University of Warwick

Ring Theory

MA4H8

Lectured by
Professor Charudatta Hajarnavis

Notes by
Oliver Clarke

2016 - 2017

Contents

Chapter 1

Rings

Sections 1.1 - 1.14 can be found on handouts 1 and 2.

1.1 Rings

Definition 1.1.1. Let R be a non-empty set which has two laws of composition defined on it. (We call these laws *addition* and *multiplication* respectively and use familiar notation). We say that R is a **ring** (with respect to the given addition and multiplication) if the following hold:

1. $a + b \in R$ and $ab \in R$ for all $a, b \in R$
2. $a + b = b + a$ for all $a, b \in R$ (Commutativity of addition)
3. $a + (b + c) = (a + b) + c$ for all $a, b, c \in R$ (Associativity of addition)
4. There exists an element $0 \in R$ such that $a + 0 = a$ for all $a \in R$
5. Given $a \in R$ there exists an element $-a \in R$ such that $a + (-a) = 0$
6. $a(bc) = (ab)c$ for all $a, b, c \in R$ (Associativity of multiplication)
7. $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$ (Distributive Laws)

Thus a ring is an additive Abelian group on which an operation of multiplication is defined; this operation being associative and distributive (both ways) with respect to the addition.

R is called a **commutative ring** if it satisfies in addition $ab = ba$ for all $a, b \in R$. The term **non-commutative ring** usually stands for a *not necessarily commutative ring.*

What follows are the headings for the topics covered in handouts 1 and 2 to keep the numbering consistent.

1.2 Properties of Addition and Multiplication

1.3 Subrings and Ideals

1.4 Cosets and Homomorphisms

1.5 The Isomorphism Theorems (Rings)

1.6 Direct Sums

1.7 Division Rings

1.8 Modules

1.9 Factor Modules and Homomorphisms

1.10 The Isomorphism Theorems (Modules)

1.11 Direct Sums of Modules

1.12 Products of Subsets

1.13 A Construction

1.14 Endomorphism Rings

Course Starts Here

If M_R is an R-module with the property, $m.1 = m$, $\forall m \in M$ then it is called **unitial** (when R has 1).

By Qu.7 Exercise Sheet 1: If R has 1 and M is a right R-module then

$$M = M_1 \oplus M_2$$

with M_1 unitial and $M_2R = 0$ so M_2 is not useful.

Define,

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

to be the collection of all *finite* sums of elements of the M_λ's.

Throughout the course we consider right modules and maps of the left. This way we avoid considering the opposite ring R^{op}. (This can be found in the Rings and Modules course).

1.15 Zorn's Lemma, WOP and Axiom of Choice

Definition 1.15.1. 1. A non-empty set S is said to be **partially ordered** if there exists a binary relation $\leq$ in S which is defined for certain pairs of elements in S and satisfies

- $a \leq a$, $\forall a \in S$
- $a \leq b, b \leq c \Rightarrow a \leq c$, $\forall a, b, c \in S$
- $a \leq b, b \leq a \Rightarrow a = b$, $\forall a, b \in S$

2. Let S be a partially ordered set. A non-empty subset τ is said to be **totally ordered** if $\forall a, b \in \tau$ either $a \leq b$ or $b \leq a$

3. Let S be a partially ordered set. An element $x \in S$ is called a **maximal element** if $x \leq y$ with $y \in S \Rightarrow x = y$. Similarly we define **minimal element**.
4. Let τ be a totally ordered subset of a partially ordered set S. We say τ has an **upper bound** (in S) if $\exists s \in S$ s.t. $\forall t \in \tau,\ t \leq s$.
5. **Zorn's Lemma**. If a partially ordered set S has the property that every totally ordered subset of S has an upper bound in S then S contains a maximal element.
6. A non-empty set S is said to be **well ordered** if it is totally ordered and every non-empty subset of S has a minimal element.
7. **WOP (Well Ordering Principle)** Any non-empty set can be well ordered.
8. **The Axiom of Choice** Given a class of non-empty sets, there exists a *choice function* i.e. a function which assigns to each of its sets one of its elements.

It can be shown that the following are logically equivalent:

- Axiom of Choice
- Zorn's Lemma
- WOP

1.16 Application of Zorn's Lemma

Definition 1.16.1. let R be a non-zero ring and $M \lhd_r R$ $[M \lhd R]$ s.t. $M \neq R$. Then M is said to be a **maximal right ideal** [**maximal ideal**] if $M' \lhd_r R$ $[M' \lhd R]$ with $M \subsetneq M \Rightarrow M' = R$.

Proposition 1.16.2. *Let R be a ring with 1, and $I \lhd_r R$ $[I \lhd R]$ s.t. $I \neq R$. Then $\exists$ a maximal right ideal [ideal] M of R s.t. $I \subseteq M$.*

Example. In $\mathbb{Z}$, $p\mathbb{Z}$ is a maximal ideal for each p prime. Let $M \neq \mathbb{Z}$ be an ideal in $\mathbb{Z}$. $\mathbb{Z}/M$ is a field $\iff$ M is maximal.

Proof. We prove the statement for right ideals. The proof for two sided ideals is the same.

Let $I \lhd_r R$, let S be the set of all proper right ideals of R containing I. Then $S \neq \emptyset$ since $I \in S$. Partially order S by inclusion, i.e. $A, B \in S$, $A \leq B$ if $A \subseteq B$.

Let $\{T_\alpha\}_{\alpha\in\Lambda}$ be a totally ordered subset of S. Consider $T = \bigcup_{\alpha\in\Lambda} T_\alpha$, then $T \lhd_r R$ [Check] and clearly $I \subseteq I$, moreover $T \neq R$ otherwise: $T = R \Rightarrow 1 \in T \Rightarrow \exists\alpha$ s.t. $1 \in T_\alpha \Rightarrow T_\alpha = R$.

Thus $T \in S$ and clearly $T_\alpha \leq T$, $\forall\alpha \in \Lambda$. So T is an upper bound for $\{T_\alpha\}_{\alpha\in\Lambda}$. Thus by Zorn's Lemma, S contains a maximal element M. M is a maximal right ideal and $I \subseteq M$. □

Remark. This proposition is false if R does not contain 1. See Rings and Modules - Remark 8.22.

Exercise. Prove that every vector space has a basis.

Corollary 1.16.3. *A ring with 1 has a maximal right ideal [ideal]*

Proof. Take $I = 0$ and apply the above proposition. □

Chapter 2

General Properties of Rings

2.1 Jacobson Radical

All rings are assumed to have 1 unless otherwise stated.

Definition 2.1.1. The intersection of all the maximal right ideals of a ring R is called its **Jacobson Radical**. Usually denoted $J(R)$ or if there is no ambiguity simply J.

Note that by 1.16.3 R has a least one maximal ideal.

Remark. At this stage, $J(R)$ is the *right Jacobson Radical*, we will show this is equal to the left

Lemma 2.1.2. *Let M be a maximal right ideal of a ring R and let $a \in R$. Define $K = \{r \in R \mid ar \in M\}$. Then $K \lhd_r R$,*

- *If $a \in M$ then $K = R$*
- *If $a \notin M$ then K is also a maximal right ideal of R*

Proof. It is clear that $K \lhd_r R$.

If $a \in M$ then $ar \in M$, $\forall r \in R$ so $K = R$

If $a \notin M$ Then $aR + M \lhd_r R$ with $M \subsetneq aR + M$. Since M is maximal, $aR + M = R$. Define an R-module homomorphism,

$$\theta : R \to R/M \text{ by}$$

$$\theta(r) = ar + M$$

[Check θ is an R-homomorphism] Since $R = aR + M$, θ is an onto map so by first isomorphism theorem $R/M \cong R/Ker(\theta) \cong R/K$. It follows that K is a maximal right ideal of R.

□

Theorem 2.1.3. *$J(R) \lhd R$ (two sided ideal)*

Proof. Clearly $J \lhd_r R$. let $j \in J$ and let $a \in R$ and suppose that $aj \notin J$. Then by definition of J, $\exists$ a maximal right ideal M s.t. $aj \notin M$.

Clearly $a \notin M$. Define $K = \{r \in R \mid ar \in M\}$. Then by the above lemma K is a maximal right ideal of R. But $J \notin K$ since $aj \notin M$ so $j \notin J$. Contradiction.

Thus $aj \in J$, $\forall j \in J, a \in M$. So $J \lhd R$.

□

Definition 2.1.4. Let R be a ring and $x \in R$. We say x is **right quasi-regular (r.q.r.)** if $1 - x$ has a right inverse i.e. $\exists y \in R$ s.t. $(1 - x)y = 1$.

A subset S of R is called **r.q.r** is every element of S is r.q.r. **Left quasi-regular (l.q.r.)** is defined analogously. A set is **quasi-regular** if it is both l.q.r. and r.q.r.

Lemma 2.1.5. *Let I be a r.q.r. right ideal of R then $I \subseteq J(R)$*

Proof. For each maximal ideal M of R let us check that $I \subseteq M$. Suppose not, then $I \nsubseteq M$ so $M \subsetneq I + M$. Thus $I + M = R$. So $1 = x + m$ for some $x \in I$ and $m \in M$. Thus $1 - x = m \in M$. Since I is r.q.r. $\exists y \in R$ s.t. $(1 - x)y = 1$ so $1 = (1 - x)y \in M$ so $M = R$. Contradiction.

Thus $I \subseteq M$ and so $I \subseteq J$. □

Lemma 2.1.6. *Let R be a ring then $J(R)$ is a r.q.r. ideal.*

Proof. let $j \in J$. Suppose $(1-j)$ has no right inverse. Then $(1-j)R \neq R$ so by 1.16.2, $\exists$ a maximal right ideal M s.t. $(1-j)R \subseteq M$. But $j \in M$ by definition of $J(R)$ so $1 = 1-j+j \in M$ so $M = R$. Contradiction.

Thus $1-j$ has right inverse for all $j \in J$. So J is r.q.r. □

Lemma 2.1.7. *Let I be an ideal of R. Then, I r.q.r. $\iff$ I l.q.r.*

Proof. Suppose I is r.q.r. Let $x \in I$. Then $\exists a \in R$ s.t.

$$(1-x)(1-a) = 1$$

$$1 - x - a + xa = 1$$

$$a = xa - x \in I$$

So $\exists t \in R$ s.t. $(1-a)(1-t) = 1$. Hence

$$1 - x = (1-x)1 = (1-x)(1-a)(1-t) = 1(1-t) = 1-t$$

Thus $(1-a)(1-x) = 1$ and x is l.q.r. The converse by symmetry. □

To sum up:

Theorem 2.1.8. *The (right) Jacobson radical is a quasi-regular ideal and contains all the r.q.r. ideals of R.*

Corollary 2.1.9. *The Jacobson radical of a ring is left-right symmetric i.e. right Jacobson radical J_r = left Jacobson radical J_l.*

Proof. J_l is a quasi-regular ideal by the left hand version of 2.1.8. So $J_l \subseteq J_r$ but $J_r \subseteq J_l$ by symmetry so $J_l = J_r$. □

Theorem 2.1.10. *Let R be a ring with Jacobson radical J then*

$$J(R/J) = \{0\}$$

Proof. (By correspondence theorem) The maximal right ideals of the ring R/J are precisely the maximal right ideals of the form M/J where M is a maximal right ideal of R. □

Let R be a commutative ring with 1. Let $M \neq R$ be an ideal. Recall M is maximal $\iff$ the ring R/M is a field.

Example 2.1.11.

1. $J(\mathbb{Z}) = 0$ because $p\mathbb{Z}$, p-prime are precisely the maximal ideals of $\mathbb{Z}$.
2. Let $R = \{a/b \mid a, b \in \mathbb{Z}, b \text{ odd}\}$. Let $0 \neq I \lhd R, I \neq R$. Let $x/y \in I$, $x, y \in \mathbb{Z}$. If x is odd then $y/x \in R$ so $1 = (x/y)(y/x) \in I$. Contradiction. Hence $I \subseteq M = \{2c/b \mid b, c \in \mathbb{Z}, b \text{ odd}\}$. This argument shows that M is the unique maximal ideal of R. So $M = J(R)$. [In fact this is $R = \mathbb{Z}_{(2)}$ - localisation of $\mathbb{Z}$ at the ideal (2)]
3. Let S be a commutative integral domain with field of fractions F. (E.g. R as in (2) and $F = \mathbb{Q}$). Construct,

$$R = \begin{bmatrix} S & F \\ 0 & F \end{bmatrix}, \quad X = \begin{bmatrix} J(S) & F \\ 0 & 0 \end{bmatrix}$$

Then $X \lhd R$

Claim. $X = J(R)$

To prove this let us use quasi-regularity. Let $\begin{bmatrix} j & f \\ 0 & 0 \end{bmatrix} \in X, j \in J(S), f \in F$. Then,

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} - \begin{bmatrix} j & f \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1-j & -j \\ 0 & 1 \end{bmatrix}$$

Now, $\exists y \in S$ s.t. $(1-j)y = 1$.

$$\begin{bmatrix} 1-j & -f \\ 0 & 1 \end{bmatrix} \begin{bmatrix} y & yf \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Thus every element of X is r.q.r, So by 2.1.8 $X \subseteq J(R)$.

Now the map: $\theta : R \to S/J(S) \oplus F$ given by $\theta \begin{bmatrix} s & f_1 \\ 0 & f_2 \end{bmatrix} = (s + J(S), f_2)$ is a surjective homomorphism of rings. $R/X \cong S/J(S) \oplus F$ as rings since $Ker(\theta) = X$. Now for rings A, B we have $J(A \oplus B) = J(A) \oplus J(B)$. Hence $J(S/J(S) \oplus F) = J(S/J(S)) \oplus J(F) = 0$. Therefore $J(R/X) = 0$. But clearly $J(R)/X$ is an r.q.r. ideal of R/X. So $J(R)/X \subseteq J(R/X) = 0$. Therefore $J(R) \subseteq X$, thus $J(R) = X$.

Exercise. Let $J = J(R)$ as in the above example. Show that $\bigcap_{n=1}^{\infty} J^n \neq 0$.

