \cap r(a) = M$ or $M \cap r(a) = 0$. But if $M \cap r(a) = M$, then $M \subset r(a)$, so $aM = 0$, contradiction. ■

Note. In a semi-prime ring, any minimal right ideal is generated by an idempotent, as the first case cannot occur.

Example 3.15. Let

$$R = \begin{bmatrix} \mathbb{Q} & \mathbb{Q} \\ 0 & \mathbb{Q} \end{bmatrix}, M_1 = \begin{bmatrix} 0 & \mathbb{Q} \\ 0 & 0 \end{bmatrix}, \text{ and } M_2 = \begin{bmatrix} 0 & 0 \\ 0 & \mathbb{Q} \end{bmatrix}.$$

Note that M_1 is the nil radical of R. Both are minimal right ideals by definition. Here $M_1^2 = 0$, $M_2 = eR$ where

$$e = e^2 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

Furthermore, $M_1 \cong \mathbb{Q} \cong M_2$ as right R-modules via the obvious map. So we have isomorphic R-modules, but where exactly one is nilpotent, exactly one is idempotently generated. However ring isomorphism preserves the property of being generated by idempotents.

3.3 The Socle

We assume in this section that modules M_R satisfy $mR = 0, m \in M \Rightarrow m = 0$. In particular this is the case when R has an identity, and is true for R_R when R is semiprime ($l(R) = 0$, as we always have $l(R)^2 = 0$).

Definition 3.16. The *socle*[2] of M_R is $E(M_R) =$ the sum of all irreducible modules, or zero if there are none. $E(R) = E(R_R)$ is the right socle of R and so by the assumption on M_R above, $E(R)$ is the sum of all minimal right ideals of R when $E(R) \neq 0$. Similarly, $E'(R) = E({}_RR)$ is the left socle of R, and when non-zero is the sum of all minimal left ideals of R.

Note. In general the left socle is different from the right. Of course, a right Artinian ring always has a non-zero right socle, as DCC is equivalent to the minimum condition.

Proposition 3.17. *(a)* $E(R) \triangleleft R$

(b) $E'(R) \triangleleft R$

It is not immediately obvious why $E(R)$ should form a left R-module.

Proof. Assume that $E \neq 0$. Clearly, $E \triangleleft_r R$. Let M be a minimal right ideal of R, with $x \in R$. Then the map $\theta : M \to xM$ given by left multiplication by x shows that either $xM = 0$ or $xM = M$, in which case xM is also a minimal right ideal. It follows that E is then also a left ideal. Similarly for (b). ■

Example 3.18. Check that the above example has $E(R) \neq E'(R)$, using exercise 36. So the left and right socles can differ.

[2]Meaning base. For groups this is defined as the subgroup generated by the minimal normal subgroups.

3.4 Semisimple Artinian Rings

Definition 3.19. A semiprime ring with *DCC* on right ideals is called a *semisimple Artinian ring.*

Remark. This is a weaker hypothesis than the ring being Artinian and a finite direct sum of simple rings, as simple rings are prime and so a finite direct sum is semiprime. However, we will show it is an equivalent condition - it is true that semisimple Artinian ring is both semisimple and Artinian. We call a ring Artinian if it has DCC on the right and the left, and has an identity. We will show (3.25) that a semiprime ring with DCC on right ideals automatically implies DCC on left ideals too. For example this follows from the Artin Weddurburn theorem. We can also prove that semisimple Artinian rings have an identity - this is one of the reasons we don't assume our rings have an identity to begin with! Therefore, as we will also show that R semiprime with DCC on right ideals implies that R is a finite direct sum of simple rings, it will turn out that such rings are both semisimple and Artinian.

Lemma 3.20. *Let R be a ring with DCC on right ideals, such that $l(R) = 0$. Suppose that for some $c \in R$, $r(c) = 0$. Then R contains an identity, and further c is a unit of R.*

Remark. We cannot do without the assumption of the existence of c. See exercise 15.

Proof. Consider the chain of right ideals

$$cR \subset c^2R \subset c^3R \subset ....$$

So for some n, $c^nR = c^{n+1}R$. Then there exists an $e \in R$ with $c^nc = c^{n+1}e$. We claim e is an identity. For all $x \in R$, $c^{n+1}x = c^{n+1}ex$, so $x = ex$, since $r(c) = 0$. So e is a left identity of R. Now we use that $l(R) = 0$. Consider $x - xe$ for $x \in R$. We want to show that this is zero. For all $y \in R$, $(x - xe)y = xy - xe(y) = xy - x(ey) = 0$. So $(x - xe)R = 0$, so $x = xe$, as $l(R) = 0$. Now as $c^nR = c^{n+1}R$, there exists $d \in R$ such that $c^ne = c^{n+1}d$, so $cd = e$, and d is a right inverse for c. Also $r(d) = 0$, so by the same argument, there exists $b \in R$ such that $db = e$. Now $b = eb = (cd)b = c(db) = ce = c$. Hence $cd = dc = e$ and c is a unit of R. ■

Theorem 3.21. *Let R be a semisimple Artinian ring. Then*

1. *R has an identity*
2. *$R = I_1 \oplus ... \oplus I_n$, where each I_j is a minimal right ideal of R.*

Proof. By DCC, each non-zero right ideal of R contains a minimal right ideal, and by 3.14, this is generated by an idempotent. We have that $l(R) = 0$, as R is semiprime. By the above, to show that R has an identity, it is enough to prove existence of some $c \in R$ with $r(c) = 0$. Choose an idempotent $f_1 \in R$ such that f_1R is minimal. If $r(f_1) = 0$, then we are done. Otherwise, considering the right ideals contained in $r(f_1)$, use the DCC to choose an idempotent $f_2 \in r(f_1)$ such that f_2R is minimal. So $r(f_1) \supsetneq r(f_1) \cap r(f_2)$, as $f_2 \in r(f_1)$ and $f_2 \notin r(f_2)$. In this way we obtain a strictly descending chain of ideals

$$r(f_1) \supsetneq r(f_1) \cap r(f_2) \supsetneq r(f_1) \cap r(f_2) \cap r(f_3) \supsetneq ....$$

As R has DCC on right ideals, this stabilises. So we obtain idempotents $f_1, ..., f_n \in R$ such that $r(f_1) \cap ... \cap r(f_n) = 0$. Let $c = f_1 + ... + f_n$. Now if $cx = 0$ for $x \in R$, then

$f_1x + ... + f_nx = 0$, so $f_1^2x + f_1f_2x + ... + f_1f_nx = 0$, thus $f_1x = 0$ and $f_2x + ... + f_nx = 0$, hence $f_2^2x + f_2f_3x + ... + f_2f_nx = 0$, so $f_2x = 0$, and continuing in this fashion, $f_ix = 0$ for all i. Therefore, $x \in r(f_1) \cap ... \cap r(f_n) = 0$. So $r(c) = 0$.

For the second part, let $I_j = f_jR$. As the f_i are idempotent, $f_1R + ... + f_nR$ is a direct sum. We have $c \in I_1 \oplus ... \oplus I_n$, and c is a unit by the above, so $R = I_1 \oplus ... \oplus I_n$. ■

Corollary 3.22. *Let R be a semisimple Artinian Ring. Then there exists idempotents $e_1, ..., e_n$ such that $1 = e_1 + ... + e_n$, and $R = e_1R \oplus ... \oplus e_nR$.*

Proof. Follows using 2.40. ■

Proposition 3.23. *The following are equivalent for a ring R.*

(a) R is semisimple Artinian

(b) R has an identity, and R_R is completely reducible.

We will use this extensively.

Proof. We have that (a) $\Rightarrow$ (b). For the other direction, we have $R = \bigoplus_\lambda I_\lambda$, where each I_λ is an irreducible submodule of R. Then we can write $1 = x_1 + ... + x_k$. For any $r \in R$, $r = rx_1 + ... + rx_k \in I_{\lambda_1} \oplus ... \oplus I_{\lambda_k}$. So $R = \bigoplus_{i=1}^k I_{\lambda_k}$, so the sum is finite. Then by 1.10 R has DCC on right ideals. Let $N = N(R)$, the nilpotent radical. By 3.13, then there exists a right ideal K of R such that $R = N \oplus K$. So $1 = n + k$. Now for some t, $(1-k)^t = n^t = 0$ as n is nilpotent. So $1 = tk - ... \pm k^t \in K$. So $K = R$. So $N = 0$. Then R is semiprime. ■

Proposition 3.24. *Let $I \triangleleft_r R$, where R is semisimple Artinian. Then $I = eR$, for some $e = e^2 \in I$.*

Proof. By the above, R_R is completely reducible and R has 1. So by 3.13, I is a direct summand of R. Hence by 2.40, there exists some $e = e^2 \in I$ such that $I = eR$. ■

So we have that R semisimple Artinian (R is semiprime and R has DCC on right ideals) is equivalent to R having an identity and R_R being completely reducible. This is all very "right handed", and we now seek to rectify this.