Caution: Let R be a ring with 1 and M a maximal (two sided) ideal of R. Then $J(R) \subseteq M$ [1]. But $J(R)$ is not in general the intersection of all maximal (two sided) ideals of R

Jacobson Radial for rings without 1

Suppose that R has 1 and $a \in R$ is r.q.r. Then $\exists b \in R$ s.t.

$$(1-a)(1-b) = 1$$

$$a + b - ab = 0 \tag{2.1}$$

This is independent of 1 so we define $a \in R$ (R without 1) is r.q.r. if $\exists b \in R$ s.t. (2.1) is satisfied.

In general maximal right ideals may not exist so we call $I \lhd R$ **modular** if $\exists e \in R$ s.t. $r - er \in I, \forall r \in R$. (If $1 \in R$ then take $e = 1$ and I is instantly modular)

By Zorn's Lemma, if R has a proper modular right ideal I then it has a maximal right ideal M s.t. $I \subseteq M$ [2]. When R has 1, every right ideal of R is modular.

$$J(R) := \begin{cases} \bigcap \text{modular maximal right ideals of } R & \text{if } R \text{ has any} \\ R & \text{otherwise} \end{cases}$$

Standard properties follow employing the methods we used previously.

2.2 Finitely Generated Modules

Definition 2.2.1. Let T be a subset of M_R. The *smallest* submodule of M containing T is called the **submodule of M generated by T**.

Formally it is the intersection of all submodules of M containing T. By convention we take 0 to be the submodule generated by $\emptyset$. Of particular importance is the case when T consists of a single element $a \in M$. In general the submodule generated by a is,

$$\{ar + \lambda a \mid r \in R, \lambda \in \mathbb{Z}\}$$

Note that out definition of ring doesn't have $1 \in R$ so $a \in aR$ is not necessarily true. If $1 \in R$ then the above set is given by aR.

Definition 2.2.2. M_R is said to be **finitely generated (f.g.)** if it is the module generated by some finite subset. If R has 1 and M is a unitial f.g. module then $\exists a_1, \ldots, a_n \in M$ s.t. $M = a_1R + \cdots + a_nR$. $a_1, \ldots, a_n$ are called the **generators of** M.

[1] Proof. Suppose not then $\exists j \in J(R)$ s.t. $j \notin M$. Define $RjR := \{\sum_{i \in I, I \text{finite}} a_i j b_i \mid a_i, b_i \in R\}$. Note $RjR \subseteq J(R)$ and is an ideal of R. So $M \subsetneq RjR + M$ is an ideal. Hence $RjR + M = R$ so $\exists x \in RjR, m \in M$ s.t. $x + m = 1$. However $J(R)$ is r.q.r. so $\exists y \in R$ s.t. $1 = (1-x)y = my \in M$ so $M = R$. Contradiction.

[2] The proof follows very similarly to 1.16.2 except we use e instead of 1 to show $T \neq R$.

Definition 2.2.3. 1. A module generated bu a single element is called a **cyclic module**. A f.g. module is a finite sum of cyclic submodules.

2. Cyclic submodules of R_R are called **principal right ideals**.

Lemma 2.2.4 (Nakayama)**.** *Let R be a ring with 1 and M_R a f.g. module. Then $MJ = M \Rightarrow M = 0$.*

Proof. Let $MJ = M$ and suppose that $M \neq 0$. $\exists m_1, \dots, m_k \in M$ s.t. $M = m_1R + \dots + m_kR$. Choose the generating set such that k is the least possible. We have $M = MJ = (m_1R + \dots + m_kR)J \subseteq m_1J + \dots + m_kJ$. Now $m_1 \in M$ so $\exists j_1, \dots, j_k \in J$ s.t. $m_1 = m_1j_1 + m_2j_2 + \dots + m_kj_k$. So $m_1(1 - j_1) = m_2j_2 + \dots + m_kj_k$. (If $k = 1$ then $m_1(1 - j_1) = 0$). Since J is quasi-regular, $m_1 = m_2j_2(1 - j_1)^{-1} + \dots + m_kj_k(1 - j_1)^{-1}$. (If $k = 1$ then $m_1 = 0$). So $m_2, \dots, m_k$ is another generating set for M. (If $k = 1$ then $M = 0$). But this contradicts the minimality of k. Thus $M = 0$. □

Remark. Nakayama's Lemma is also proved for rings without 1. Simply use the definition of r.q.r. given by identity (2.1).

Application 2.2.5. Let R be a ring with 1 and M_R a f.g. module. If $(M/MJ)_R$ is cyclic then so is M_R.

Proof. $\exists m \in M$ s.t. $M/MJ = (mR + MJ)/MJ$. So $M = mR + MJ$ and this implies that $[M/mR]J = [M/mR]$ where M/mR is viewed as a right R-module. By Nakayama's Lemma, $[M/mR] = 0$. So $M \subseteq mR$. But clearly $mR \subseteq M$ thus M is cyclic i.e. $M = mR$. □

In particular, if J_R is f.g. then J/J^2 cyclic $\Rightarrow J$ principal.

2.3 Nil and Nilpotent subsets

Definition 2.3.1. Let $S \subseteq R$ be a non-empty subset of a ring R.

- S is said to be **nil** is $\forall s \in S, \exists k_s \in \mathbb{Z}, k_s \geq 1$ s.t. $s^{k_s} = 0$.
- S is said to be **nilpotent** if $\exists k \in \mathbb{Z}, k \geq 1$ s.t. $S^k = 0$. Where $S^k = \{\sum_{i=1}^{n} s_{i_1} \dots s_{i_k} \mid n \in \mathbb{N}, s_{i_j} \in S\}$.

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

If S consists of a single element then there is no difference between nil and nilotent. By convention we say nilpotent.

Proposition 2.3.2. *Let R be a ring with 1 Every nil one sided ideal lies inside $J(R)$.*

Proof. Let I be a nil right ideal and $x \in I$. Then $x^k = 0$ for some $k \geq 1$. We have $(1 - x)(1 + x + \dots + x^{k-1}) = 1$. Therefore x is r.q.r. and so by 2.1.5. $I \subseteq J(R)$. □

Remark. The above is also true for rings without 1.

Lemma 2.3.3. *Let R be a ring*

- *If I and K are nilpotent right ideals then so are $I + K$ and RI.*
- *Every nilpotent right ideal lies inside a nilpotent ideal.*

Proof. • Suppose that $I^m = 0$ and $K^n = 0$, $m, n \geq 1$. Consider $(I + K)^{m+n-1}$. A typical term of the expansion is of the form $X_1 \dots X_{m+n-1}$ where $X_i = I$ or K.

There are at lease m I's in this term of else there are at least n K's in it. Since $IK \subseteq I$ and $KI \subseteq K$, it follows that $X_1 \dots X_{m+n-1} = 0$. Thus $I + K$ is nilpotent.

$(RI)^m = (RI) \dots (RI) \subseteq R(IR)^{m-1}I \subseteq RI^m = 0$

- Let I be nilpotent right ideal. We have $I \subseteq I + RI$ and $I + RI$ is an ideal which is nipotent by the above.

□

Definition 2.3.4. The sum of all nilotent ideals of a ring R is called the **nilpotent radical** of R (older name: Wedderburn Radical). It is usually denoted $N(R)$. Note that $N(R) \subseteq J(R)$ always by 2.3.2. It follows from 2.3.3. that $N(R) = \sum$ nilpotent right ideals $= \sum$ nilpotent left ideals. Clearly $N(R)$ is a nil ideal but need not be nilpotent itself.

Exercise. Let n be a nilpotent element of a commutative ring. Show that the ideal generated by n is nilpotent.

Example 2.3.5 (Zassenhaus's)**.** Let F be a field, I the open interval $(0, 1)$ and R a vector space over F with basis $x_i \mid i \in I$.

Define multiplication on R by extending the following product of basis elements,

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

Now every element of R can be written uniquely in the form $\sum_{i\in I} a_i x_i$ where $a_i \in F$ and $a_i = 0$ for all but finitely many i. Check that R is nil but not nilpotent [3]. In fact $N(R) = R$ [4].

Proposition 2.3.6. *Let R be a commutative ring. Then $N(R)$ is the set of all nilpotent elements of R. (This is false for non-commutative rings).*

Proof. $n \in R$ nilpotent in a commutative ring R. Then [exercise] (n) is a nilpotent ideal. □

Example 2.3.7. 2.3.6. is false in general for non-commutative rings. Take $R = M_2(\mathbb{Q})$. 0 and R are the only ideals so $N(R) = 0$ (because $1 \in R$). However $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = 0$ so there are nilpotent elements not in $N(R)$.

Also note that $J(R) = 0$ but the above element is quasi-regular.

2.4 Prime and Semi-Prime Ideals

Let R be a commutative ring. $P \lhd R$, P is prime if $ab \in P, a, b \in R \Rightarrow a \in P$ or $b \in P$. We seek a definition for prime ideals for non-commutative rings. We would like a definition such that: 0 is a prime ideal for $\mathbb{Z}$ means 0 is a prime ideal for $M_2(\mathbb{Z})$.

Definition 2.4.1. An ideal P of a ring R is said to be a **prime ideal** if $AB \subseteq P,\ A, B \lhd R \Rightarrow A \subseteq P$ or $B \subseteq P$. We exclude R from the set of prime ideals.

Example. Let R be a ring with 1. Show that a maximal ideal is prime.

Proposition 2.4.2. *The following are equivalent for an ideal $P \neq R$ of R.*

1. *P is a prime ideal*
2. *$AB \subseteq P,\ A, B \lhd_r R \Rightarrow A \subseteq P$ or $B \subseteq P$*
3. *$CD \subseteq P,\ C, D \lhd_l R \Rightarrow C \subseteq P$ **or** $D \subseteq P$*
4. *$aRb \subseteq P,\ a, b \in R \Rightarrow a \in P$ or $b \in P$*

Proof. (2) ⇒ (1) trivial.

(1) ⇒ (4) Let $aRb \subseteq P$ with $a, b \in R$. Then $(RaR)(RbR) \subseteq RaRbR \subseteq RPR \subseteq P$. Now $RaR, RbR \lhd R$ so $RaR \subseteq P$ or $RbR \subseteq P$. WLOG, suppose $RaR \subseteq P$. Let $\langle a \rangle = \{\lambda a + ra + as + \sum_{\text{finite}} r_i a s_i \mid \lambda \in \mathbb{Z}, r, s, r_i, s_i \in R\} \lhd R$. Since $RaR \subset P$ then $\langle a \rangle^3 \subseteq P$, hence $\langle a \rangle \subseteq P$ so $a \in P$.

(4) ⇒ (2) Let $A, B \subseteq P$, $\quad A, B \lhd_r R$. Suppose that $A \not\subseteq P$ then $\exists a \in A$. Let $b \in B$. Then $aRb \subseteq P$ so by assumption $b \in P$ so $B \subseteq P$.

We have shown (2) ⇒ (1) ⇒ (4) ⇒ (2) and similarly we can show (3) ⇒ (1) ⇒ (4) ⇒ (3). □

[3] Proof. let $x = \sum_{i\in I} a_i x_i \in R$ suppose $k \in I$ is the smallest value s.t. $a_k \neq 0$. Then $x^{\lceil 1/k \rceil} = 0$ so R is nil. However for all $k \geq 1$, $x^k_{1/(k+1)} = x_{(1-1/k)} \neq 0$ so R is not nilpotent.

[4] Note that R is a commutative ring and so (x_i) is nilpotent for all $i \in I$ (by the exercise above). So $R \supseteq N(R) \supseteq \sum_{i\in I}(x_i) = R$ so $N(R) = R$

Definition 2.4.3. R is called a **prime** ring if 0 is a prime ideal of R. A commutative integral domain is a prime ring.

Corollary 2.4.4. *Let $P \neq R$ be an ideal of a commutative ring R then P is a prime ideal if and only if $ab \in P,\ a,b \in R \Rightarrow a \in P$ or $b \in P$.*

Let R be a commutative ring with 1 and $P \lhd R, P \neq R$ then, P is a prime ideal $\iff$ The ring R/P is an integral domain.

Example. $M_2(\mathbb{Z})$ is prime [Exercise].

Definition 2.4.5. Let R be a ring with 1 and (a_{ij}) an n by n matrix with $a_{ij} \in R$. Define the **matrix units** E_{ij} to be the matricies with 1 in the ij'th position and 0's everywhere else.

We have,

$$(a_{ij}) = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}E_{ij}$$

as a unique sum of E_{ij}'s. Multiplication of matrix units,

$$E_{ij}E_{kl} = \begin{cases} E_{il} & \text{if } j = k \\ 0 & \text{if } j \neq k \end{cases}$$

Theorem 2.4.6. *Let R be a ring with 1.*

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

Proof. 1. Trivial.

2. Let $X \lhd M_n(R)$, we have to show there exists an ideal I of R s.t. $X = M_n(I)$. Let $A = (a_{ij}) = \sum_{i,j} a_{ij}E_{ij} \in X$. Consider (fixed) α, β, $1 \leq \alpha, \beta \leq n$. We have X is an ideal so

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

hence

$$a_{\alpha\beta}E_{11} \in X \tag{2.2}$$

Now let I be the set of all elements of R which occur in the $1,1$ entry of the some matrix in X. We shall show that $I \lhd R$ and $X = M_n(I)$.

Let $a, b \in I$, it is easy to see that $a - b \in I$. Now let $a \in I$ and $r \in R$. Let a be the $1,1$ entry of $A = (a_{ij})$ then $(a_{ij}) = \sum_{i,j} a_{ij}E_{ij}$ with $a_{11} = a$. So $E_{11}(\sum_{i,j} a_{ij}E_{ij})(rE_{11}) \in X$. So $a_{11}rE_{11} \in X$ and hence $ar \in I$. Similarly on the left hand side, $(rE_{11}(\sum_{i,j} a_{ij}E_{ij})E_11) = ra_{11}E_{11} \in X$ So $I \lhd R$

Now $C = (c_{ij}) = \sum_{i,j} c_{ij}E_{ij} \in X$, $(c_{ij} \in R)$. Now by (2.2), each $c_{ij} \in I$ so $c \in M_n(I)$ hence $X \subseteq M_n(I)$.