Proposition 3.25. *A semisimple Artinian ring is left right symmetric: a semiprime ring with DCC on right ideals also has DCC on left ideals.*

Proof. By 3.23, $R = e_1R \oplus ... \oplus e_nR$, where $1 = e_1 + ... + e_n$. $e_i^2 = e_i$, $e_ie_j = 0$ for $i \neq j$, and each e_iR is a minimal right ideal. By exercise 22, each Re_i is a minimal left ideal, so we have $R = Re_1 \oplus ... \oplus Re_n$, by 2.40. So ${}_RR$ is Artinian by 1.10. ■

3.5 Ideals in Semisimple Artinian Rings

Lemma 3.26. *Let R be a semisimple Artinian ring, $A \triangleleft R$. Then there exists central idempotent $e \in A$ such that $A = eR = Re$.*

Proof. We have $A = eR$ and $e = e^2$, by 3.24. So $A = eR = Re$, $e \in C(R)$, by 2.45. ■

Corollary 3.27. *If R, A are as in the above, the there is an ideal B with $R = A \oplus B$.*

See exercise 8 for failure in general - A two sided does not imply B is.

Proof. By the above lemma, $A = eR$ with $e = e^2 \in C(R)$. By Peirce decomposition 2.39, we have that $R = eR \oplus (1-e)R$. Now $1-e \in C(R)$ since $e \in C(R)$. So $B := (1-e)R \triangleleft R$. ■

Theorem 3.28. *Let R be an semisimple Artinian ring. Then R is expressible as a finite direct sum of minimal ideals $R = S_1 \oplus ... \oplus S_m$. The S_i are the only minimal ideals of R.*

Generally, R can be a direct sum of right ideals in lots of different ways. However for two sided ideals this is unique!

Proof. Let S_1 be a minimal ideal of R, which exists by DCC. By the above corollary, there is an ideal T_1 such that $R = S_1 \oplus T_1$. If $T_1 \neq 0$, then T_1 contains a minimal ideal of R, call this S_2. As above, $R = S_2 \oplus K$ for some ideal K of R. Now we use the Dedekind modular law:

$$T_1 = T_1 \cap R = T_1 \cap (S_2 \oplus K) = S_2 \oplus T_1 \cap K = S_2 \oplus T_2$$

where $T_2 = T_1 \cap K$. We have $R = S_1 \oplus T_1 = S_1 \oplus S_2 \oplus T_2$. If $T_2 \neq 0$ proceed similarly. We obtain

$$T_1 \supsetneq T_2 \supsetneq ...$$

By DCC this must stop, so eventually some $T_m = 0$. At this stage, $R = S_1 \oplus ... \oplus S_m$. To see these are the only minimal ideals of R, let S be a minimal ideal of R. Then $SR \neq 0$, as R has 1, so $SS_j \neq 0$ for some j. This is an ideal of R, and lies inside both S_j and S. Therefore, $S = SS_j = S_j$. ■

Note that the uniqueness proof doesn't work for one sided ideals.

3.6 The Artin-Wedderburn Theorem

Our proofs here will use right handed conditions only, so when we are done we can give an alternative proof of the symmetry of definition of Semisimple Artinian rings.

Theorem 3.29. *A semisimple Artinian Ring R, is a unique finite direct sum of simple right Artinian rings.*

Proof. By the above $R = S_1 \oplus ... \oplus S_m$, is a unique direct sum of minimal ideals. By 2.49, each S_i is a simple right Artinian ring. ■

Recall that if $A_R \cong B_R$ as right modules, then $\mathrm{End}_R(A) \cong \mathrm{End}_R(B)$ as rings. Given X_R, let $X^{(n)}$ denote $X \oplus ... \oplus X$, n times.

Theorem 3.30 (Artin-Wedderburn Theorem)**.** *R is a semisimple Artinian ring if and only if $R = S_1 \oplus ... \oplus S_m$ where $S_i \cong M_{n_i}(D_i)$, $n_i \geq 1$ and D_i's division rings.*

Note that each S_i is a both a minimal ideal and a ring with identity in it's own right.

Proof. "$\Rightarrow$": $R = S_1 \oplus ... \oplus S_m$ as rings, where each S_i is simple and right Artinian. It is enough then to show that if S is a simple right Artinian ring then $S \cong M_n(D)$ as rings for some n and some division ring D. As such S are prime (as simple) so semiprime, and have DCC on right ideals, S is semiprime Artinian, therefore by 3.21,

$S = I_1 \oplus ... \oplus I_n$ is a direct sum of minimal right ideals. By exercise 32, $I_j \cong I_k$ as right S-modules. Therefore, as right S modules, $S_S \cong I_1^{(n)}$. Now as rings, by 0.5, $S \cong \mathrm{End}_S(S_S) \cong \mathrm{End}_S(I_1^{(n)}) \cong M_n(\mathrm{End}_S(I_1)) = M_n(D)$, where $D = \mathrm{End}_S(I_1)$ is a division ring by Schur's Lemma.
"$\Leftarrow$": Each S_i is a simple right Artinian ring by 2.14, so each S_i as a right R-module is right Artinian. So as the sum of Artinian is Artinian, so R_R is Artinian, i.e. R is a right Artinian ring. Thus R is semisimple Artinian. ■

Corollary 3.31. *A semisimple Artinain ring is left right symmetric.*

Proof. The "$\Rightarrow$" part of the above proof used only DCC on right ideals. Now $M_{n_1}(D_1) \oplus ... \oplus M_{n_m}(D_m)$ is also left Artinian. ■

That is the second proof of the above. We will not actually use the Artin-Weddurburn theorem itself in any further sections, but we will use the theory that got us here. However, it's statement is important to keep in mind.

3.7 Modules Over Semisimple Artinian Rings

Theorem 3.32. *Let R be a simplesimple Artinian ring. M_R a non-zero unital R module. Then M_R is completely reducible.*

Proof. $R = I_1 \oplus ... \oplus I_n$, a direct sum of minimal right ideals, by 3.21. Let $m \in M$. Then $m = m1 \in mI_1 + ... + mI_n$. Each mI_j is zero or irreducible. So each $m \in M$ lies in a sum of irreducible submodules of M, and so we can write M_R as the sum of irreducible modules, hence M_R is completely reducible. ■

Corollary 3.33. *Let R be a ring with 1. Then R is semisimple Artinian if and only if every unital right R module is completely reducible. (if and only if every left R module is completely reducible, by the symmetry.)*

Proof. "$\Rightarrow$": By above. "$\Leftarrow$": In particular, R_R is completely reducible, and as R has 1, by 3.23 the result follows. ■

Lemma 3.34. *Let R be a right Artinian ring, and $N = N(R)$. Then the ring R/N is semisimple Artinian.*

Proof. By Hopkins Theorem 2.31, N is nilpotent. Then it follows that the ring R/N is semiprime, and has DCC on right ideals (because all quotients do). ■

The following is (also) called Hopkin's Theorem.

Theorem 3.35. *A right Artinian ring is right Noetherian.*

Proof. Let $N = N(R)$. By above, R/N is a semisimple Artinian ring. By 2.32, there exists a smallest integer $k \geq 1$ such that $N^k = 0$. Consider the chain

$$R \supsetneq N \supsetneq N^2 \supsetneq ... \supsetneq N^k = 0$$

Let $N^0 = R$. For $0 \leq j \leq j-1$, each N^j/N^{j+1} is a unital right R/N-module, so by 3.32, N^j/N^{j+1} is completely reducible. As N^j/N^{j+1} has DCC as a right module (for either ring), it must be a *finite* direct sum of irreducible submodules. So by 1.10, each

N^j/N^{j+1} is an Noetherian right module, for $0 \leq j \leq j-1$. Then in particular, N^{k-1} and N^{k-2}/N^{k-1} are Noetherian right modules. Then by 1.9, N^{k-2} has ACC on right modules. Proceeding this way we obtain that R_R has ACC. Thus R is a right Noetherian ring. ■

Caution: This does not apply to modules!