Finally let $D = (d_{ij}) = \sum_{i,j} d_{ij}E_{ij} \in M_n(I)$. By definition of I, for each i, j: $d_{ij}E_{11} \in X$. So $E_{i1}(d_{ij}E_11)E_{1j} \in X$. So $d_{ij}E_{ij} \in X$. Hence $D \in X$ and so $M_n(I) \subseteq X$.

□

Remark. This works only for two-sided ideals. E.g. $X := \begin{bmatrix} 2\mathbb{Z} & 2\mathbb{Z} \\ 0 & 0 \end{bmatrix} \lhd_r M_2\mathbb{Z}$ but $X \neq M_2(I)$ for all $I \lhd_r \mathbb{Z}$

Exercise. 1. Let R be a ring with 1 and P a prime ideal of R. Show that $M_n(P)$ is a prime ideal of $M_n(R)$.

2. Let R be a ring with 1 and $I \lhd R$. Show that $M_n(R/I) \cong M_n(R)/M_n(I)$.

Corollary 2.4.7. *If R is a prime ring with 1 then so is the ring $M_n(R)$*

Proof. Follows from the above theorem. □

Definition 2.4.8. An **integral domain** is a ring R s.t. $ab = 0,\ a, b \in R \Rightarrow a = 0$ or $b = 0$.

For us an integral domain need not be commutative.

An integral domain is trivially a prime ring. A matrix ring over an integral domain is a prime ring. Thus $M_n(\mathbb{Z})$ is a typical example of a prime ring.

Definition 2.4.9. Let $I \neq R$ be an ideal of a ring R, I is said to be a **semi prime ideal** if $A^n \subseteq I,\ A \lhd R \Rightarrow A \subseteq I$.

R is called a **semi prime ring** if 0 is a semi prime ideal.

Thus R is semi prime ring $\iff$ R has no non-zero nilpotent ideal $\iff$ R has no non-zero nilpotent right ideal [left ideal] $\iff$ $N(R) = 0$.

Example.
- A prime ideal is semi prime and moreover:
- An arbitrary intersection of prime ideals of a ring is semi prime.

Thus is $\mathbb{Z}$, $6\mathbb{Z} = 2\mathbb{Z} \cap 3\mathbb{Z}$ is a semi prime ideal of $\mathbb{Z}$.

A result analogous to 2.4.2 can be proved for semi prime ideals [Exercise].

Proposition 2.4.10. *Let R be a ring. The intersection of all prime ideals of R is a nil ideal.*

Proof. If $x \in R$ is not nilpotent then we show there exists a prime ideal of R excluding it.

Let S be the collection of all ideals of R which contain no power of x. $S \neq \emptyset$ because $0 \in S$, since x is not nilpotent. Check that Zorn's Lemma applies[5]. So S contains a maximal element P say. Claim: P is prime. If not then there exists ideals A, B of R s.t. $AB \subseteq P$ but $A \not\subseteq P$ and $B \not\subseteq P$. So $P \subsetneq A + P$ and $P \subsetneq B + P$ so there exists integers m, n s.t. $x^m \in A + P$ and $x^n \in B + P$ by maximality of $P \in S$. But $x^{m+n} \in (A + P)(B + P) \subseteq P$. Contradiction. So P is prime. □

Exercise. Let R be the ring from Zassenhaus's example. Show that R cannot contain a prime ideal P.

Corollary 2.4.11. *Let R be a ring and assume that R has a prime ideal. Let X be the intersection of all prime ideals of R, then*

1. *$N(R) \subseteq X$, always.*
2. *$N(R) = X$, when R is commutative.*

Proof.
1. Easy.
2. By 2.4.6 $N(R)$ consists of all nilpotent elements of R, so by 2.4.10 $X \subseteq N(R)$.

□

2.5 Completely Reducible Modules

Definition 2.5.1. A right R-module M is said to be **irreducible** (or simple) if:

1. $MR = 0$
2. M contains no submodules other than 0 and M.

If R has 1 and M is unitial then (1.) is automatically satisfied.

Example 2.5.2.
1. If p is a prime in $\mathbb{Z}$, $\mathbb{Z}/p\mathbb{Z}$ is an irreducible $\mathbb{Z}$-module.
2. Every ring with 1 has an irreducible submodule because by 1.16.2 R contains a maximal ideal, M say. Then R/M is an irreducible right R-module.
3. Let V be a vector space over a field F. Then any 1-dimensional subspace is an irreducible F-module.

V has the following interesting property: V is the sum of irreducible submodules, i.e. 1-dimensional subspaces. Moreover this sum is direct, i.e. V has a basis. Over an arbitrary ring, not all modules have this property.E.g. $\mathbb{Z}/4\mathbb{Z}$ as a $\mathbb{Z}$-module. $2\mathbb{Z}/4\mathbb{Z}$ is the only non-zero submodule, so $\mathbb{Z}/4\mathbb{Z}$ is not the direct sum of irreducible submodules. We investigate modules which do have this property.

Definition 2.5.3. A module M is said to be **c.r. - completely reducible** (semi simple) if M is expressible as the sum of irreducible submodules.

[5] Let $\{T_a\}_{a\in A}$ be a totally ordered subset of S. Let $T = \bigcup_{a\in A} T_a$ then $T \in S$ since it contains no power of x and is an ideal of R. So $\{T_a\}_{a\in A}$ is bounded above by T. Since $T_a \subseteq T$ for all $a \in A$ we may apply Zorn's Lemma

Example. 1. Let F be a field. Then every non-zero F-module is c.r.

2. $\mathbb{Z}/6\mathbb{Z}$ is a c.r. $\mathbb{Z}$-module. It is $2\mathbb{Z}/6\mathbb{Z} \oplus 3\mathbb{Z}/6\mathbb{Z}$

Lemma 2.5.4. *Let M be a right R module s.t. $M = \sum_{\lambda\in\Lambda} M_\lambda$ where each M_λ is an irreducible submodule of M. Let K be a submodule of M, there exists a subset $\mu \subseteq \Lambda$ s.t. $M = K \oplus \sum_{m\in\mu} M_m$.*

sketch. Consider S the set of submodules $K + \sum_{\alpha\in A} M_\alpha$ s.t. the sum is direct, where $A \subseteq \Lambda$. Apply Zorn's Lemma (checking it's conditions) to obtain a maximal element of S say $X = K \oplus \sum_{m\in\mu} M_m$.

Claim: $X = M$. Choose $\lambda \in \Lambda$. We have either $X \cap M_\lambda = 0$ or M_λ by irreducibility of M_λ. If $X \cap M_\lambda = 0$ this contradicts maximality of X in S. So $X = M$. □

Proposition 2.5.5 (Dedekind Modular Law)**.** *Let A, B, C be submodules of M_R s.t. $B \subseteq A$. Then,*

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

Proof. Elementary. □

Theorem 2.5.6. *Let M be a non-zero right R-module. TFAE:*

1. *M_R is c.r.*
2. *M is a direct sum of irreducible submodules.*
3. *$mR = 0, m \in M \Rightarrow m = 0$ and every submodule of M is a direct summand of M.*

Proof. (1) ⇒ (2) Take $K = 0$ is 2.5.4.

(2) ⇒ (3) Suppose that $mR = 0$ for some $m \in M$. Let $M = \sum_{\lambda\in\Lambda} M_\lambda$, with M_λ irreducible. Then $m = m_1 + \dots m_k$ for some $m_i \in M_{\lambda_i}$. Now if $mr = 0$ for some $r \in R$ then, $m_1 r + \dots + m_k r = 0$. So $m_i r = 0$ for $i \in \{1, \dots, k\}$ since the sum of the M_λ is direct.

Define $K_j = \{x \in M_{\lambda_j} \mid xR = 0\}$. Then K_j is a submodule of M_{λ_j}. So $K_j = 0$ or $K_j = M_{\lambda_j}$ since M_{λ_j} is irreducible. But $K_j \neq M_{\lambda_j}$ since $M_{\lambda_j} R \neq 0$ by definition of irreducible. So $K_j = 0$ for $j = 1, \dots, k$ and hence $m_j = 0$ for $j = 1, \dots, k$. Thus $m = 0$. The second part follows from 2.6.4.

(3) ⇒ (1) First we aim to show that M has an irreducible submodule. Note that by the Dedekind mdoular law, the hypothesis on M is inherited by every submodule of M.

Let $0 \neq y \in M$, let S be the set of all submodules K of M s.t. $y \notin K$. $S \neq \emptyset$ since $0 \in S$. Partially order S by inclusion. Check that Zorn's Lemma applies here. So S contains a maximal element call it A. $A \neq M$ since $y \notin A$. By hypothesis there exists a submoldule $B \neq 0$ s.t. $M = A \oplus B$.

Claim: B is irreducible, $BR \neq 0$ by assumption. Suppose B contains a submodule B_1 s.t. $0 \subsetneq B_1 \subsetneq B$. Then there exists $B_2 \neq 0$ a submodule s.t. $B = B_1 \oplus B_2$. $y \in A \oplus B_1$ and $y \in A \oplus B_2$. By maximality of A in S, so $y \in (A \oplus B_1) \cap (A \oplus B_2) = A$. Contradiction. So no such B_1 can exist. So B is irreducible.

Let K be the sum of all irreducible submodules of M. If $K \neq M$, there exists a submodule $L \neq 0$ s.t. $M = K \oplus L$. As above, L contains an irreducible submodle of M. Contradiction. Since K contains all irreducible submodules of M. So $M = K$ and so M is c.r. □

Remark. The first condition of part (3) holds automatically when R has 1 and M is unitial.

Question. For which R ring is R_R c.r?

Example 2.5.7. When R_R and $_RR$ are c.r.

1. Let $R = M_n(D)$, a matrix ring over a division ring. Here R_R and $_RR$ are c.r.

   Proposition. *Let $E_{ij}, 1 \leq i, j \leq n$ be the matrix units of R. Consider $I_j = E_{jj}R$, then I_j is a right ideal of R.*

$$I_j = \left\{ \begin{pmatrix} 0 \\ \star \cdots \star \\ 0 \end{pmatrix} \in R \;\middle|\; \textit{non-zero entries lie on the jth row} \right\}$$

   I_j is an irreducible right R-module

Proof. Suppose $0 \subsetneq X \subseteq I_j$ where $X \triangleleft_r R$. Then X has a non-zero matrix, $A = (a_{\alpha\beta})$ say. A must have a non-zero entry and since $A \in I_j$, we must have $a_{jk} \neq 0$ for some k. Let B be the matrix with a_{jk}^{-1} in the kj^{th} position and 0 everywhere else. Then $AB = E_{jj}$, so $E_{jj} \in X$. SInce $A \in X$ and $X \triangleleft_r R$ thus $E_{jj}R \subseteq X \subseteq I_j = E_{jj}R$. So $X = E_{jj}$. Also $I_jR \neq 0$ since $1 \in R$. Thus each I_j is an irreducible right R-module.

Now $R = I_1 \oplus \cdots \oplus I_n$. So R is c.r. Similarly for ${}_RR$, here the irreducible ideals are columns. □

2. Let $R = R_1 \oplus \cdots \oplus R_m$ a direct sum of rings, where $R_i = M_{n_i}(D_i)$ for D_i division rings and n_i positive integers. Again R_R and ${}_RR$ are c.r.

Proof. Since $R_i \triangleleft R$ each R_i can be considered as an R_i-module or an R-module. Further the R-submodules and R_i-submodules coincide: (Note: $R_iR_j = 0$ if $i \neq j$)

Now by part (1), each R_i is a sum of irreducible R_i-submodules. SO R_i is a sum of irreducible R-submodules so R is the sum of irreducible R-submodules. □

Later we will show that if R has 1 and R_R is c.r. then R is necessarily of this form. As a consequence we will have: R_R is c.r. $\iff$ ${}_RR$ is c.r.

2.6 Idempotent Elements

Definition 2.6.1. An element $e \in R$ is called an **idempotent element** if $e^2 = e$

Example 2.6.2. 1. 0 and 1 are idempotent elements

2. In $\tilde{\mathbb{Z}} = \mathbb{Z}/6\mathbb{Z}$, $\bar{3}, \bar{4}$ are idempotent

3. In $M_2(\mathbb{Z})$, $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ are idempotent.

Lemma 2.6.3. *Let R be a ring and let $e \in R$ be idempotent. Then $R = eR \oplus K$ where $K = \{x - ex \mid x \in R\} \triangleleft_r R$.*

Proof. Clearly eR and K are right ideals of R. Let $x \in R$, then $x = ex + (x - ex) \in eR \oplus K$. Let $z \in eR \cap K$ then $z = ea = b - eb$ for some $a, b \in R$. $ea = e^2a = eb - e^2b = eb - eb = 0$ so $z = 0$. And so $eR \cap K = \{0\}$ and the sum is direct. □

Corollary 2.6.4 (Peirce Decomposition)**.** *Let R be a ring with 1. $e \in R$ an idempotent element, then $R = eR \oplus (1 - e)R$*

Proof. By the previous lemma, for a ring R with 1 we have $K = (1 - e)R$. □

Proposition 2.6.5. *Let R be a ring with 1. Suppose that $R = I_1 \oplus \cdots \oplus I_n$ a direct sum of right ideals. Then we can write $1 = e_1 + \cdots + e_n$ with $e_j \in I_j$ then the e_j's have the following properties*

1. *each e_j is idempotent*
2. *$e_ie_j = 0$ if $i \neq j$*
3. *$I_j = e_jR$*
4. *$R = Re_1 \oplus \cdots \oplus Re_n$*

Proof. (1) and (2). For each j we have, $e_j = 1e_j = e_1e_j + \cdots + e_{j-1}e_je_j^2 + e_{j+1}e_j + \cdots + e_ne_j$. So

$$e_j - e_j^2 = e_1e_j + \cdots + \hat{e_je_j} + \cdots + e_ne_j \in I_j \cap (\sum_{s \neq j} I_s) = 0$$

Hence $e_j = e_j^2$. Also notice that each term e_ie_j belongs to $I_i \cap I_j$ so must be zero because R is a direct sum of I_j's.