Corollary 3.36. *Every finitely generated module over a right Artinian ring has a composition series.*

Proof. Let M_R be a finitely generated module over a right Artinian ring R. By the above, R is right Noetherian. So as R has a unit, by 1.11 M has both ACC and DCC on submodules. So by 1.19, M has a composition series. ■

4 Quotient Rings

From 1900-1920 it was known that R semiprime and DCC implies Artin-Wedderburn, so you know exactly the structure of R. Hopkins proved that DCC implies ACC. In the 1950's, the question was what can we draw from the weaker hypothesis of R semiprime, and ACC. People thought these assumptions were too general to say anything meaningful. This leads us onto Goldie's theorems, and how to generalise fields of fractions to non-commutative rings.

Definition 4.1. An element c of a ring is *right regular* if $r(c) = 0$, *left regular* if $l(c) = 0$, and *regular* if both. A ring Q is called a quotient ring if Q has 1, and every *regular* element of Q is a unit.

By 3.20, every right Artinian ring is a quotient ring. In particular, a division ring is a quotient ring.

Definition 4.2. Let Q be a ring with 1 and R a subring of Q. The ring Q is said to be a *right quotient ring* of R, if:

1. Every regular element of R is a unit of Q.
2. Every element of Q is expressible as ac^{-1}, where $a, c \in R$ and c is regular.

A left quotient ring is defined analogously. It is not obvious that these exist or are unique when they do.

Example 4.3. (a) Any field of fractions of an integral domain is a right quotient ring for the integral domain.

(b) Consider $\mathbb{Z} \subset 2\mathbb{Z} \subset \mathbb{Z}_{(p)} = \{\frac{a}{c} \mid a, c \in \mathbb{Z}, p \nmid c, p \text{ prime}\} \subset \mathbb{Q}$. Then $\mathbb{Q}$ is a right quotient ring of $\mathbb{Z}$ and so of all those in between (as is true in general). Note that $2\mathbb{Z}$ is not unital, but we don't require a subring to have a unit even if the bigger ring does.

(c) $M_n(\mathbb{Q})$ is a left (and right) quotient ring of $M_n(\mathbb{Z})$. The regular elements are those with non-zero determinant, as for a regular A, we can find a matrix B (the adjoint) with $AB = BA = dI_n$, for some $d = \det(A) \in \mathbb{Z} \setminus 0$.

Note that if Q is a right quotient ring of R, then Q is a quotient ring. If R has a right quotient ring Q, then we say that R has a *right order* on Q. The following is the analogue of a common denominator.

Proposition 4.4. *Suppose that R has a right quotient ring Q. Let $c_1, ..., c_n$ be regular elements of R. Then there exists $r_1, ..., r_n, c \in R$ with c regular such that $c_i^{-1} = r_i c^{-1}$ for all i.*

Proof. By induction on n. For $n = 1$, let $r_1 = c_1$, $c = c_1^2$. Now assume that we have obtained $t_1, ..., t_{n-1}, d \in R$, with d regular, and $t_i^{-1} = t_i d^{-1}$. Consider $d^{-1} c_n$. As Q is a right quotient ring for R, we have $d^{-1} c_n = r r_n^{-1}$ for some r, r_n with r_n regular. We have $c_n r_n = dr = c$ say, so c is regular in R. Now $c_i^{-1} = t_1 d^{-1} = t_1(rc^{-1}) = r_i c^{-1}$, where $r_i = t_i r \in R$ for all $i < n$. Also $c_n^{-1} = r_n c_n^{-1}$. ■

Proposition 4.5. *Let R be a ring with a right quotient ring Q.*

(a) If $I \triangleleft_r R$, then $IQ \triangleleft_r Q$, and every element of IQ is expressible as xc^{-1} with $x \in I$, and c regular in R.

(b) If $K \triangleleft_r Q$, then $K \cap R \triangleleft_r R$, and $(K \cap R)Q = K$.

Proof. (a) Clearly $IQ \triangleleft_r Q$. IQ is finite sums of products, so there is still some work to do. A typical element of IQ is

$$\alpha = t_1 q_1 + ... + t_k q_k$$

with $t_i \in I$ and $q_i \in Q$. So

$$\alpha = t_1 a_1 c_1^{-1} + ... + t_k a_k c_k^{-1}$$

with $a_i, c_i \in R$, c_i regular. By the above, we can find $r_1, ..., r_k, c \in R$ with c regular, such that $c_j^{-1} = r_j c^{-1}$ (common denominator c). So

$$\alpha = (t_1 a_1 r_1 + ... + t_k a_k r_k) c^{-1}.$$

(b) Clearly $K \cap R \triangleleft_r R$. Clearly $(K \cap R)Q \subset K$, and we can write any $k \in K$ as $k = ac^{-1}$, $a, c \in R$, and thus $k \in (K \cap R)Q$, as $a = (ac^{-1})c \in K$, and $c^{-1} \in Q$.

■

Corollary 4.6. *Suppose that R has a right quotient ring Q. If R is right Noetherian, then Q is right Noetherian too.*

Proof. This follows from (b) above: start with a chain in Q, and intersect this with R, which then must stabilise, because R is Noetherian. ■

Now, we want to prove uniqueness of right quotient rings.

Lemma 4.7. *Let R_1, R_2 be rings with right quotient rings Q_1, Q_2 respectively. Suppose that $R_1 \cong R_2$. Then $Q_1 \cong Q_2$.*

Proof. Let $f : R_1 \to R_2$ be the isomorphism. A typical element of Q_1 is ac^{-1} with $a, c \in R$ and c regular. Note that $f(c)$ is regular in R_2. Define $F : Q_1 \to Q_2$ by $F(ac^{-1}) = f(a)f(c)^{-1}$. We need to check that this is well-defined. Suppose that $ac^{-1} = bd^{-1}$, with c, d regular. Then $ac^{-1}d = b$. (if R was commutative could just conclude that $ad = bc$). Now we have $c^{-1}d = ef^{-1}$ for some $e, f \in R_1$, with f regular. So $df = ce$, hence $f(df) = f(ce)$, so $f(d)f(f) = f(c)f(e)$. Both $f(f)$, $f(c)$ are regular in R_2, so we have

$$f(c)^{-1}f(d) = f(e)f(f)^{-1} \quad (*)$$

But $b = aef^{-1}$, so $bf = ae$, hence $f(bf) = f(ae)$, so $f(b)f(f) = f(a)f(e)$, thus $f(b) = f(a)f(e)f(f)^{-1}$, so by $(*)$, $f(a)f(c)^{-1} = f(b)f(d)^{-1}$, as required. Similarly, F is a homomorphism, and bijective. For example, to prove additivity, use the common denominator. Note that for injectivity, you can reverse the above argument. ■

Corollary 4.8. *If R has two right quotient rings then these are isomorphic via an isomorphism which is the identity map on R.*

4.1 The Ore Condition

Now we consider the question of existence of quotient rings. This is a much longer road than that of establishing uniqueness.

Definition 4.9. Let $\emptyset \neq S \subset R$ be a subset. S is multiplicatively closed if $s_1, s_2 \in S \Rightarrow s_1 s_2 \in S$. R has the *right Ore condition* with respect to S if given $a \in R$, $s \in S$, there exist $a_1 \in R$, $s_1 \in S$ with $as_1 = sa_1$. This is also known as the right common multiple property.

One can think of the Ore Condition as a "poor man's commutativity".

Example 4.10. The set of regular elements is multiplicatively closed, provided it is non-empty.

Lemma 4.11. *Let S be a multiplicatively closed subset of R. Suppose that the elements of S are regular in R and that R has the right Ore condition with respect to S. Let $(x, c), (y, d), (r, s) \in R \times S$. such that $cr = ds$ and $xr = ys$. Then for any $a, b \in R$, $ca = db$ implies that $xa = yb$.*

Think about what this means in terms of fractions, and common multiples. Recall that if R is a (commutative) integral domain, then we can construct a field of fractions. Contrast the equivalence relation there with what we are doing.

Proof. Since R has the right Ore condition with respect to S, there exists $(\lambda, \mu) \in R \times S$ such that $b\mu = s\lambda$. Now $ca\mu = db\mu = ds\lambda = cr\lambda$. So $a\mu = r\lambda$ as $r(c) = 0$. Hence $xa\mu = xr\lambda = \mu d\lambda = yb\mu$. Thus $xa = yb$ since $l(u) = 0$. ■

Remark. We used both left and right regularity of elements of S.

Theorem 4.12. *Let R be a ring with at least one regular element. Let S be the set of all regular elements or R. (In an integral domain this is all non zero elements.) Then R has a right quotient ring if and only if R satisfies the right Ore condition with respect to S.*

Note. Often we just take S as here to be the set of all regular elements, and by "R satisfies the right Ore condition", we mean with respect to this S.