(3) and (4), exercise. □

Example 2.6.6. Let $R = M_n(\mathbb{Z})$, take e_j to be the matrix with 1 in the jj^{th} position and 0 everywhere else. Then $1 = e_1 + \cdots + e_n$ and $R = e_1R \oplus \cdots \oplus e_nR$.

e_jR is the set of matrices whose non-zero entries lie in the j^{th} row. Similarly Re_j is the set of matrices whose non-zero entries lie in the j^{th} column.

Definition 2.6.7. Let R be a ring, define $C(R) = \{x \in R \mid xr = rx, \forall r \in R\}$ called the **centre** of R, it is a subring of R. In general it is not an ideal.

Lemma 2.6.8. *Let $I \triangleleft R$ be an ideal with $I = eR = Rf$ where $e = e^2, f = f^2$. Then*

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

Proof. 1. $e = e^2$ so $e = af$ for some $a \in R$. $e = af = af^2 = (af)f = ef$. $f = f^2$ so $f = eb$ for some $b \in R$. $f = eb = e^2b = e(eb) = ef$. So $e = ef = f$.

2. $x \in I \Rightarrow x = e\alpha = \beta e$ for some $\alpha, \beta \in R$. Hence $ex = x = xe$
3. Exercise [6]

□

Proposition 2.6.9. *Let R be a ring with 1. Suppose that $R = A_1 \oplus \cdots \oplus A_k$ a direct sum. Let $1 = e_1 + \cdots + e_k$ with $e_i \in A_i$. Then*

1. *$e_j \in C(R)$ for $i = 1, \ldots, k$*
2. *$e_j^2 = e_j, \forall j,\ e_ie_j = 0, \forall i \neq j$*
3. *$A_j = e_jR + Re_i, j = 1, \ldots, k$*
4. *e_j is the identity for the ring A_j.*

Proof. Follows from 2.6.5 and 2.6.8 □

2.7 Annihilators and Minimal Right Ideals

Definition 2.7.1. Let S be a non-empty subset of M_R. We define the **right annihilator of** S to be $r(S) = \{r \in R \mid Sr = 0\}$. For left modules the **left annihilator** $l(S)$ is defined analogously.

Clearly $r(S) \triangleleft_r R, l(S) \triangleleft_l R$. In most applications, S is a sunset of R itself do we can consider both $r(S)$ and $l(S)$.

A right ideal I is said to be an **annihilator right ideal** or simply a **right annihilator** if $I = r(S)$ for some subset S of R. Similarly for **left annihilators**.

Definition 2.7.2. A non-zero right ideal M of R is said to be **minimal right ideal** if $M' \subsetneq M, M' \triangleleft_r R \Rightarrow M' = 0$. If R has 1, minimal right ideals of R are precisely the irreducible submodules of R_R.

Lemma 2.7.3. *Let M be a minimal right ideal of a ring R then either, $M^2 = 0$ or $M = eR$ for some $e = e^2 \in M$.*

Proof. Suppose that $M^2 \neq 0$, then $\exists a \in M$ s.t. $aM \neq 0$. Now $aM \triangleleft_r R$ and $aM \subseteq M$. Since $a \in M$ hence $aM = M$ thus $\exists e \in M$ s.t. $ae = a$. In particular $e \neq 0$. Also $a = ae = ae^2$. So $a(e - e^2) = 0$. Thus $e - e^2 \in M \cap r(a)$. Now $M \cap r(a) \triangleleft_r R$ and $M \cap r(a) \subseteq M$ so $M \cap r(a) = 0$ or $M \cap r(a) = M$.

If $M \cap r(a) = M$ then $M \subseteq r(a)$ so $aM = 0$. Contradiction.

Thus $e - e^2 = 0$ and $e = e^2$. Now $0 \neq e = e^2 \in eR$, so $eR \neq 0$. But $eR \triangleleft_r R$ and $eR \subset M$ since $e \in M$. Thus $M = eR$. □

Example 2.7.4. Take $R = \begin{bmatrix} \mathbb{Q} & \mathbb{Q} \\ 0 & \mathbb{Q} \end{bmatrix}$. Let $M_1 = \begin{bmatrix} 0 & \mathbb{Q} \\ 0 & 0 \end{bmatrix}$ and $M_2 = \begin{bmatrix} 0 & 0 \\ 0 & \mathbb{Q} \end{bmatrix}$. Both M_1 and M_2 are minimal right ideals of R. $M_1^2 = 0$ and $M_2^2 = M_2 = eR$ where $e = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$. We also have $M_1 \cong M_2$ as right R-modules.

[6] let $x \in R$ and consider $ex - xe \in eR$. Since e is the identity of eR, $ex - xe = e(ex - xe)e = e^2xe - exe^2 = exe - exe = 0$ so $ex = xe$.

2.8 Homomorphisms of Irreducible Modules

Proposition 2.8.1. *Let M, K be right R-modules and $\theta : M \to K$ a non-zero R-module homomorphism.*

1. *If M is irreducible then θ is a monomorphism.*
2. *If K is irreducible then θ is an epimorphism.*
3. *If M, K are irreducible then θ is an isomorphism.*

Proof. Note that $Im(\theta)$ and $Ker(\theta)$ are submodules of K and M respectively. The results follow easily from this fact. □

If $\theta : M \to M$ is an isomorphism then the inverse map (as a set theoretic map) θ^{-1} is also an isomorhism. Moreover $\theta\theta^{-1} = \theta^{-1}\theta = 1_M$ the identity map on M.

Corollary 2.8.2 (Schur's Lemma)**.** *If M_R is irreducible then $\mathcal{E}_R(M)$ is a division ring.*

Proof. By the above, every non-zero element of $\mathcal{E}_R(M)$ is an isomorphism. □

Definition 2.8.3. Let R be a ring, the **right socle** $E(R)$ is defined,

$$E(R) := \begin{cases} \text{The sum of all minimal right ideals of } R & \text{if } R \text{ has any} \\ 0 & \text{if } R \text{ has none} \end{cases}$$

The **left socle** $E'(R)$ is defined similarly.

Proposition 2.8.4. $E(R) \triangleleft R$

Proof. Trivial if $E(R) = 0$.

Suppose $E(R) \neq 0$. Let M be a minimal right ideal of R and $x \in R$. Then the map $\theta : m \to xm,\ m \in M$ shows that either $sM = 0$ or $xM \cong M$ and so xM is a minimal right ideal hence $xm \in E$. It follows that $E(R) \triangleleft_l R$ and so $E(R) \triangleleft R$. □

$$E(M_R) := \begin{cases} \text{sum of all irreducible submodules} & \text{if } M \text{ has any} \\ 0 & \text{otherwise} \end{cases}$$

Chapter 3

Chain Conditions

3.1 Introduction

Definition 3.1.1. Let S be a non-empty collection of submodules M_R.

1.
   - An element $K \in S$ is said to be **maximal** in S if there does not exist $K' \in S$ with $K \subsetneq K'$.
   - Similarly for **minimal** element.

2. M_R is said to have the **ascending chain condition (ACC)** for submodules in S if every increasing chain of submodules $A_1 \subseteq A_2 \subseteq \ldots,\ A_i \in S$ has equal terms after a finite number of terms. i.e. $\exists n \geq 1$ s.t. $A_n = A_{n+1} = \ldots$.

3. M_R is said to have the **maximum condition** on submodules in S if every non-empty subcollection of submodules in S has a submodule maximal in that subcollection.

The **descending chain condition** and **minimum condition** are defined similarly.

Proposition 3.1.2. *Let S be a non-empty collection submdoules of M_R. Then TFAE:*

1. *M has ACC [DCC] on submodules in S.*

2. *M has the maximum [minimum] condition on submodules in S.*

Proof. Exercise. □

We shall be applying the above in particular when S is the set of all right annihilators of a ring.

The statement *M has ACC* means M has ACC on the set of all submodules of M. Similarly for DCC.

Proposition 3.1.3. *TFAE for M_R*

1. *M_R has ACC*

2. *M_R has the maximum condition*

3. *Every submodule of M_R is finitely generated.*

Proof. Exercise or see *Rings and Modules Prop. 5.3* □

Example 3.1.4. $\mathbb{Z}_\mathbb{Z}$ has ACC since every ideal of $\mathbb{Z}$ is principle.

Remark. ACC does not imply the existence of an integer n s.t. all chains have stopped at the n^{th} step

Proposition 3.1.5. *Let K be a submodule of M_R then M has ACC [DCC] if and only if both K and M/K have ACC [DCC].*

Proof. (⇒) Clear.

(⇐) Let $M_1 \subseteq M_2 \subseteq \dots$ be an ascending chain of submodules. Consider the chains $M_1 \cap K \subseteq M_2 \cap K \subseteq \dots$ and $M_1 + K \subseteq M_2 + K \subseteq \dots$.

The first chain stops since it consists of submodules in K, so $\exists k \geq 1$ s.t. $M_k \cap K = M_{k+i} \cap K$, $\forall i \in \mathbb{N}$.

The second chain stops since it consists of submodules which are in 1-1 correspondence with those in M/K so $\exists l \geq 1$ s.t. $M_l + K = M_{l+i} + K$, $\forall i \in \mathbb{N}$. Let $n = \max\{k, l\}$. Then by the Dedekind Modular Law, $M_{n+i} = M_{n+i} \cap (M_{n+i} + K) = M_{n+i} \cap (M_n + K) = M_n + (M_{n+i} \cap K) = M_n + (M_n \cap K) = M_n$, $\forall i \in \mathbb{N}$. Thus M has ACC. Simiarly for DCC. □

This proposition has many useful consequences.

Corollary 3.1.6. *Let $M_1, \dots, M_n$ be submodules of M_R. If each M_i has ACC [DCC] then so does their sum $K = M_1 + \dots + M_n$.*

Proof. By induction on n. If $n = 1$ then it is clear. Assume that $L = M_1 + \dots M_{n-1}$ has ACC. $K/L = (L + M_n)/L \cong M_n/(L \cap M_n)$ by the second isomorphism theorem. K/L has ACC since $M_n/(L \cap M_n)$ is a factor of M_n which has ACC. Since L has ACC by hypothesis so K has ACC. Similarly for DCC. □

Corollary 3.1.7. *Let R be a ring with 1 and ACC [DCC] on right ideals. Let M_R be a (unitial) finitely generated module. Then M_R has ACC [DCC] on submodules*

Proof. Since M is unitial and finitely generated, $\exists m_1, \dots, m_k \in M$ s.t. $M = m_1R + \dots + m_nR$. By 3.1.6 it is enough to show m_iR has ACC [DCC] on submodules. Let $\theta_i : R \to m_iR$ be the map given by $\theta_i(r) = m_ir, r \in R$. Then θ_i is an R-homomorphism from R_R onto m_iR. So $m_iR \cong R_R/Ker(\theta_i)$. Since R has ACC on submodules it follows that each m_iR has ACC on submodules. Similarly for DCC. □

Remark. Suppose we try to extend the above result when R does not have 1: For ACC the result still holds. For DCC the result is false.

Corollary 3.1.8. *If R has ACC [DCC] on right ideals then so does the ring $M_n(R)$.*

Proof. Consider $M_n(R)$ as a right R-module. Let T_{ij} be the set of all matrices in $M_n(R)$ with 0's everywhere except possibly in the ij^{th} place. Then each T_{ij} is an R-submodule of $M_n(R)$ and clearly $T_{ij} \cong R_R$. Each T_{ij} has ACC [DCC] on R-submodules but $M_n(R) = \sum_{i,j} T_{ij}$. By 3.1.6 $M_n(R)$ has ACC [DCC] on R-submodules. But clearly a right ideal of $M_n(R)$ is an R-submodule so $M_n(R)$ has ACC [DCC] on right ideals. □

- A module with ACC on submodules is called a **Noetherian module**.
- A module with DCC on submodules is called an **Artinian module**.
- A ring with ACC on right ideals is called a **right Noetherian ring**.
- A ring with 1 and DCC on right ideals is called **right Artinian ring**

Similarly for **left Noetherian** and **left Artinian**.

Let $R[x]$ be a the ring of polynomials in x with coefficients from R. When multiplying two polynomials we assume that x commutes with elements of R. We shall state without proof the following,

Theorem 3.1.9 (Hilbert Basis Theorem)**.** *If R is a right Noetherian ring with 1 then so is $R[x]$. (Proof is given in Rings and Modules 5.10)*

3.2 Composition Series

Neither ACC or DCC acting alone lead to an integer n s.t. all chains stop after n steps. However the two chain conditions together do guarantee the existence of such an integer.

Definition 3.2.1. A module M is said to have **finite length** if there exists a chain of submodules,

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

such that no submodule can be properly inserted between M_i and M_{i+1}. If R has 1 and M is unitial then this means M_i/M_{i+1} is irreducible.

(3.1) is called a **composition series** for M_R. The factor modules M_i/M_{i+1} are called **factors** of the composition series. k is called the length of the series.

Two composition series,

$$M = M_0 \supsetneq \cdots \supsetneq M_s = 0$$

$$M = K_0 \supsetneq \cdots \supsetneq K_t = 0$$

are said to be **equivalent** if $s = t$ and there exists a permutation $\pi : \{0, 1 \ldots, s-1\} \to \{0, 1 \ldots, s-1\}$ s.t

$$M_i/M_{i+1} \cong K_{\pi(i)}/K_{\pi(i)+1}, \text{ for } 0 \leq i \leq s-1$$

Example 3.2.2.

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

and

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

are two equivalent composition series for $(\mathbb{Z}/6\mathbb{Z})_{\mathbb{Z}}$.

Lemma 3.2.3. *M_R has a composition series if and only if M_R has ACC and DCC on submodules.*

Proof. ($\Leftarrow$) The obvious approach works.

($\Rightarrow$) By induction on k, the least length of a composition series for M.

If $k = 1$, M has no submodules other than $0 \subsetneq M$. So M has both ACC and DCC.