Proof. "⇒": Let $a \in R$, $c \in S$. Then by definition of a right quotient ring, we must have that $c^{-1}a = a_1 c_1^{-1}$ for some $a_1 \in R$, and $c_1 \in S$. So $ac_1 = ca_1$.

"⇐": Define an equivalence relation $\equiv$ on $R \times S$ as follows: $(x, c) \equiv (y, d) \Leftrightarrow$ there exists $(r, s) \in R \times S$ such that $cr = ds$ and $xr = ys$. This is clearly reflexative. For symmetry, assume that $(x, c) \equiv (y, d)$. By the right Ore condition, we can find $(r_1, s_1) \in R \times S$ such that $dr_1 = cs_1 (*)$. Since $(x, c) \equiv (y, d)$, we can find $(r, s) \in R \times S$ such that $cr = ds$ and $xr = ys$. Then by the above technical lemma, we have that $yr_1 = xs_1$. Thus $(y, d) \equiv (x, c)$ by this and $(*)$. Suppose now that $(x, c) \equiv (y, d) \equiv (z, e)$. By the right Ore condition, there exists $(r, s) \in R \times S$ such that $cr = es$, and there exists $(r_2, s_2) \in R \times S$ such that $dr_2 = (es)s_2 = (cr)s_2 = c(rs_2)$, so this gives that $yr_2 = xrs_2$. Again the technical lemma gives that $dr_2 = ess_2$, so $yr_2 = zss_2$. So $xrs_2 = yr_2 = zss_2$. Hence $xr = zs$ since s_2 is regular. So the relation is transitive.

Let $Q = \{(x, c) \mid (x, c) \in R \times S\}/\sim$. Now we need to turn this into a ring. Denote the class of (x, c) by $\frac{x}{c}$. Define

$$\frac{x}{c} + \frac{y}{d} := \frac{xr + ys}{ds},$$

where $(r, s) \in R \times S$ is such that $cr = ds$. This is well defined: Suppose that $\frac{x}{c} = \frac{x'}{c'}$ and $\frac{y}{d} = \frac{y'}{d'}$. Then by the right Ore condition, there is $(r', s') \in R \times S$, with $cr' = d's'$, and $(\rho, \sigma) \in R \times S$ such that $ds\rho = d's'\sigma$. By the technical lemma, we have that $ys\rho = y's'\sigma$. Now

$$cr\rho = ds\rho = d's'\sigma = c'r'\sigma$$

By the lemma, $xr\rho = x'r'\sigma$, so

$$(xr + ys)\rho = xr\rho + ys\rho = x'r'\sigma + y's'\sigma = (x'r' + y's')\sigma$$

Thus $\frac{xr+ys}{ds} = \frac{x'r'+y's'}{d's'}$. With similar techniques, it can be shown that Q under this addition is an Abelian group. Define

$$\frac{x}{c} \cdot \frac{y}{d} := \frac{x\lambda}{d\mu}$$

where $(\lambda, \mu) \in R \times S$ is such that $y\mu = c\lambda$. Show that this product is also well defined, and that $(Q, +, \cdot)$ forms a ring. Q also has the following properties:

1. Q has an identity $1 = \frac{d}{d}$ for any regular $d \in S$.
2. R can be embedded in Q as a subring, via

   $$x \mapsto \frac{xd}{d},$$

   again for (any) $d \in S$, the map is independent of choice of d, and a ring monomorphism.
3. Identifying R with it's image in Q, elements of S are units of Q, and Q is the right quotient ring.

■

Note. Note that there is actually work to be done to prove this is a symmetric equivalence relation, which is quite rare. We won't use the details of this construction later, as usual with these sorts of things.

So the question still remains, as to how often does Ore's condition hold / the right quotient ring exists.

4.2 Integral Domains

Definition 4.13. A module M_R is said to have finite Goldie (or uniform) dimension, if M contains no infinite direct sum of (non-zero) submodules.

Artinian and Noetherian modules have finite Goldie dimension, as an infinite direct sum allows to construct an infinite ascending/descending chain. So we can consider this a weaker requirement then the strong conditions of being Noetherian or Artinian.
The following technical lemma will help us make this definition more tractable.

Lemma 4.14. *Let R be a ring and $c \in R$ such that $r(c) = 0$. Let $I \triangleleft_r R$, with $I \cap cR = 0$. Then $I + cI + c^2 I + ...$ is a direct sum.*

Proof. Let $x_0 + cx_1 + c^2 x_2 + ...c^n x_n = 0$. Then $x_0 = 0$, as $-x_0 \in I \cap cR = 0$. Then $cx_1 + c^2 x_2 + ...c^n x_n = 0$, so as $r(c) = 0$, $x_1 + c^1 x_2 + ...c^{n-1} x_n = 0$. Similarly, $x_1 = 0$. Continue, to obtain that $x_i = 0$ for all i. Hence the sum is direct. ■

It is fairly easy to see that if a domain has a right quotient ring D, then D must be a division ring. Indeed, an integral domain R satisfies the following condition, as it has a field of fractions, and so R_R has finite Goldie dimension - integral domains can contain no infinite direct sum. This is in line with the motto - "whatever you do for general rings, check what this means in the commutative case".

Theorem 4.15. *Let R be a domain. Then R has right quotient* division *ring if and only if R_R is finite dimensional.*

We prove a far stronger result.

Proof. "$\Rightarrow$": Let I, K be two non-zero right ideals of R. Let $0 \neq a, c \in I, K$ respectively. By the right Ore condition, there exists $a_1, c_1 \in R$ with $c_1 \neq 0$, such that $ac_1 = ca_1$. Thus $0 \neq ac_1 = ca_1 \in I \cap K$. Thus R_R cannot contain an infinite direct sum of right ideals.
"$\Leftarrow$": We use the above lemma. Let $a, c \in R$ with $c \neq 0$. If $a = 0$, then we have $ac = ca$. So assume that $a \neq 0$. So $aR \neq 0$. So $aR \cap cR \neq 0$, by the lemma. So there exists $a_1, c_1 \in R$ with $c_1 \neq 0$ such that $ac_1 = ca_1$. So by Ore's theorem, R has a right quotient ring which must be a division ring, as every non-zero element is regular so a unit of the quotient ring. ■

This is a special case of Goldie's theorem, see 5.11. In this case the proof is quite straightforward. The theorem shows that the Ore condition can be obtained naturally, in a far easier way than you might expect.
Now we give an example to show that a right quotient ring need not exist. Recall that if k is a field, then $k[x]$ is a PID. This is proven using the Euclidean algorithm, on the degree of the polynomial.

Example 4.16 (G.Higman)**.** We exhibit an integral domain, which has a quotient ring on the left, but not on the right. To construct, let F be a field with a monomorphism $F \to F$, $a \mapsto \bar{a}$ $(a \in F)$ which is not surjective. Let $\{\bar{a} \mid a \in F\} =: \bar{F} \subsetneq F$. Let $R = F[x]$, as a set, but with multiplication defined by $xa = \bar{a}x$, and the distributive law. It can be checked that this defines an integral domain (by a degree argument). Furthermore, R has the Euclidian algorithm, so every left ideal of R is principal. (The commutative proof works here for left ideals but not right because of the twist.) So by the above, R has a left quotient division ring. However, R does not satisfy the right Ore condition (with respect it's non-zero/regular elements): Consider $x+a$ and x^2 in R, where $a \in F \setminus \bar{F}$. Suppose that there exists $f(x), g(x)$ such that $(x+a)f(x) = x^2 g(x)$. Then $(x+a)(b_0 + b_1 x + ... + b_k x^k) = x^2(c_0 + ... + c_{k-1}x^{k-1})$ for some $b_i, c_i \in F$, where $b_k \neq 0$. So

$$ab_0 + (\bar{b}_0 + ab_1)x + ... + (\bar{b}_{k-1} + ab_k)x^k + \bar{b}_k x^{k+1} = (\bar{\bar{c}}_0 + ... + \bar{\bar{c}}_{k-1} x^{k-1})x^2$$

so $\bar{b}_k = \bar{\bar{c}}_{k-1}$. Being a monomorphism, this implies that $b_k = \bar{c}_{k-1} \in \bar{F}$. Now $\bar{b}_{k-1} + ab_k = \bar{c}_{k-2}$. This implies that $a \in \bar{F}$ unless $b_k = 0$, so $b_k = 0$. Therefore, the only option is $f = g = 0$.

Remark. (a) The ring $R \oplus R^{\text{op}}$ with have a quotient ring on neither side.

(b) In fact, Mal'cer has constructed an example of an integral domain which is not embeddable in any division ring.

If we have quotient rings on the right and left then the following shows that these must be the same.

Proposition 4.17. *If R has a left quotient ring P and a right quotient ring Q, then $Q \cong P$ which is the identity on R, and Q is also a left quotient ring, P a right quotient ring.*

Proof. Consider the arbitrary element ac^{-1} of Q, with $a, c \in R$ and c regular. Since R has the left Ore condition, there exists $a_1, c_1 \in R$ with c_1 regular, such that $c_1 a = a_1 c$. So $ac^{-1} = c_1^{-1} a \in Q$. Then Q is a left quotient ring, and we obtain the isomorphism from the earlier uniqueness theorem. ■

5 Goldie's Theorems

Recall that DCC implies ACC for rings, semiprime and DCC implies Artin Wedderburn. We now seek to answer the question of what semiprime and ACC imply.

5.1 The Singular Submodule

Definition 5.1. Let $M \neq 0$ be a right R-module. A submodule E of M is called *essential* if $E \cap K \neq 0$, whenever $K \neq 0$ is a submodule of M.

Every non-zero ideal of a commutative domain is essential - take the product of a non zero element of E and of K. See also exercise 29, which gives that if A is a submodule of M_R, then there exists a submodule B of M such that $A \oplus B$ is essential.

Lemma 5.2. *Let E be an essential submodule of M_R. Let $a \in M$. Define*

$$F = \{r \in R \mid ar \in E\}.$$

Then F is an essential right ideal of R.

Proof. Clearly F is a right ideal of R. Now let $0 \neq I \triangleleft_r R$. If $aI = 0$, then $0 \neq I \subset F \cap I$. Now assume that $aI \neq 0$, thus aI is a non-zero submodule of M and therefore $aI \cap E \neq 0$. So there exists $x \in E$, $t \in I$ such that $0 \neq x = at$. Hence $0 \neq t \in F \cap I$. Thus F is essential in R. ■

Proposition 5.3. *Let M be a right R module. Define*

$$Z(M) = \{m \in M \mid mE_m = 0 \textit{ for some essential right ideal } E_m \textit{ of } R\}$$

Then $Z(M)$ is a submodule of M.

Note. The right singular ideal $Z(R)$ of R can also be written as:

$$Z(R) = \{x \in R \mid r(x) \text{ is essential in } R\}.$$

Proof. Let $m_1, m_2 \in Z(M)$, so $m_1E_1 = 0$, $m_2E_2 = 0$, for some essential right ideals E_1, E_2 of R. Then $m_1 - m_2 \in Z(M)$, as $(m_1 - m_2)(E_1 \cap E_2) = 0$, and $E_1 \cap E_2$ is an essential right ideal still. It is not obvious how to proceed, but we can use the preceding lemma. Let $m \in Z(M)$, $a \in R$. Then there exists an essential right ideal E of R, such that $mE = 0$. Define $F = \{r \in R \mid ar \in E\}$. By the lemma with $M_R = R_R$, F is an essential right ideal of R. Now $maF \subset mE = 0$, hence $ma \in Z(R)$. ■

Definition 5.4. $Z = Z(M)$ as defined above is called the singular submodule of M.

$Z = Z(R_R)$ is clearly a two sided ideal of R. Similarly $Z' = Z({}_RR)$ is a two sided ideal of R. However, these need not be the same! We call Z the *right singular ideal of* R, and Z' the *left singular ideal of* R.

Lemma 5.5. *Let R be a ring with ACC on right annihilators. Then*

(a) $Z(R)$ is a nil ideal.

(b) If R is a semiprime ring, then $Z = 0$.

Proof. The first is done by "Fittings Lemma".

(a) Let $z \in Z$. Claim: there is some $n \geq 0$ such that $z^nR \cap r(z^n) = 0$. The chain

$$r(z) \subset r(z^2) \subset ...$$

must stabilise: $r(z^n) = ... = r(z^{2n})$. Let $y \in z^nR \cap r(z^n)$. $y = z^nt$ for some $t \in R$, and $z^ny = 0$, implies that $z^{2n}t = 0$, so $t \in r(z^{2n}) = r(z^n)$. So $y = z^nt = 0$. Now $z^n \in Z$ since Z is an ideal of R. Hence $r(z^n)$ is essential by the above note. So $z^nR = 0$ and $z^{n+1} = 0$.

(b) Follows directly from Utumi's Lemma 2.33.

■

Definition 5.6. R is a called a *right Goldie ring* if R_R is finite dimensional and R has ACC on right annihilators.

A integral domain is then a Goldie ring. A right Noetherian ring is a right Goldie ring.

Lemma 5.7. *Let R be a semiprime right Goldie ring, and $c \in R$. Then $r(c) = 0 \Rightarrow l(c) = 0$.*

Proof. Now cR is essential by 4.14. So $l(c) \subset Z(R)$. By 5.5(b), $Z(R) = 0$ and thus $l(c) = 0$. ■

Remark. So right regular elements are left regular automatically. Note $l(c) = 0 \not\Rightarrow r(c) = 0$ - see exercise 48.

5.2 Goldie's Theorems

The following proposition is key.

Proposition 5.8. *Every essential right ideal of a semiprime right Goldie ring R contains a regular element.*

Proof. Let E be an essential right ideal of R. Then by Utumi's lemma 2.33, E cannot be nil (all nil one sided ideals are zero). Using ACC on right annihilators, choose $c_1 \in E$ such that $r(c_1)$ is maximal in $\{r(x) \mid 0 \neq x \in E,\ x \text{ not nilpotent}\} \neq \emptyset$. Then $r(c_1) = r(c_1^2)$. If $E \cap r(c_1) = 0$, then $r(c_1) = 0$. So by 5.7, c_1 is regular. If $E \cap r(c_1) \neq 0$, then as above, $E \cap r(c_1)$ is not nil. Choose $c_2 \in E \cap r(c_1)$ such that $r(c_2)$ is maximal in $\{r(x) \mid 0 \neq x \in E \cap r(c_1),\ x \text{ not nilpotent}\} \neq \emptyset$. Then $r(c_2) = r(c_2^2)$. We claim $r(c_1 + c_2) = r(c_1) \cap r(c_2)$. Clearly $r(c_1 + c_2) \supset r(c_1) \cap r(c_2)$. Conversely, if $c_1 y = -c_2 y$ for some $y \in R$, then $c_1^2 y = -c_1 c_2 y = 0$, so $y \in r(c_1^2) = r(c_1)$, so $c_1 y = 0$, and so also $c_2 y = 0$, thus $r(c_1 + c_2) = r(c_1) \cap r(c_2)$. Similarly, if $c_1 a = c_2 b \in c_1 R \cap c_2 R$, then $c_1 a = c_1^2 a = c_1 c_2 b = 0$, as $c_2 \in r(c_1)$, thus $c_1 R \cap c_2 R$ is a direct sum. If $r(c_1 + c_2) \neq 0$, then choose $c_3 \in E \cap r(c_1) \cap r(c_2) \neq 0$. Repeat process, to obtain $r(c_1 + c_2 + c_3) = r(c_1) \cap r(c_2) \cap r(c_3)$, and $(c_1 R \oplus c_2 R) + c_3 R$ is a direct sum. As R_R is finite dimensional, this procedure cannot continue indefinitely, so we obtain $c = c_1 + \ldots + c_n$ with $c \in E$ and $r(c) = 0$. ■

This is similar to the proof that semiprime Artinian rings have identity, as that proof was inspired by this.

Lemma 5.9. *If K is a nilpotent (two sided) ideal of a ring R, then $l(K)$ (also two sided) is an essential right ideal of R.*

Proof. Let $0 \neq I \triangleleft_r R$. If $IK = 0$, then $0 \neq I \subset l(K) \cap I$. Otherwise, since K is nilpotent, there exists $n > 1$ such that $IK^n = 0$, but $IK^{n-1} \neq 0$. But then $0 \neq IK^{n-1} \subset l(K) \cap I$. So $l(K)$ is essential as a right ideal. ■

Lemma 5.10. *Let R be a ring, with a right quotient ring Q. Then*

1. *E essential right ideal of $R \Rightarrow EQ$ essential right ideal of Q.*
2. *F essential right ideal of $Q \Rightarrow F \cap R$ essential right ideal of R.*

Proof.

1. Let $K \neq 0$ be a right ideal of Q. Then $K \cap R$ is a right ideal of R, and so intersects E non-trivially, $a \in E \cap K \cap R$. Then $a = a1 \in EQ$. So EQ is essential.
2. Let $0 \neq J \triangleleft_r R$. We want to show $F \cap J = (F \cap R) \cap J \neq 0$. Now JQ is a non-zero ideal of Q, so $t \in JQ \cap F \neq 0$. We can write $t = xc^{-1}$ for $x \in J$, $c \in R$ regular. Then $tc = x \neq 0$, $tc \in F \cap J$, so $F \cap J \neq 0$, and $F \cap R$ is essential in R.