We assume the result for all modules with shortest composition series whose length is $k-1$. Let $M = M_0 \supsetneq \cdots \supsetneq M_k = 0$ be a shortest length composition series for M. Then clearly $M_1 \supsetneq \cdots \supsetneq M_k = 0$ is a shortest length composition series for M_1. By the induction hypothesis M_1 has both ACC and DCC. By of course M_0/M_1 has both ACC and DCC so by 3.1.5 M has both ACC and DCC. □

Lemma 3.2.4. *Let M_R be a module with has a composition series. Then any other series can be refined to a composition series by inserting extra terms as necessary.*

Proof. Let $M = A_0 \supsetneq A_1 \supsetneq \cdots \supsetneq A_k = 0$ be a series of submodules of M. By 3.2.3 M has both ACC and DCC. Choose a submodule B_1 with $A_0 \supseteq B_1 \supsetneq A_1$ s.t. B_1 is minimal over A_1. If $A_0 \neq B_1$ choose B_2 s.t. $A_0 \supseteq B_2 \supsetneq B_1$ and B_2 is minimal over B_1. By ACC this process must stop, thus we obtain a chain between A_0 and A_1 which cannot be lengthened. Repeat this between A_i and A_{i+1} to obtain a composition series. □

Theorem 3.2.5 (Jordan-Holder)**.** *Any two composition series are equivalent for a module of finite length.*

Proof. For a module of finite length, let $\lambda(M)$ be the length of a shortest composition series for M. By induction on $\lambda(M)$.

If $\lambda(M) = 1$ then the theorem holds trivially.

Now assume that the result holds for modules X_R s.t. $\lambda(X) \leq s-1$. Now suppose that M has a shortest composition series

$$M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_s = 0 \tag{3.1}$$

thus $\lambda(M) = s$. Let,

$$M = K_0 \supsetneq K_1 \supsetneq \cdots \supsetneq K_n = 0 \tag{3.2}$$

be another composition series for M. Since M_{s-1} and we either have $M_{s-1} = K_{n-1}$ or $M_{s-1} \cap K_{n-1} = 0$.

- Case 1: $M_{s-1} = K_{n-1}$. In this case he have,

$$M/M_{s-1} = M_0/M_{s-1} \supsetneq M_1/M_{s-1} \supsetneq \ldots M_{s-2}/M_{s-1} \supsetneq M_{s-1}/M_{s-1} = 0 \tag{3.3}$$

  similarly,

$$M/M_{s-1} = K_0/M_{s-1} \supsetneq K_1/M_{s-1} \supsetneq \ldots K_{s-2}/M_{s-1} \supsetneq K_{s-1}/M_{s-1} = 0 \tag{3.4}$$

  These are two composition series for M/M_{s-1} and clearly $\lambda(M/M_{s-1} = s-1$ By induction hypothesis, $n-1 = s-1$ i.e. $s = n$ and 3.3 and 3.4 are equivalent. It follows (by the third isomorphism theorem) that 3.1 and 3.2 are equivalent.

- Case 2: $M_{s-1} \cap K_{n-1} = 0$. So $M_{s-1} + K_{n-1}$ is a direct sum. By 3.2.4 we can construct a composition series,

$$0 \subsetneq M_{s-1} \subsetneq M_{s-1} \oplus K_{n-1} \subsetneq Q_{t-3} \subsetneq \cdots \subsetneq Q_0 = M \tag{3.5}$$

By case 1, s = t and 3.5 is equivalent to 3.1. Now consider,

$$0 \subsetneq K_{n-1} \subsetneq M_{s-1} \oplus K_{n-1} \subsetneq Q_{t-3} \subsetneq \cdots \subsetneq Q_0 = M \tag{3.6}$$

By inspection 3.6 is a composition series and is equivalent to 3.5. By case 1, $n = t$ and is equivalent to 3.2.

So $s = t = n$ and 3.1 is equivalent to 3.2.

□

3.3 Nil implies Nilpotent Theorems

Recall $N(R) = \sum$ nilpotent ideals. So $N(R)$ is nil (and in general not nilpotent E.g. Zassenhaus's example).

Let R be a ring and M a minimal right ideal of R. Then it is easy to check that $MJ = 0$, where $J = J(R)$. In particular $l(J) \neq 0$.

Theorem 3.3.1. *Let R be a ring with DCC on right ideals. Then $J(R)$ is nilpotent.*

Proof. The chain $J \supseteq J^2 \supseteq \dots$, stops. So $\exists k$ s.t. $J^k = J^{k+1}$. In particular $l(J^k) = l(J^{k+1})$. Let $\bar{R}$ be the ring $R/l(J^k)$ and let bars denote images in $\bar{R}$. Clearly $\bar{J}$ is r.q.r ideal in $\bar{R}$ so $\bar{J} \subseteq J(\bar{R})$.

Suppose that $\bar{R}$ is a non-zero ring. Then by DCC $\bar{R}$ contains a minimal right ideal so by the comment above, there exists $\bar{0} \neq \bar{x} \in \bar{R}$ s.t. $\bar{x}\bar{J} = \bar{0}$ so in R we have $xJ \subseteq l(J^k)$. So $xJ^{k+1} = 0$ and so $x \in l(J^{k+1}) = l(J^k)$. Thus $\bar{x} = \bar{0}$. Contradiction.

Hence $\bar{R}$ must be the zero ring. So $R \subseteq l(J^k)$, thus $J^{k+1} = 0$ (in fact $J^k = 0$ if R has 1) and J is nilpotent. □

Corollary 3.3.2 (Hopkins)**.** *Nil one sided ideals are nilpotent in a ring with DCC on right ideals.*

Proof. Nil one sided ideals lie in $J(R)$. □

Lemma 3.3.3 (Utumi - 1963)**.** *Let R be a ring with ACC on right annihilators. If R has a non-zero nil one sided ideal then R contains a non-zero nilpotent right ideal.*

Proof. Suppose first that R contains a non-zero nil left ideal A. Let $r(a)$ be maximal in the set $\{r(y) \mid 0 \neq y \in A\}$.

Claim: $aRa = 0$.

Let $t \in R$. If $ta = 0$ then $ata = 0$. Now assume $ta \neq 0$. Then there exists an integer $k > 1$ s.t. $(ta)^k = 0$ and $(ta)^{k-1} \neq 0$ since $ta \in A$ which is nil. So $ta \in r[(ta)^{k-1}]$. But clearly $r[(ta)^{k-1}] \supseteq r(a)$. By maximality of $r(a)$, we must have $r[(ta)^{k-1})] = r(a)$. so $ta \in r(a)$ and thus $ata = 0$.

This gives $(a)^3 = 0$ where (a) is the right ideal generated by $a \neq 0$. Now suppose that we have $0 \neq B \triangleleft_r R$ with B nil. If $B^2 = 0$ then we are done. (B is non-zero nilpotent right ideal). If not there exists $b \in B$ s.t. $Bb \neq 0$. Thus $Rb \neq 0$. Now Rb is a nil left ideal. Take $A = Rb$ and we are done by the first part. □

Lemma 3.3.4. *Let R be a ring with ACC on right ideals then R contains a unique maximal (among the nilpotent ideals) nilpotent ideal N and N contains all nilpotent one-sided ideals of R.*

Proof. Exercise □

Theorem 3.3.5 (Lentzki)**.** *Let R be a ring with ACC on right ideals. Then nil one-sided ideals of R are nilpotent.*

Proof. By 3.3.4 R has a unique maximal nilpotent ideal N say. Suppose that R has a nil one-sided ideal X s.t. $X \not\subseteq N$. Then $X + N/N$ is a non-zero nil one-sided ideal of the right Noetherian ring R/N. By 3.3.3 R/N contains a non-zero nilpotent right ideal, I say. But then for some k, $I^k \subseteq N$. But for some $\tilde{k}$, $I^{k\tilde{k}} \subseteq N^{\tilde{k}} = 0$ so $I \subseteq N$. So I was 0 in R/N. Contradiction. □

Chapter 4

Semi-simple Artinian Rings

4.1 Idempotent Generators of Right Ideals

Definition 4.1.1. A ring with no non-zero nilpotent right ideals and DCC on right ideals is called a **semi-simple Artinian ring**.

Note that by 2.3.3 part 2 and symmetry, a ring contains no non-zero nilpotent right ideal or left ideal.

Remark.

1. The left-right symmetry of semi-simple Artinian rings will be established later
2. We shall justify the use of the term *Artinian* by showing the existence of an identity.
3. We shall not define *semi-simple* on its own but in general the term can be interpreted in two different ways
   (a) direct sum of simple rings .
   (b) J(R) = 0. Sometimes called Jacobson semi-simple.

Recall that is M is a minimal right ideal the n either $M^2 = 0$ or $M = eR$, $e^2 = e$. However our definition of semi-simple Artinian rings ensures $M^2 \neq 0$.

Proposition 4.1.2. *Let R be a semi-simple Artinian ring and I a right ideal of R. Then $I = eR$ for some $e = e^2 \in I$.*

Proof. Trivial for $I = 0$.

Assume that $I \neq 0$. Claim: $\exists e = e^2 \in I$ s.t. $I \cap r(e) = 0$.

By the minimum condition, every non-zero right ideal contains a minimal right ideal so by 2.7.3 each contains a non-zero idempotent. Let E be the set of non-zero idempotents in I. By the above $E \neq \emptyset$. Suppose that the claim is false. Let $I \cap r(a)$ be minimal in the set $S = \{I \cap r(x) \mid x \in E\}$. By assumption $I \cap r(a) \neq 0$. So by the above $I \cap r(a)$ contains a non-zero idempotent, b say. We have $b^2 = b$ and $ab = 0$. Now consider $c = a + b - ba$. Then $c \in I$ since $a, b \in I$ we have $ca = (a + b - ba)a = a \neq 0$. In particular $c \neq 0$. $cb = (a + b - ba)b = b$ hence $c^2 = c(a + b - ba) = ca + cb - cba = a + b - ba = c$ thus $c \in E$.

We shall show $I \cap r(c) \subsetneq I \cap r(a)$ for a contradiction. Let $t \in I \cap r(c)$ so $ct = 0$ and $act = 0$. Then $a(a + b - ba)t = 0$ and so $at = 0$ and $t \in I \cap r(a)$. $b \in I \cap r(a)$ but $b \notin I \cap r(c)$ since $cb = b \neq 0$. Thus we get the contradiction to the minimality of $I \cap r(a)$.

So $\exists e \in E$ s.t. $I \cap r(e) = 0$. For $x \in I$, $x - ex \in I \cap r(e) = 0$ so $x = ex$, $\forall x \in I$. Since $I \lhd_r R$, thus $I = eR$ with $e = e^2 \in I$. □

Corollary 4.1.3. *Let R be a semi-simple Artinian ring and $A \lhd R$. Then $\exists e = e^2 \in A$ s.t. $A = eR = Re$.*

Proof. By 4.1.2, $A = eR$ for some $e = e^2 \in A$ since A is a right ideal of R. Let $K = \{x - ex \mid x \in A\}$, then $K \lhd_l R$ since $A \lhd_l R$. We have $Ke = 0$ and so $KeR = 0$. Hence $K^2 = 0$ since $K \subseteq eR = A$. Now $K = 0$ since R contains no non-zero nilpotent left ideals. So $x = ex$, $\forall x \in A$. Hence $A \subseteq Re$, but $Re \subseteq A$ as $e \in A$ and $A \lhd_l R$. Thus $A = eR = Re$ with $e = e^2$. □

Corollary 4.1.4. *A semi-simple Artinian ring has an identity.*

Proof. Take $A = R$ in 4.1.3 □

Theorem 4.1.5. *TFAE for a ring R*

1. *R is a semi-simple Artinian ring*

2. *R has 1, R_R is c.r.*

Proof. (1) $\Rightarrow$ (2) By 4.1.4 R has 1. Let $I \lhd_r R$, by 4.1.2 $I = eR$ for some $e = e^2 \in I$. So by Peirce Decomposition 2.6.4 I is a direct summand in R. So every submodule of R_R is a direct summand of R_R. So by 2.5.6, R_R is c.r.

(2) $\Rightarrow$ (1) We have $R = \sum_{\lambda \in \Lambda} I_\lambda$, where each I_λ is an irreducible submodule of R_R. Then $1 = x_1 + \dots x_n$ for some $x_i \in I_{\lambda_i}$. Now for any $r \in R$, $r = 1.r = x_1 r + \cdots + x_n r \in I_{\lambda_1} \oplus \cdots \oplus I_{\lambda_n}$. So $R = I_{\lambda_1} \oplus \cdots \oplus I_{\lambda_n}$ and Λ is a finite set. R has DCC on right ideals by 3.6.1 since each right submodule I_{λ_i} is irreducible and trivially has DCC. Now let T be a nilpotent right ideal of R. Then $R = T \oplus K$ for some $K \lhd_r R$ by 2.5.6. So $1 = t + k$ for some $t \in T$ and $k \in K$. Now t is nilpotent so $t^m = 0$ for some $m \geq 1$ and so $(1-k)^m = 0$. So $1 - mk + \cdots \pm k^m = 0$. So $1 = mk - \cdots \mp k^m \in K$. So $1 \in K$ and $K = R$ Thus $T = 0$ and R is a semi-simple Artinian ring. □

Corollary 4.1.6. *Let R be a semi-simple Artinian ring then $R = I_1 \oplus \cdots \oplus I_n$ where each I_j is a minimal right ideal.*

Proof. This is done in the above proof. □

Corollary 4.1.7. *A direct sum of matrix rings over division rings is a semi-simple Artinian ring.*

Proof. We showed in 2.5.7 that for such a ring R_R is c.r. □

4.2 Ideals in Semi-Simple Artinian Rings

Proposition 4.2.1. *Let R be a semi-simple Artinian ring, then*

1. *Every ideal of R is generated by an idempotent which lies in $C(R)$, the centre of R.*

2. *There is a 1-1 correspondence between ideals of R and idempotents in $C(R)$.*

Proof.

1. See 4.1.3 and 2.6.8 part 3.

2. For $e = e^2 \in C(R)$ define $f(e) = eR \lhd R$. Check that f is the required bijection.

□

Definition 4.2.2. An ideal I of R is said to be a **minimal ideal** if $I \neq 0$ and $I' \subseteq I$ with $I' \lhd R \Rightarrow I' = 0$.

Theorem 4.2.3. *Let R be a semi-simple Artinian ring. Then R has a finite number of minimal ideals, their sum is direct and moreover it is R.*

Proof. Every non-zero ideal of R contains a minimal ideal by the minimum condition. Let S_1 be a minimal ideal of R, then by 4.2.1, $S_1 = e_1 R = R e_1$ where $e_1^2 = e_1 \in C(R)$. So $(1-e_1)^2 = 1 - e_1 \in C(R)$. We have a direct sum of ideals, $R = S_1 \oplus T_1$ where $T_1 = (1-e_1)R = R(1-e_1)$

If $T_1 \neq 0$, T_1 contains a minimal ideal of R, S_2 say. As above $R = S_2 \oplus K$ for some $K \lhd R$. Now $T_1 = T_1 \cap R = T_1 \cap (s_2 \oplus K) = S_2 \oplus (T_1 \cap K)$ by Dedekind Modular Law. Let $T_2 = T_1 \cap K$ then we have $T_1 = S_2 \oplus T_2$.

If $T_2 \neq 0$ then proceed as before and continue this process. We have $T_1 \supsetneq T_2 \supsetneq \dots$ so by DCC this must stop. It can only stop when $T_m = 0$ for some m and at this stage we have $R = S_1 \oplus \cdots \oplus S_m$ as a direct sum of minimal ideals.

Now let S be a minimal ideal of R. $SR = 0$ since R has 1. So $SS_j \neq 0$ for some $1 \leq j \leq m$. Now SS_j is an ideal of R and also $SS_j \subseteq S$ and $SS_j \subseteq S_j$. Since S, S_j are minimal we have $S = SS_j = S_j$. □

4.3 Simple Artinian Rings

Definition 4.3.1. R is said to be a **simple** ring if 0 and R are the only ideals of R.

Remark. A commutative simple ring is a field.

Let R be a simple ring. Consider $R^2 \lhd R$. Either $R^2 = 0$ or $R^2 = R$.

Suppose $R^2 = 0$. Then $xy = 0, \forall x, y \in R$. So any additive subgroup of R is an ideal of R. So the additive subgroup of R has no subgroup other than 0 and R. Hence the additive group of R must be a cyclic group of prime order p. So we have determined the complete structure of R.

$$R = 0, 1, \ldots, p-1$$

where addition is $\mod (p)$ and multiplication of any two elements is 0. Thus when studying simple rings we assume $R^2 = R$. (Of course $R^2 = R$ when R has 1 as in the case of semi-simple Artinian rings). Thus $N(R) = 0$ in this case.

A simple ring with DCC on right ideals will be called a **simple Artinian ring**. Thus a simple Artinian ring is also a semi-simple Artinian ring.

Lemma 4.3.2. *Let R be a semi-simple Artinian ring and let I be a non-zero ideal of R. Then I itself is a semi-simple Artinian ring. In particular when I is a minimal ideal, I is a simple Artinian ring.*

Proof. Consider I as a ring itself. Claim: $K \lhd_r I \Rightarrow K \lhd_r R$.

By 4.1.3 we have $I = eR = Re$ with $e = e^2 \in I$. Now let $k \in K$ and $r \in R$. $kr = (ke)r$, since e is the identity of I. So $kr = k(er) \in K$ since $k \in K$, $er \in I$ and K is a right ideal of $I = eR$. So K is an ideal of R.

It follows that I has DCC on its right ideals and $N(I) = 0$. If I is minimal then by the above it must be simple Artinian. (Note that I is a ring with identity) □

Theorem 4.3.3. *Let R be a semi=simple Artinian ring then R is expressible as a finite direct sum of simple Artinian rings and this expression is unique.*

Proof. By 4.2.3 we have,

$$R = S_1 \oplus \cdots \oplus S_m$$

where S_i is a minimal ideals. Hence these are simple Artinian by 4.3.2. Uniqueness follows from 4.2.3. □

4.4 Artin Wedderburn Theorem

Check section 1.14 - Handout 1. It is routine to check that if $A_R \cong B_R$ then $\mathcal{E}_R(A) \cong \mathcal{E}_R(B)$ as rings. Recall also 1.14.1, for a ring R with 1, $R \cong \mathcal{E}_R(R_R)$ as rings.

Given X_R, let $X^{(n)}$ denote $X \oplus \cdots \oplus X$ - n-times.

Lemma 4.4.1. $\mathcal{E}_R(X^{(n)}) \cong M_n(\mathcal{E}_R(X))$ *as rings.*

Proof. See - Handout 3. □

Theorem 4.4.2 (Artin-Wedderbrun)**.**

$$R \textit{is a semi-simple Artinian ring} \iff R = S_1 \oplus \cdots \oplus S_m$$

where $S_i \cong M_{n_i}(D_i)$ for positive integers n_i and division rings D_i.

Proof. ($\Rightarrow$) $R = S_1 \oplus \cdots \oplus S_m$ where each S_i is simple Artinian by 4.3.3. $S_i = I_1 \oplus \cdots \oplus I_{n_i}$ a direct sum of minimal right ideals for some integers n_i by 4.1.6. But $I_j \cong I_k, \forall j, k$ by Example Sheet 5 Qu. 2. So we have $S_i \cong I_1 \oplus \cdots \oplus I_1$ - n_i-times.

Now $S_i \cong \mathcal{E}_S(S_{iS_i}) \cong M_{n_i}(\mathcal{E}_S(I_1)) = M_{n_i}(D_i)$, where $D_i = \mathcal{E}_S(I_1)$ is a division ring by Schur's Lemma 2.8.2.

($\Leftarrow$) Done by 2.5.7. □

Theorem 4.4.3. *A semi-simple Artinian ring is left-right symmetric*

Proof. Right hand conditions $\iff$ R is a direct sum of matrix rings over division rings $\iff$ Left hand conditions □

Another proof of symmetry is given in Example sheet 6, Qu. 5.

4.5 Right Artinian Rings are Right Noetherian

Lemma 4.5.1. *Let R be a right Artinian right and $N = N(R)$. Then the ring R/N is a semi-simple Artinian ring.*

Proof. By Hopkin's 3.3.2, N is nilpotent. It follows that R/N is semi-simple Artinian. □

Theorem 4.5.2. *Let R be a semi-simple Artinian ring and M_R a non-zero (unitial) module. then M_R is c.r.*

Proof. We have $R = I_1 \oplus \cdots \oplus I_n$ is a direct sum of minimal right ideals by 4.1.6. let $m \in M$, then $m = m1 \in mI_1 + \cdots + mI_n$. Each mI_j is either 0 or irreducible. Thus each $m \in M$ lies in a sum of irreducible submodules. Hence M is c.r. □

Consider M_R and let K be a submodule. Then M/K is naturally an R-module. Suppose that $I \triangleleft R$.

Question. Is M an R/I-module?

Yes, if $MI = 0$. In this case we can define $m[x + I] = mx,\ m \in M, x \in R$.

Recall from 1.13, if M is a right R-module, $I \triangleleft R$ s.t. $MI = 0$. Then M is also a right R/I-module and R-submodules of M coincide with the R/I-submodules.

Theorem 4.5.3 (Hopkins)**.** *A right Artinian ring is right Noetherian*

Proof. Let $N = N(R)$ by 4.5.1 R/N is semi-simple Artinian. By 3.3.2 there exists a smallest integer $k \geq 1$ s.t. $N^k = 0$. Consider the chain:

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

Let $N^0 := R$. Each N^j/N^{j+1} is unitial right R/N-module for each j. By 4.5.2 N^j/N^{j+1} is c.r. Since N^j/N^{j+1} is an Artinian right module, it must be a *finite* direct sum of irreducible submodules. So by 3.1.6 each N^j/N^{j+1} is a Noetherian right module for each j. Thus in particular N^{k-1} and N^{k-2}/N^{k-1} are Noetherian. So N^{k-2} has ACC as a right R-module. Proceed in this way, R_R has ACC as required. □

Corollary 4.5.4. *A f.g. right module M over a right Artinian right has a composition series.*

Proof. R has both ACC and DCC. □

Recap.

- R is semi-prime + DCC ⇒ Artin-Wedderburn
- R is semi-prime + DCC (+1) ⇒ ACC
- R is semi-prime + ACC ⇒ ?

Chapter 5

Quotient Rings

5.1 Definitions and Elementary Properties

Definition 5.1.1. 1. An element $c \in R$ is said to be,

- **right regular** if $r(c) = 0$
- **left regular** if $l(c) = 0$
- **regular** if $l(c) = r(c) = 0$

2. A ring Q is called a **quotient ring** if it has 1 and every regular element of Q is a unit in Q. Example: A division ring is a quotient ring.

Proposition 5.1.2. *Let Q be a right Artinian ring and let $c \in Q$ s.t. $r(c) = 0$. Then c is a unit. In particular Q is a quotient ring.*

Proof. Exercise. □

Definition 5.1.3. 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} with $a, c \in R$ and c regular

Recall an easy example. Let D be a commutative integral domain. Then it has a field of fractions F.

Note that if Q is a right quotient ring of R then Q is a quotient ring as defined at the start of this chapter.

Example 5.1.4. $\mathbb{Q}$ is a quotient ring (field) of $\mathbb{Z}$, $2\mathbb{Z}$ and $\mathbb{Z}_{(p)} := \{\frac{a}{c} \mid a, c \in \mathbb{Z}, p \nmid c\}$.

A **left quotient ring** is defined analogously.

Definition 5.1.5. A ring R is said to be a **right order** in Q if Q is a right quotient ring R.

Lemma 5.1.6. *Suppose that R has a right quotient ring Q. Let $c_1, \ldots, c_n$ be regular elements. Then there exists $r_q, \ldots, r_n, c \in R$ with c regular s.t.*

$$c_i^{-1} = r_i c^{-1}$$

for each i.

Remark. Compare this to finding a common denominator c for a set of fractions in $\mathbb{Q}$

Proof. By induction on n. For $n = 1$, take $r_1 = c_1$ and $c = c_1^2$.

Now assume that we have obtained $t_1, \ldots, t_n, d$ with d-regular s.t. $c_i^{-1} = t_i d^{-1}$ for each i. Consider $d^{-1}c_n$, since Q is a right quotient ring for R we have $d^{-1}c_n = rr_n^{-1}$ for some $r, r_n \in R$ with r_n regular. So $c_n r_n = dr = c$ say, then c is regular in R and $c_i^{-1} = t_i d^{-1} = ti(rc^{-1}) = r_i c^{-1}$, where $r_i = t_i r \in R$ for each i. Also $c_n^{-1} = r_n c^{-1}$ □

Proposition 5.1.7. *let R be a ring with a right quotient ring Q. Then,*

1. *If $I \lhd_r R$ then $IQ \lhd_r Q$ and every element of IQ is expressible as xc^{-1} with $x \in I$, c regular in R.*
2. *If $K \lhd_r Q$ then $K \cap R$ is a right ideal of R and $(K \cap R)Q = K$.*

Proof. 1. Clearly $IQ \lhd_r Q$. A typical element of IQ is

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

with $t_i \in I, q_i \in Q$.

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

with $a_j, c_j \in R$ and c_j regular. By 5.1.6 there exists $r_1, \ldots, r_k, c \in R$ with c regular s.t. $c_j^{-1} = r_j c^{-1}$ for each j. So,

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

for some $x \in I$.

2. Exercise

□

Corollary 5.1.8. *Suppose that R has a right quotient ring Q. If R is right Noetherian then so is Q.*

Proof. Follows from part 2 above. □

Lemma 5.1.9. *Let R_1 and R_2 be rings with right quotient rings Q_1 and Q_2 respectively. Suppose that $R_! \cong R_2$ then $Q_1 \cong Q_2$.*

Proof. Let θ be the isomorphism between R_1 and R_2. A typical element of Q_1 is ac^{-1} with $a, c \in R$ and c regular. Define

$$\bar{\theta} : Q_1 \to Q_2$$

$$\bar{\theta}(ac^{-1}) = \theta(a)[\theta(c)]^{-1}$$

note that $\theta(c)$ is regular in R_2. We must check this map is well defined. Suppose that $ac^{-1} = bd^{-1}$ for some $a, b, c, d \in R$, c, d regular. Then $ac^{-1}d = b$. Now $c^{-1}d = ef^{-1}$ for some $e, f \in R$, f regular. So $\theta(d)\theta(f) = \theta(c)\theta(e)$. Note that $\theta(f)$ and $\theta(c)$ are regular in R_2. So we have,

$$[\theta(c)]^{-1}\theta(d) = \theta(e)[\theta(f)]^{-1} \tag{5.1}$$

but $b = aef^{-1}$ so $bf = ae$ and $\theta(b)\theta(f) = \theta(a)\theta(e)$. So, $\theta(b) = \theta(a)\theta(e)[\theta(f)]^{-1}$. So by 5.1 , $\theta(a)[\theta(c)]^{-1}\theta(d) = \theta(b)$. Thus $\theta(a)[\theta(c)]^{-1} = \theta(b)[\theta(d)]^{-1}$.

Similarly for the other conditions for $\bar{\theta}$ □

Corollary 5.1.10. *The right quotient ring is unique in the sense that, if R has a right quotient ring Q_1 and Q_2 then the identity map on R can be extended to a ring isomorphism between Q_1 and Q_2.*

Proof. Take $\theta = Id : R \to R$ □

Hence we may speak of *the* right quotient ring of R.

5.2 The Ore Condition

Review.

- Let R be a commutative integral domain. To construct a field of fractions considered the set of ordered pairs $[a, c], c \neq 0$.
- First we turn this set into a ring by introducing addition and multiplication

$$[a, c] + [b, d] = [ad + bc, cd]$$

$$[a, c][b, d] = [ab, cd]$$

- Then define an equivalence relation $[a, c] \sim [b, d] \iff ad = bc$

- define $a/c :=$ the equivalence class of $[a, c]$
- check the operations are well defined on the equivalence classes.

Definition 5.2.1. Let S be a non-empty subset of a ring R. S is said to be **multiplicatively closed** if $s_1, s_2 \in S \Rightarrow s_1 s_2 \in S$.

We say R has the **right Ore Condition w.r.t** S if given $a \in R, s \in S, \exists a_1 \in R, s_1 \in S$ s.t. $as_1 = sa_1$.