■

Theorem 5.11 (Goldie's Theorem, 1960)**.** *A ring R has a semisimple Artinian right quotient ring $Q \Leftrightarrow R$ is a semiprime right Goldie ring.*

Being semiprime Noetherian is (strictly) stronger than the right condition. The key recurrent point of the proof is that every essential ideal contains a right regular (so left regular) element.

Proof. "$\Leftarrow$": Let $a, c \in R$, with c regular. By 4.14, cR is essential in R. Let $F = \{r \in R \mid ar \in cR\}$. Then $F \lhd_r R$, and by 5.2, F is also essential. So by 5.8, F contains a regular element, call it c_1. Thus $ac_1 = ca_1$ for some $a \in R$, and by Ore's theorem, R has a right quotient ring, call it Q. We want to show that this is semisimple Artinian. Let G be an essential right ideal of Q. Then by the above, $G \cap R$ is an essential right ideal of R. By 5.8, $G \cap R$ contains a regular element, so G contains a unit of Q, hence $G = Q$. So every right ideal of Q is a direct summand of Q, by exercise 29. Thus Q_Q is completely reducible. As Q has a unit, then Q is semisimple Artinian.

"$\Rightarrow$": Let E be an essential right ideal of R. By the previous lemma, EQ is an essential right ideal of Q. Q semisimple Artinian, so every right ideal is a direct summand. Hence $EQ = Q$. So $1 = xc^{-1}$, for some $x \in E$, $c \in R$, regular, as $1 \in EQ$. So $c = x \in E$. Thus every essential right ideal of R contains a regular element. Trick: Suppose K is a nilpotent ideal of R. By 5.9, $l(K)$ (two sided) is essential as a right ideal. So $l(K)$ contains a regular element, which forces $l(K) = 0$. So R is semiprime.

A direct sum of right ideals of R extends to one of Q (I_i goes to I_iQ), so R cannot be an infinite direct sum. Hence R_R is finite dimensional. Finally, for any annihilator right ideal $r_R(T)$, we have $r_R(T) = r_Q(T) \cap R$.

Q has ACC on right ideals (every ideal idempotently generated, so principal), hence R has ACC on right annihilators. ■

The proof used effectively all the theory we have developed so far. This theorem is from 1967, due to Goldie, and is a simplified version of his original proof. R semiprime and DCC implies that R is isomorphic to a product of matrix rings over division rings. The weaker condition, R semiprime and ACC, then implies R has a right quotient ring which is a product of matrix rings over division rings. This came as a surprise at the time, as this weak condition contains a large class of rings.

5.3 The Prime Case

We now see what happens if the ring is prime. If A is an ideal of R, then the right ideal AQ of Q is not necessarily a two-sided ideal of Q. However we can ensure it is a left ideal when Q is Noetherian.

Lemma 5.12. *Let R be a ring with a right quotient ring Q. Suppose that Q is right Noetherian. Then $A \lhd R \Rightarrow AQ \lhd Q$.*

Proof. Clearly, $AQ \lhd_r Q$. Let c be a regular element of R. Now for all $i > 0$, $c^i AQ \subset AQ$ so we can consider the chain

$$AQ \subset c^{-1}AQ \subset c^{-2}AQ \subset$$

of right ideals in Q. This stabilises, hence for some k, $c^{-k}AQ = c^{-(k+1)}AQ$, hence $AQ = c^{-1}AQ$. This holds for any regular $c \in R$, so as we can write any element of Q as ac^{-1} where $a, c \in R$ and c is regular, $(ac^{-1})AQ = a(AQ) \subset AQ$, so AQ is a left ideal of Q. ■

Theorem 5.13 (Goldie, 1958)**.** *A ring R has a simple Artinain right quotient ring if and only if R is a prime right Goldie ring.*

Proof. "$\Leftarrow$": By Goldie's Theorem, we know R has a semisimple Artinian right quotient ring Q and we just need to show this is simple. Let $AB = 0$, with $A, B \lhd Q$, then

$(A \cap R)(B \cap R) = 0$. So as R is prime, either $A \cap R = 0$, or $B \cap R = 0$. Hence $A = (A \cap R)Q = 0$ or $B = (B \cap R)Q = 0$, so $A = 0$ or $B = 0$.
"$\Rightarrow$": R is a semiprime right Goldie ring. Let $AB = 0$, with $A, B \lhd R$, suppose $B \neq 0$. By the above, $BQ \lhd Q$. So $BQ = Q$, because Q is simple. So $0 = AB = ABQ = AQ$. Thus $A = 0$, and R is a prime ring. ■

Note that this shows that if R is a prime ring, then it's right quotient must be prime too. Chronologically, the main theorem was done 2 years later, and this corollary before! In the remaining sections, we will do some small topics where this machinery is used.

5.4 Quasi-Frobenius Rings

Definition 5.14. A ring R is called *Quasi-Frobenius* (QF) if

(a) R has DCC on right and left ideals

(b) Every right ideal of R is a right annihilator.

(c) Every left ideal of R is a left annihilator.

Remark. Recall that Artinain means that our ring has identity. We cannot say that these rings are Artinian, but we shall prove that they all have an identity in this section.

Example 5.15. (a) All semisimple Artinian rings are Quasi-Frobenius.

(b) Let F be field and G a finite group. Then the group ring is Quasi-Frobenius (we won't prove this though). Note that when the characteristic does not divide $|G|$, the $F[G]$ is semisimple Artinian. If F has characteristic $p > 0$ and $p \mid |G|$, then let $x = \sum_{g \in G} g$. This is central and xR is nilpotent, as $x^2 = |G|x = 0$ (so Mashke's Theorem is an if and only if statement).

An equivalent way to state the definition is the following.

Definition 5.16. A ring R is called *Quasi-Frobenius* (QF) if

(a) R has DCC on right and left ideals.

(b) $I \lhd_r R \Rightarrow I = rl(I)$.

(c) $I \lhd_l R \Rightarrow I = lr(I)$.

Lemma 5.17. *Let R be a Quasi-Frobenius ring, Then:*

(a) $I \lhd_r R \Rightarrow I = rl(I)$ and $I \lhd_l R \Rightarrow I = lr(I)$.

(b) R is Noetherian.

(c) $xR = 0$ and $x \in R \Rightarrow x = 0$, and $Rx = 0$, $x \in R \Rightarrow x = 0$.

Proof. For (a) and (b) see 2.7. For (c) we have $0 = rl(0) = r(R)$, and $0 = lr(0) = l(r)$. ■

Recall that $Z = Z(R)$ is the right singular ideal of R, and $Z' = Z'(R)$ is the left singular ideal of R, and these don't typically agree (example: upper triangular matrices). Also, $E(R)$ is the right socle, $E'(R)$ the left, and $N = N(R)$ the nilpotent radical.

Theorem 5.18. *In a Quasi-Frobenius ring R, then $E(R) = l(N) = E'(R) = r(N)$.*

Proof. If F is an essential right ideal of R, then $F \supset E$, as F is essential, so $Z \subset l(E)$. Also as R has DCC on the right, all right ideals contain a minimal right ideal, hence E is essential and $l(E) \subset Z$. Thus $Z = l(E)$. Now R is right Noetherian, so by 5.5 Z is nil, and by 2.31 Z is nilpotent, thus $l(E) = Z \subset N$. Hence $E = rl(E) \supset r(N)$. But $EN = 0$, so $E \subset l(N)$. So we have that $r(N) \subset E \subset l(N)$. Symmetrically, we have that $l(N) \subset E' \subset r(N)$. So these are all equal. ■

Remark. You cannot just use exercise 36 to say $E = l(N)$, as this requires existence of the identity.

Theorem 5.19. *Let R be a ring with DCC on left and right ideals, $l(R) = 0 = r(R)$, and $E \subset E'$. Then R has an identity.*

Proof. By Hopkin's Theorem 2.31, N is nilpotent, so $N \neq R$, as $l(R) = 0$. Hence R/N is a non-zero semisimple Artinian ring, and so has an identity, $e + N$, by 3.21 . Then $R = N + Re$. So $0 = r(R) = r(N) \cap r(Re) = E' \cap r(Re)$. Since $NE = 0$ always, so

$$E' \cap r(Re) = E \cap r(Re) = r(Re)$$

as E is an essential right ideal. So the result follows by 3.20. ■

Ref: Orders in Quasi-Frobenius rings, Journal of Algebra, 1971, pages 329-345.