Intuition: Let R be a ring with right quotient ring Q and let $a, c \in R$, c regular. Then $c^{-1}a = a_1 c_1^{-1}$ for some $a_1, c_1 \in R$, c_1 regular. Then the Ore Condition is,

$$ac_1 = ca_1$$

Lemma 5.2.2. *Let S be a multiplicatively closed subset of R and suppose that S consists of regular elements of R. Suppose that R has a right Ore condition w.r.t S. Let $(x, c), (y, d)$ and $(r, s) \in R \times S$ s.t.*

- $cr = ds$
- $xr = ys$

Then, $ca = db \Rightarrow xa = yb$ for all $a, b, \in R$.

Proof. Since R has the right Ore condition w.r.t S, $\exists(\lambda, \mu) \in R \times S$ s.t. $b\mu = s\lambda$. Now $ca\mu = db\mu = ds\lambda = cr\lambda$. So $a\mu = r\lambda$ since $r(c) = 0$. Hence $xa\mu = xr\lambda = ys\lambda - yb\mu$. So $xa = yb$ since $l(\mu) = 0$. ☐

Remark. Observe that we need both left and right regularity of elements of S.

Theorem 5.2.3 (Ore's)**.** *Let R be a ring with at least one regular element. Let S be the set of all regular elements of R. Then R has a right quotient ring $Q \iff R$ has the right Ore condition w.r.t S.*

Proof. ($\Rightarrow$) Let $a, c \in R$ with c regular. Then $c^{-1}a \in Q$ so $\exists a_1, c_1 \in R$ with c_1 regular s.t. $c^{-1}a = a_1 c_1$ by the definition of right quotient ring. So $ac_1 = ca_1$ and R has the right Ore condition w.r.t S.

($\Leftarrow$) Define an equivalence class on $R \times S$ as follows, $(x, c) \sim (y, d) \iff \exists(r, s) \in R \times S$ s.t. $cr = ds$ and $xr = ys$. To check that $\sim$ is an equivalence relation:

- Reflexive: $(x, c) \sim (x, c)$, clear.
- Symmetric: Suppose that $(x, c) \sim (y, d)$. Then by the right Ore condition $\exists(r_1, s_1) \in R \times S$ s.t. (i) $dr_1 = cs_1$. Since $(x, c) \sim (y, d)$, $\exists(r, s) \in R \times S$ s.t. (ii) $cr = ds$ and $xr = ys$. By 5.2.2, (i) and (ii) imply that (iii) $yr_1 = xs_1$. Thus $(y, d) \sim (x, c)$ by (i) and (iii).
- Transitive: Suppose that $(x, c) \sim (y, d)$ and $(y, d) \sim (z, e)$. By the right Ore condition $\exists(r, s) \in R \times S$ with $cr = es$. Also $\exists(r_2, s_2) \in R \times S$ s.t. $dr_2 = (es)s_2$. By 5.2.2, this gives $yr_2 = xrs_2$. Again by 5.2.2 and $dr = ess_2$ gives us $yr_2 = zss_2$. So $xrs_2 = yr_2 = zss_2$. Hence $xr = zs$ since S_2 is regular. Thus $(x, c) \sim (z, e)$.

Denote the equivalence class of (x, c) under $\sim$ by x/c. Denote,

$$Q = \left\{ \frac{x}{c} \mid (x, c) \in R \times S \right\}$$

We shall now define ring operations on Q s.t. Q becomes the right quotient ring of R. Given x/c and y, d define

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

where $(r, s) \in R \times S$ is s.t. $cr = ds$.

We must check that $+$ is well defined. So suppose $(x, c) \sim (x', c')$ and $(y, d) \sim (y', d')$. By the right Ore condition $\exists(r', s') \in R \times S$ s.t. $c'r' = d's'$. Again $\exists(\rho, \sigma) \in R \times S$ s.t. $ds\rho = d's'\sigma$. By 5.2.2 we have $ys\rho = y's'\sigma$. Now $cr\rho = ds\rho = d's'\sigma = c'r'\sigma$ So by 5.2.2, $xr\rho = x'r'\sigma$. Thus $(xr + ys)\rho = xr\rho + ys\rho = x'r'\sigma + y's'\sigma = (x'r' + y's')\sigma$. Thus $+$ is well defined.

Proceeding with similar techniques it can be shown that $(Q, +)$ is an abelian group. Next given x/c and $y/d \in Q$ define,

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

where $(\lambda, \mu) \in R \times S$ is s.t. $y\mu = c\lambda$. It can be shown that this is also well defined and that $(Q, +, \cdot)$ is a ring. ☐

5.3 Integral Domains

Definition 5.3.1. A module M_R is said to be **finite (Goldie) dimensional** if it does not contain an infinite direct sum of non-zero submodules.

Artinian and Noetherian modules are finite dimensional. R is called a **right finite dimensional ring** if R_R is finite dimensional.

Lemma 5.3.2. *Let R be a ring and let $c \in R$ s.t. $r(c) = 0$. Let $I \triangleleft_r R$ s.t. $cR \cap I = 0$. Then $I + cI + c^2I + \dots$ is a direct sum.*

Proof. Exercise. □

Recall that for us an integral domain need *not* be commutative. It is easy to see that if an integral domain has a right quotient ring D then it must be a division ring. (Exercise)

Theorem 5.3.3. *Let R be an integral domain. Then R has a right quotient division ring $\iff$ R_R is finite dimensional.*

Proof. ($\Rightarrow$) Let I, K be right ideals of R. Let $0 \neq a \in I, 0 \neq c \in K$. By the right ore Condition there exists $a_1, c_1 \in R$ with $c_1 \neq 0$ s.t. $ac_1 = ca_1$. Thus $0 \neq ac_1 = ca_1 \in I \cap K$. Hence R_R cannot contain an infinite direct sum. (Above we showed that any two ideals intersect non-trivially)

($\Leftarrow$) let $a, c \in R$ with $c \neq 0$. If $a = 0$ then we have $ac = ca$ so assume $a \neq 0$. Then $aR \neq 0$ by 5.3.2 $aR \cap cR \neq 0$. Hence $\exists a_1, c_1 \in R$ with $c_1 \neq 0$ s.t. $ac_1 = ca_1$. So by Ore's Theorem, R has a right quotient ring which must be a division ring. □

Remark. 1. Commutative integral domains satisfy the above condition.

2. The above theorem is a special case of Goldie's Theorem.

Recall, if K is a field them the commutative ring $K[x]$ is a PID. (By the Euclidean Algorithm)

Example 5.3.4 (G. Higman)**.** There exists an integral domain which has a quotient ring on the left by not on the right. Let F be a field with a monomorphism $F \to F : a \to \bar{a}$, which is not an automorphism. (Exercise: find such a field and monomorphism). let $\bar{F} = \{\bar{a} \mid a \in F\}$. Then $\bar{F} \neq F$. taking x to be an indeterminate over F, let $F[x]$ be the ring of polynomials $\{a_0 + a_1x + \dots + a_kx^k \mid k \geq 0, a_i \in F\}$ where multiplication is defined by, $xa = \bar{a}x, a \in F$ and the distributive laws.

It can be checked that,

1. R is an integral domain (degree argument).

2. R has the Euclidean Algorithm so that every left ideal of R is principal (The argument does not work on the right.)

So by 5.3.3 R has left quotient division ring.

However R does not have the right Ore condition w.r.t non-zero elements. Consider $x+a, x^2 \in R$ with $a \in F \backslash \bar{F}$. Suppose there exits polynomials f, g s.t. $(x+a)f(x) = x^2g(x)$. So $(x+a)(b_0+b_1x+\dots b_kx^k) = x^2(c_0 + c_1x + \dots + c_{k-1}x^{k-1})$ where $b_i, c_j \in F$. So, $ab_0 + (\bar{b}_0 + ab_1)x + \dots + (\bar{b}_{k-1} + ab_k)x^k + \bar{b}_kx^{k+1} = \bar{\bar{c}}_0x^2 + \bar{\bar{c}}_1x^3 + \dots + \bar{\bar{c}}_{k-1}x^{k+1}$. So $\bar{b}_k = \bar{\bar{c}}_{k-1}$ and so $b_k = \bar{c}_{k-1} \in \bar{F}$. Now $\bar{b}_{k-1} + ab_k = \bar{\bar{c}}_{k-1}$. This will give $a \in F$ unless $b_k = 0$. Hence $b_{k-1} = \bar{\bar{c}}_{k-2} \in \bar{F}$.

We continue in this way and force each $b_i = 0$. So $f(x) = g(x) = 0$. So R does not have the right Ore condition.

Remark. 1. The ring $R \oplus R^{\text{op}}$ will have a quotient ring on neither side.

2. In fact, Malcev has constructed an integral domain which is not embeddable in *any* division ring.

Proposition 5.3.5. *If R has a left quotient ring Q' and a right quotient ring Q then Q is also a left quotient ring of R and $Q \cong Q'$.*

Proof. Consider the arbitrary element $ac^{-1} \in Q$ where $a, c \in R$, c regular. Since R has the left Ore condition we have $c_1a = a_1c$ for some $a_1, c_1 \in R$ with c_1 regular. So $ac^{-1} = c_1^{-1}a_1 \in Q$ thus Q is a left quotient ring of R. By 5.1.10 $Q \cong Q'$. □

Chapter 6

Goldie's Theorems

6.1 The Singular Submodule

Definition 6.1.1. A submodule E of M is said to be **essential** in M if $E \cap K \neq 0$ whenever K is a non-zero submodule of M. Every non-zero ideal of a commutative integral domain is essential.

Lemma 6.1.2. *Let E be an essential submodule of M_R. Let $a \in M$ and define $F = \{r \in R \mid ar \in E\}$. Then F is also an essential right ideal.*

Proof. It is clear that $F \triangleleft_r R$. Let $0 \neq I \triangleleft_r R$. If $aI = 0$ then $I \subseteq F \cap I$ and so $F \cap I \neq 0$. Now assume $aI \neq 0$. Then aI is a non-zero submodule of M. Hence $aI \cap E \neq 0$. So $\exists x \in E, t \in I$ s.t. $0 \neq x = at$. Hence $0 \neq t \in F \cap I$ and thus $I \cap F \neq 0$ □

Proposition 6.1.3. *let M_R be a right module, define $Z(M) = \{m \in M \mid mE = 0$, some essential right ideal E of R $\}$. Then $Z(M)$ is a submodule of M.*

Proof. Let us check that $m_1 - m_2 \in Z(M)$ for $m_1, m_2 \in Z(M)$. This is easy.

Let $m \in Z(M), a \in R$ there exists an essential right ideal E s.t. $mE = 0$. Define $F = \{r \in R \mid ar \in E\}$. By 6.1.2 applied to R_R and E, F is an essential right ideal in R. Now $maF \subseteq mE = 0$ hence $ma \in Z(M)$. Thus $Z(M)$ is a submodule of M. □

Definition 6.1.4. $Z(M)$ define above is called the **singular submodule** of M. $Z(R_R)$ is clearly an ideal, it is called the **right singular ideal of** R.$Z'(R)$ the left singular ideal is defined analogously.

In general $Z(R) \neq Z'(R)$.

Lemma 6.1.5. *Let R be a ring with ACC on right annihilators. Then,*

1. *Z(R) is a nil ideal*
2. *If further R is semi-prime then $Z(R) = 0$.*

Proof. Let $z \in Z := Z(R)$. Claim: $\exists n \geq 1$ s.t. $z^n R \cap r(z^n) = 0$. The chain $r(z) \subseteq r(z^2) \subseteq \dots$ stops so $\exists n \geq 1$ s.t. $r(z^n) = r(z^{n+1}) = \cdots = r(z^{2n})$. Let $y \in z^n R \cap r(z^n)$. Then $y = z^n t$ for some $t \in R$ and $z^n y = 0$. $z^{2n} t = 0$ and $t \in r(z^{2n}) = r(z^n)$ hence $y = z^n t = 0$. So we have showed the claim.

But $z^n \in Z$ since $Z \triangleleft R$. hence $r(z^n)$ is essential. it follows that $z^n R = 0$ so $z^{n+1} = 0$ and Z is a nil ideal.

Part 2 follows from Utumi's lemma 3.3.3 □

Lemma 6.1.6. *Let R be a right finite dimensional ring and $c \in R$ s.t. $r(c) = 0$, then cR is an essential right ideal.*

Proof. Since R_R is finite dimensional, $cR \cap I \neq 0$ for any non-zero right ideal by 5.3.2 □

Definition 6.1.7. R is called a **right Goldie ring** if R is finite dimensional and R has ACC on right annihilators.

A commutative integral domain is trivially a Goldie Ring. A right Noetherian ring is a Goldie ring.

Proposition 6.1.8. *Let R be a semi-prime right Goldie ring, then $r(c) = 0 \Rightarrow l(c) = 0$*

Proof. By 6.1.6 cR is essential. By 6.1.5 part 2, $Z(R) = 0$ it follows that $l(c) = 0$. □

Remark. condition for $l(c) \not\Rightarrow$ condition for $r(c)$ in the above ring.

6.2 Goldie's Theorem

Proposition 6.2.1. *Every essential right ideal of a semi-prime right Goldie ring contains a regular element.*

Proof. Let E be an essential right ideal of R. Then by 3.3.3 E is not nil. Choose $x_1 \in E$ s.t. $r(x_1)$ is maximal in $\{r(x) \mid 0 \neq x \in E, x \text{ not nilpotent}\}$. Then $r(x_1) = r(x_1^2)$.

- If $E \cap r(x_1) = 0$ then $r(x_1) = 0$. So by 6.1.6, $x_1 \in E$ is a regular element.
- If $E \cap r(x_1) \neq 0$ then as above $E \cap r(x_1)$ is not nil. Choose $x_2 \in r(x_1) \cap E$ s.t. $r(x_2)$ is maximal in the set $\{r(x) \mid 0 \neq x \in E \cap r(x_1)\}$. Then $r(x_2) = r(x_2^2)$.

Claim: $r(x_1 + x_2) = r(x_1) \cap r(x_2)$.