Corollary 5.20. *Any Quasi-Frobenius Ring has an identity.*

5.5 The Goldie Dimension of a Module

In this section we shall assume that for all modules M_R, $mR = 0 \Rightarrow m = 0$. For example this always holds when R is unital and M_R is a unital R module.

Definition 5.21. U_R is said to be *uniform*, if $U \neq 0$, and $U_1 \cap U_2 \neq 0$ for any U_i submodules of U_R.

Clearly irreducible submodules are uniform, and if R is a domain, then R_R is uniform.

Proposition 5.22. *U_R is uniform, if and only if $U \neq 0$ and for any non zero $u_1, u_2 \in U$, there exists $r_1, r_2 \in R$ such that $u_1 r_1 = u_2 r_2 \neq 0$.*

Lemma 5.23. *Let $M_R \neq 0$ be finite dimensional. Then M contains a uniform submodule.*

Proof. If M not uniform, it contains a direct sum $M_1 \oplus M_2$. If M_1 not uniform, then it contains a direct sum $M_{1_1} \oplus M_{1_2}$. So we have a direct sum $M_{1_1} \oplus M_{1_2} \oplus M_2$. This cannot continue forever, as finite dimensional. ■

Theorem 5.24. *Let $M_R \neq 0$ be finite dimensional. Then there exist uniform submodules $U_1, ..., U_n$ of M such that their sum is direct, and $U_1 \oplus ... \oplus U_n$ is essential in M.*

Proof. By the above, M contains a uniform submodule U_1. If U_1 is not essential, then there exists $0 \neq X_1$ such that $U_1 \cap X_1 = 0$. Choose U_2 uniform in X_1. If $U_1 \oplus U_2$ not essential, then etc. Since M contains no infinite dimensional direct sum, this process must terminate. ■

Think of uniform as analog here, of irreducible modules in Artinian case. We will now investigate the number n of uniform submodules in the direct sum.

Proposition 5.25. *Let M_R be a module containing a direct sum of uniform submodules $S = U_1 \oplus ... \oplus U_n$, which is essential in M. Suppose that for all i we have submodules V_i with $0 \neq V_i \subset U_i$. Then $V_1 \oplus ... \oplus V_n$ is also essential in M.*

Proof. Let $S_1 = V_1 \oplus U_2 \oplus ... \oplus U_n$. It is sufficient to show that S_1 is essential in M. Let $0 \neq X$ be a submodule of M. Then $X \cap S \neq 0$. Choose $0 \neq x = u_1 + ... + u_n$ with $u_i \in U_i$. If $u_1 = 0$, then $x \in S_1 \cap X$. If $u_1 \neq 0$, then by 5.22, there exists $r \in R$ with $0 \neq u_1 r \in V_1$. Then $0 \neq xr = u_1 r + u_2 r + ... + u_n r \in S_1 \cap X$. ■

Recall: If V is a finite dimensional vector space, then any two basis have the same number of elements. For two bases $x_1, ..., x_k$, and $y_1, ..., y_l$ look at $x_2, ..., x_n$. We must have at least one of y_i not a linear combination of $x_2, .., x_k$. Say y_1. So $y_1, x_2, ..., x_k$ are linearly independent, and we can write x_1 as a linear combination, so forms a basis. If $k > l$, then $y_1, ..., y_l, ..., x_k$ is a basis, which is tosh. By symmetry, we also can't have $k < l$. So $k = l$.

Theorem 5.26. *Let M_R have finite (Goldie) dimension. Then the integer n of 5.24 is an invariant of the module.*

Proof. Suppose that $S = U_1 \oplus \cdots \oplus U_k$, and $T = V_1 \oplus \cdots \oplus V_l$ are both direct sums of uniform submodules which are essential in M. Consider $S_1 = U_2 \oplus \cdots \oplus U_n$. Suppose for a contradiction that $S_1 \cap V_j \neq 0$ for all j. Then S_1 is essential : for any submodule $K \neq 0$, $K \cap V_j \neq 0$ for some V_j, thus $(K \cap V_i) \cap (S_1 \cap V_i) \neq 0$, so $K \cap S_1 \neq 0$. But S_1 is not essential as $S_1 \cap U_1 = 0$. Therefore there exists some V_i with $S_1 \cap V_i = 0$. Without loss of generality, this is V_1, so the sum $S_2 := (V_1 \cap U_1) \oplus U_2 \oplus \cdots \oplus U_k$ is direct, and is essential by the above. Continuing this way, removing U_2, the submodule $(V_1 \cap U_1) \oplus U_3 \oplus \cdots \oplus U_k$ intersects trivially some V_i, for $i \neq 1$, and by the same reasoning $S_3 = (V_1 \cap U_1) \oplus (V_2 \cap U_2) \oplus U_3 \oplus \cdots \oplus U_k$ is direct and essential. If $k > l$, then $(V_1 \cap U_1) \oplus (V_2 \cap U_2) \oplus \cdots \oplus (V_l \cap U_l) \oplus \cdots \oplus U_k$ is essential in M, which is impossible, as $U_k \cap V_i$ for some i, so the sum is not direct. Therefore, $k \leq l$, and by symmetry $k \geq l$, thus $k = l$. ■

Definition 5.27. Let M_R be finite dimensional. Then the invariant $n \in \mathbb{N}$ is called the *Goldie* (or *Uniform*) dimension. It is denoted by $\dim M$. We define $\dim M = 0$ for $M = 0$, and $\dim M = \infty$ if not finite Goldie dimensional.

Clearly $\dim M = 1$ if and only if $M \neq 0$ and M is uniform. Goldie introduced this dimension to prove his original theorems, but the modern proof which we have done doesn't use it. However, this still has many uses.

6 Exercises

6.1 Questions

1. Suppose that R satisfies all ring axioms for a ring with identity, except that for all $x, y \in R$, $x + y = y + x$. Show that this axiom is implied by the rest.

2. Let R be a generalised Boolean ring: for any $x \in R$, $x^2 = x$. Show that R is commutative (first show that $x + x = 0$ for all $x \in R$).

3. A *left-identity* for a ring R is $e \in R$ with $ex = x$ for all $x \in R$. Similarly a right-identity is $e \in R$ with $xe = x$ for all $x \in R$.

   (a) Show that if a ring has a left-identity and a right-identity, then these must be the same element. Therefore, if an identity exists, it must be unique.

   (b) Give an example of a ring R with infinitely many left-identities (try and find a subring of a 2×2 matrix ring).

4. Let R, S be rings, and $\theta : R \to S$ a homomorphism of rings. Show that $\ker(\theta)$ is an ideal of R, and $\theta(R)$ is a subring of S. Show that $\theta(R)$ need not be an ideal.

5. Show that for a division ring D (D has an identity, and every non-zero element is a unit), D has no right ideals other than 0 and D.

6. (Converse) Let D be a ring with identity. Suppose that D has no right ideals other than 0 and D. Show that D is a division ring. Show that, replacing the assumption D has an identity with $D^2 \neq 0$, the same conclusion holds.

7. Let R be a ring with identity, and M a right R-module. Show there exist submodules M_1, M_2 of M with $M = M_1 \oplus M_2$, where M_1 is unital, and $M_2R = 0$ ($mr = 0$ for all $r \in R$ and $m \in M_2$).

8. Let R be a ring with identity, with $R = A \oplus B$ a direct sum of right ideals. If A is a two-sided ideal, does it then follow that B is also two-sided? Proof or counterexample.

9. Let A and B be ideals of a ring R, with $R = A \oplus B$. Show that $R/A \cong B$ as rings.

10. Show that $f : \mathbb{H} \to M_2(\mathbb{C})$,

$$f : a + bi + cj + dk \mapsto \begin{pmatrix} a + bi & c + di \\ -c + di & a - bi \end{pmatrix},$$

    is an injective ring homomorphism.

11. Show that a submodule of a finitely generated module need not be finitely generated.

12. Show that $\mathbb{Q}$ is not finitely generated as a $\mathbb{Z}$-module.

13. Let R be a ring with identity, and M a unital cyclic right R module. Show that $M \cong R/I$ for some right ideal I of R.

14. Let F be a field. Let $A = F \oplus F$, a ring under the standard operations. Show that:

    (a) $(0, F)$ and $(F, 0)$ are irreducible A-submodules.

(b) $(0, F)$ and $(F, 0)$ are isomorphic as F-modules, but *not* as A-modules.

15. Recall lemma 3.20, which says that if R is a ring with DCC on right ideals, $0 = l(R)$, and R contains an element $c \in R$ with $r(c) = 0$, then R contains an identity. The following shows that the condition $r(c) = 0$ cannot be weakened to $r(R) = 0$.

    (Baer's Example) Let F be a finite field, and

    $$R = \begin{bmatrix} F & 0 & 0 \\ F & 0 & 0 \\ F & F & F \end{bmatrix}$$

    Show that R is a ring, and that $l(R) = 0 = r(R)$, but that R does not have an identity.

16. Let M be a right R-module, and $\theta \in \operatorname{End}(M)$. Show that θ is an isomorphism when

    (a) M is Artinian and θ is a monomorphism.

    (b) M is Noetherian and θ is an epimorphism.

17. Show that both

    $$\begin{bmatrix} \mathbb{Z} & 4\mathbb{Z} \\ \mathbb{Z} & \mathbb{Z} \end{bmatrix} \text{ and } \begin{bmatrix} \mathbb{Z} & 2/2\mathbb{Z} \\ 0 & 2/2\mathbb{Z} \end{bmatrix}$$

    are Noetherian rings.

18. Show that both

    $$\begin{bmatrix} \mathbb{Q} & \mathbb{Q} \\ 0 & \mathbb{Q} \end{bmatrix} \text{ and } \begin{bmatrix} \mathbb{R} & \mathbb{C} \\ 0 & \mathbb{C} \end{bmatrix}$$

    are Artinian rings.

19. Let

    $$R = \begin{bmatrix} \mathbb{Q} & \mathbb{R} \\ 0 & \mathbb{R} \end{bmatrix}$$

    Show that

    (a)
    $$N = \begin{bmatrix} 0 & \mathbb{R} \\ 0 & 0 \end{bmatrix}$$
    is an ideal of R.

    (b) $R/N \cong \mathbb{Q} \oplus \mathbb{R}$ as rings.

    (c) N_R is irreducible.

    (d) R is a right Artinian ring.

    (e) $\mathbb{R}$ is not a finitely generated $\mathbb{Q}$-module.

    (f) R is not a left Artinian ring (consider ${}_RN$).

20. Show that a finite direct sum of prime rings with identity is a semi-prime ring.

21. Let R be a semiprime ring. Show that

    (a) If I is an ideal of R, then $l(I) = r(I)$, and $I + r(I)$ is a direct sum.

(b) If M is a minimal right ideal of R then RM is a minimal ideal of R.

22. Let e be an idempotent of a semi-prime ring R. Prove that eR is a minimal right ideal if and only if the ring eRe is a division ring. Deduce that eR is a minimal right ideal if and only if Re is a minimal left ideal.

23. Let $S \neq \emptyset$ be a subset of a ring R. Show that

    (a) $r(S) \triangleleft_r R$ and $l(S) \triangleleft_l R$.

    (b) If $S \triangleleft_r R$, then $r(S) \triangleleft R$.

    (c) $rlr(S) = r(S)$ and $lrl(S) = l(S)$.

24. Let R be a ring with identity, and P maximal in the set $\{r(I) \mid 0 \neq I \triangleleft_r R\}$. Show that P must be a prime ideal of R.

25. Let M be minimal right ideal and K a nil right ideal of a ring R. Show that $MK = 0$.

26. Let $S = \{x_a\}_{a \in \mathcal{A}}$ be a set of vectors in a vector space V. Define what it means for S to span V and for S to be linearly independent. Prove that every vector space has a basis.

27. Show that a finitely generated module has a maximal submodule.

28. Let R be a ring which is not nil. Prove that the intersection of all prime ideals of R is a nil ideal (Show that if $x \in R$ is not nilpotent, then there exists a prime ideal P with $x \notin P$).

29. Let M be a right R-module with a submodule A. Show there exists a submodule B of M such that $A \oplus B$ is essential in M.

30. Let R be a ring with identity, M a unital irreducible right R-module. Show that $M \cong R/K$, where K is maximal right ideal of R.

31. Suppose that M is a right R-module, and $mR = 0$ for $m \in M$ only for $m = 0$. Prove that the socle of M is the intersection of all its essential submodules.

32. Let R be a prime ring. Show that any two minimal right ideals of R are isomorphic as right R-modules (If I and K are such then $IK \neq 0$).

33. Let R be a right Noetherian ring. Let I be an ideal of R such that R/I is a right Artinian ring. Show that for all $n \geq 1$, the ring R/I^n is right Artinian (see 0.4).

34. Let I be a right ideal of a ring R. Suppose that there exist prime ideals $P_1, ..., P_n$ of R such that $I \subset \cup_{i=1}^n P_i$. Show that for some i, $I \subset P_i$ (Use induction on n. Consider terms such as $IP_2 \cdots P_n$).

35. Let E be the right socle of a ring R. Prove that $E^2 = E^3$. Provide an example to show that $E \neq E^2$ in general.

36. Let R be a right Artinian ring. Show that $E = l(N)$, where E is the right socle, and N the nilpotent radical of R (view $l(N)$ as a module over an appropriate ring).

37. Give an example of an Artinian ring where the left and right socles differ (see example 3.18).

38. Let R be a commutative Noetherian ring with identity. Prove that R is an Artinian ring if and only if every prime ideal of R is a maximal ideal (Hint: $\{0\}$ is a product of prime ideals).

39. Show that a prime right Artinian ring must be a simple ring.

40. Show that a prime ideal in a right Artinian ring must be a maximal ideal.

41. Prove that a nil one-sided ideal in a right Artinian ring R must be nilpotent, by using the fact that the ring R/N is a semisimple Artinian, where N is the nilpotent radical of R.

42. Let M be a module of finite length. Let K be a submodule of M. Show that $|M| = |K| + |M/K|$, where $|X|$ denotes the composition length of the module X.

43. Let R be a right Artinian ring. Let I be an ideal of R such that $I = aR = Rb$ for some $a, b \in R$. Show that $I = bR = Rb$ (first show that for all $x \in R$, $xR \cong R/r(x)$, and then use a composition length argument).

44. Show that a left Artinian and right Noetherian ring must necessarily be right Artinian too.

45. Let M be a (unital) irreducible module over a semisimple Artinian ring R. Show that $M \cong I$, where I is a minimal right ideal of R.

46. Show that the right singular ideal of a right Artinian ring R is $l(E)$, where E is the socle of R.

47. Find the quotient rings of
$$\begin{bmatrix} \mathbb{Z} & 2\mathbb{Z} \\ \mathbb{Z} & \mathbb{Z} \end{bmatrix} \text{ and } \begin{bmatrix} \mathbb{Z} & \mathbb{Z} \\ 0 & \mathbb{Z} \end{bmatrix}.$$

48. Consider the matrix
$$c = \begin{pmatrix} x+a & x^2 \\ 0 & 0 \end{pmatrix},$$
in the ring $M_2(R)$, where R is the integral domain from example 4.16, and $x+a$, x^2 the elements considered there. Show that c is right regular but not left regular in $M_2(R)$.

49. Prove that a non-zero ideal of a prime ring is essential as a right ideal.

50. Show that a prime right Goldie ring with a non-zero (right) socle must be simple Artinian.

51. (Non-examinable) Let V be a vector space over $\mathbb{Q}$, with basis $\{x_1, x_2, ...\}$. Let R be the ring of endomorphisms of V. Consider the endomorphisms of V defined by
$$\begin{aligned} e(x_1, x_2, ...) &= (x_1, 0, x_3, 0, x_5, ...) \\ f(x_1, x_2, ...) &= (0, x_2, 0, x_4, 0, ...) \\ t(x_1, x_2, ...) &= (x_1, 0, x_2, 0, x_3, ...) \\ u(x_1, x_2, ...) &= (x_1, x_3, x_5, ...) \\ t'(x_1, x_2, ...) &= (0, x_1, 0, x_2, 0, x_3, ...) \\ u'(x_1, x_2, ...) &= (x_2, x_4, x_6, ...) \end{aligned}$$

Show that

(a) $e + f = \mathbb{1}_V$.

(b) $t = et$ and $tu = e$.

(c) $tR = eR$.

(d) $t'u' = f$ and $t' = ft'$.

(e) $t'R = fR$.

(f) t and t' are injective.

(g) $\{t, t'\}$ is a free basis for R_R.

Deduce that two free basis' of R need not have the same number of elements (Recall that a *finite free basis* of F_R is $f_1, ..., f_n \in F$, where any element $r \in R$ can be written uniquely as $r = f_1r_1 + \cdots + f_nr_n$). This shows that n need not be an invariant, as it is in the commutative case.

Solutions are available upon request - send me an email.