Clearly $r(x_1) \cap r(x_2) \subseteq r(x_1 + x_2)$ and if $(x_1 + x_2)y = 0, y \in R$ then $x_1 y = -x_2 y$, so $x_1^2 y = -x_1 x_2 y = 0$ and so $y \in r(x_1^2) = r(x_1)$. Hence $x_1 y = x_2 y = 0$, proving the claim.

The same argument shows that $x_1 R + x_2 R$ is direct. If $r(x_1 + x_2) \neq 0$ then $E \cap r(x_1 + x_2) \neq 0$. Now choose $x_3 \in E \cap r(x_1 + x_2)$ and this process repeats. $r(x_1 + x_2 + x_3) = r(x_1) \cap r(x_2) \cap r(x_3)$ and $x_1 R + x_2 R + x_3 R$ is a direct sum.

Since R is finite dimensional this procedure cannot continue indefinitely. Thus we obtain, $c = x_1 + \dots x_n$ s.t. $c \in E$ and $r(C) = 0$. By 6.1.8 c is a regular element. □

Lemma 6.2.2. *If K is a nilpotent ideal then $l(K)$ is essential as a right ideal.*

Proof. Let $0 \neq I \lhd_r R$. If $IK = 0$ then $0 \neq I \subseteq I \cap l(K)$. Otherwise $\exists n \geq 1$ s.t. $IK^n = 0$ but $IK^{n-1} \neq 0$. then $0 \neq IK^{n-1} \subseteq I \cap l(K)$. So $l(K)$ is essential. □

Lemma 6.2.3. *let R be a ring with right quotient ring Q. Then,*

1. *If E is an essential right ideal of R then EQ is an essential right ideal of Q.*
2. *If F is an essential right ideal of Q then $F \cap R$ is an essential right ideal of R.*

Proof. Exercise. □

Theorem 6.2.4 (Goldie's - 1960)**.** *The ring R has a semi-prime Artinian right quotient ring $\iff$ R is a semi-prime right Goldie ring.*

Proof. ($\Leftarrow$) Let $a, c \in R$ with c regular. By 6.1.6 cR is essential in R. Let $F = \{r \in R \mid ar \in cR\}$. Then $F \lhd_r R$. By 6.1.2 F is essential, so by 6.2.1 F contains a regular element c_1 say. So $ac_1 = ca_1$ for some $a_1 \in R$. Thus by ore's Theorem R has a right quotient ring Q say. Let G be an essential right ideal of Q. By 6.2.3 $G \cap R$ is an essential right ideal of R. By 6.2.1 $G \cap R$ contains a regular element. So G contains a unit of Q hence $G = Q$. Thus by Exercise sheet 2 Qu. 7, every right ideal of Q is a direct summand of Q. Also Q has 1 so Q is semi-simple Artinian.

($\Rightarrow$). let E be an essential right ideal of R. By 6.2.3 EQ is an essential right ideal of Q. But Q is semi-simple Artinian so $EQ = Q$. So $1 \in EQ$ hence $1 = xc^{-1}$ for some $x \in E$ and $c \in R$ with c regular. So $c = x \in E$. Thus every essential right ideal of R contains a regular element. Let K be a nilpotent ideal of R, by 6.2.2 $l(K)$ is an essential right ideal of R and so contains a regular element. Thus $K = 0$ and R is semi-prime.

We need to show the right Goldie condition. It is easy to see that direct sums in R extend to direct sums in Q. Thus R_R is finite dimensional. Finally for any annihilator right ideal $r_R(T)$ for some $T \subseteq R$, we have

$$r_R(T) = r_Q(T) \cap R \tag{6.1}$$

Now Q has ACC on right ideals (Check this - See section on *idempotent Generation*). Hence by 6.1, R has ACC on right annihilators. □

Remark. This proof was due to Goldie - 1967

Summary:

- Q semi-simple + DCC on right ideals $\Rightarrow$ Q is semi-simple Artinian, $Q = \bigoplus_i M_{n_i}(D_i)$
- R semi-prime + ACC on right annihilators $\Rightarrow$ R has right quotient ring Q and Q is semi-simple Artinian.

6.3 The Prime Case

Lemma 6.3.1. *Let R be a ring with right quotient ring Q. Suppose that Q is right Noetherian. Then $A \triangleleft R \Rightarrow AQ \triangleleft Q$.*

Proof. It is clear that $AQ \triangleleft_r Q$. Let c be a regular element of R. Consider the chain $AQ \subseteq c^{-1}AQ \subseteq c^{-2}AQ \subseteq \ldots$, which is a chain of right idels in Q. Since Q is right Noetherian this chain stops so there exists $k \geq 1$ s.t. $c^{-k}AQ = c^{-(k+1)}AQ$ so $AQ = c^{-1}AQ$. It follows that AQ is a left ideal of Q thus $AQ \triangleleft R$. □

Theorem 6.3.2 (Goldie - 1958)**.** *The ring R has a simple Artinian right quotient ring $\iff$ R is a prime right Goldie ring.*

Proof. ($\Leftarrow$) By 6.2.4, R has a semi-simple Artinian right quotient ring Q. Let $AB = 0$ with $AB \triangleleft Q$ then $(A \cap R)(B \cap R) = 0$ in R. So $A \cap R = 0$ or $B \cap R = 0/$ Hence $A = (A \cap R)Q = 0$ or $B = (B \cap R)Q = 0$. Thus Q is a prime ring. By Exercise sheet 6 Qu. 1, Q is simple Artinian.

($\Rightarrow$) By 6.2.4, R is a semi-prime right Goldie ring. Let $AB = 0$ where $A, B \triangleleft R$ and $B \neq 0$. By 6.3.1, $BQ \triangleleft Q$, so $BQ = Q$ since Q is simple. Hence $0 = AB = ABQ = AQ$. Thus $A = 0$ and R is a prime ring. □

Chapter 7

The Jacobson Problem (Conjecture)

Assume that all rings in this chapter have 1.

7.1 The commutative case

Primary Decomposition.

Definition 7.1.1. Let $I \triangleleft R$, then I is said to be **meet-irreducible** if $I = A \cap B$ with $A, B \triangleleft R \Rightarrow I = A$ or $I = B$.

Proposition 7.1.2. *Let R be a ring with ACC on ideals. Then every ideal of R is expressible as a finite intersection of meet-irreducible ideals.*

Proof. Suppose not. By ACC, there exists a maximal counterexample $I \triangleleft R$ not meet-irreducible. So there exists ideals $A, B \in R$ s.t. $I = A \cap B$ with $A \supsetneq I$ and $B \supsetneq I$. Since I is a maximal counterexample, both A and B are finite intersections of meet-irreducible ideals. Hence so is I. Contradiction. Hence no such counterexample exists. □

For this section we make the additional assumption that all rings are commutative.

Definition 7.1.3.
- An ideal Q of R is said to be **primary** if, $ab \in Q, a, b \in R \Rightarrow a \in Q$ or $b^n \in Q$ for some $n \geq 1$.
- Clearly a prime ideal is primary.
  If $R = F[x]$, F a field then x^2R is primary.
- R is called a **primary ring** if 0 is a primary ideal.
- R is said to have a **primary decomposition** if every ideal of Example: R is a finite intersection of primary ideals.
- $Q \triangleleft R$. Note Q is primary $\iff$ R/Q is a primary ring.

Theorem 7.1.4 (Noether)**.** *Every Noetherian ring has a primary decomposition.*

Proof. By 7.1.2, it is enough to show that a meet-irreducible is primary. WLOG assume that 0 is meet-irreducible. Let $ab = 0$, $a, b \in R$. Then by Fitting's Lemma 6.1.5 $\exists n \geq 1$ s.t. $b^nR \cap r(b^n) = 0$. Since 0 is meet-irreducible either; $b^nR = 0$ or $ann(b^n) = 0$. Thus $b^n = 0$ or $a = 0$. So 0 is a primary ideal. □

Definition 7.1.5. Let Q be a primary ideal. Let P/Q be the nilpotent radical of the ring R/Q. Then P is called the **radical** of Q and Q is called **P-primary**. We denote the radical of Q by $\sqrt{Q}$.

Recall that in a commutative ring, $N(R)$ is the set of all nilpotent elements. It is easy to see that a finitely generated nil ideal in a commutative ring is nilpotent.

Proposition 7.1.6. *Let Q be a primary ideal and $P = \sqrt{Q}$.*

1. *P is a prime ideal*
2. *If further R is Noetherian then $P^k \subseteq Q$ for some $k \geq 1$.*

Proof.
1. Let $ab \in P$ with $a, b \in R$ then $(ab)^n \in Q$ for some $n \geq 1$. So $a^n b^n \in Q$, if $a \notin P$ then $a^n \notin Q$. So $(b^n)^s \in Q$ for some $s \geq 1$ by definition of primary. Thus $b \in P$ and P is a prime ideal.

2. P/Q is a finitely generated nil ideal of R/Q hence is nilpotent.

□

Theorem 7.1.7. *Let R be a commutative Noetherian ring. Let $J := J(R)$. Then,*

$$\bigcap_{n=1}^{\infty} J^n = 0$$

Proof. Let $X = \bigcap_{n=1}^{\infty} J^n$. Let $XJ = Q_1 \cap \cdots \cap Q_n$, with $P_i = \sqrt{Q_i}$ be a primary decomposition. By 7.1.6 part 2, $\exists k_i \geq 1$ s.t. $P_i^{k_i} \subseteq Q_i$. Now suppose $X \nsubseteq Q_i$ then $J \subseteq P_i$ since Q_i is P_i-primary. But $X \subseteq J^{k_i}$ so $X \subseteq Q_i$ for each i. So $X \subseteq XJ$ and $X = XJ$. Now $X = 0$ by Nakayama's Lemma. □

Given this, Jacobson wondered if $\bigcap_{n=1}^{\infty} J^n = 0$ also in non-commutative (right) Noetherian rings. This is not true for all right Noetherian rings, see Herstein's example (1965) example sheet 5, Qu. 5. As of today it is still open for (two sided) Noetherian rings.

Aside: We can define a topology on R where the powers of J are the open sets. Then this topology if hausdorff $\iff \bigcap_{n=1}^{\infty} J^n = 0$.

Definition 7.1.8. A commutative ring R is said to be **local** if $J(R)$ is its unique maximal ideal. Let R be a local ring. It is easy to see that $u \in R$ is a unit $\iff u \notin J$.

Theorem 7.1.9. *Let R be a commutative Noetherian ring s.t. $J = aR$ for some $a \in J(R)$. Then R is either a PID or an Artinian principal ideal ring.*

Proof. We shall show that every proper non-zero ideal of R is a power of J. We have $J^m = a^m R$ for all $m \geq 1$. let $I \lhd R, R \supsetneq I \supsetneq 0$. Then $I \subseteq J$ and since $\bigcap_{n=1}^{\infty} J^n = 0$, $\exists k \geq 1$ s.t. $I \subseteq J^k$ but $I \nsubseteq J^{k+1}$. Choose $x \in I$ s.t. $x \notin J^{k+1}$. Then $x = a^k t$ for some $t \in R, t \notin J$. So t is a unit of R hence $a^k = xt^{-1} \in I$. Thus $I = J^k = a^k R$ and I is principal. Now there are two cases:

1. Suppose that J is not nilpotent. Let a, b be non-zero non-units in R. Then $(aR)(bR) = J^{\alpha} J^{\beta} = J^{\alpha+\beta} \neq 0$ for some $\alpha, \beta \geq 1$. Then R is an integral domain thus R is a PID.

2. Suppose that J is nilpotent. Let $J^s = 0$ then $R, J, J^2, \ldots, J^{s-2}, J^s = 0$ are the only ideal. So in particular R is Artinian.

□

Example 7.1.10 (Noether's Example)**.**

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

R is Artinian, 0 is a meet-irreducible ideal. But 0 is not *primary* in any useful way. (You may like to develop your own theory to deal with such examples).

7.2 Rings of Krull Dimension 1

Definition 7.2.1. The **Garbriel-Rentschler Krull dimension** of M_R is defined as follows.

- K.dim$(M) = -1$ if $M = 0$
- K.dim$(M) = 0$ if M non-zero and Artinian
- K.dim$(M) = \alpha$ (α an ordinal) if K.dim(M) $\nless \alpha$ and for every chain $M_1 \supseteq M_2 \supseteq \ldots$ of submodules, $\exists n \geq 1$ s.t. K.dim$(M_i/M_{i+1}) < \alpha$, $\forall i \geq n$.

Example.

- K.dim$(\mathbb{Z}) = 1$.
- K.dim$(K[x]) = 1$, K a field.
- In fact K.dim$(R) = 1$ for any R a commutative PID.

Lemma 7.2.2. *Let R be a ring s.t. K.dim(R_R) ≤ 1 and let $c \in R$ s.t. $r(c) = 0$. Then R/cR is a right Artinian R-module.*

Proof. Consider $R \supseteq cR \supseteq c^2R \supseteq \dots$, since K.dim$(R_R) \leq 1$, $\exists n \geq 1$ s.t. $c^nR/c^{n+1}R$ since $r(c) = 0$ [1]. □

Lemma 7.2.3. *Let M_R be Artinian and Noetherian (i.e. a module with a composition series). Then $MJ^n = 0$ for some $n \geq 1$.*

Proof. Let $M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_n = 0$ be a composition series for M. Then each M_i/M_{i+1} is irreducible for each i. Now $(M_i/M_{i+1})J = 0$ (See section 3.3). it follows that $MJ^n = 0$. □

Theorem 7.2.4. *Let R be a prime Noetherian ring with K.dim(R) ≤ 1 then $\bigcap_{n=1}^{\infty} J^n = 0$*

Proof. If $E(R) \neq 0$ then R is simple Artinian by Exercise sheet 8, Qu. 2. In this case $J = 0$. So now assume that $E(R) = 0$, then

$$\bigcap_{\substack{F\text{-essential} \\ \text{right ideal}}} F = 0$$

Now by 6.2.1, F contains a regular element, c say. And by 7.2.2 R/cR is Artinian so R/F is Artinian. So by 7.2.3, $\exists n_F \geq 1$ s.t. $J^nF = RJ^n \subseteq F$. Hence,

$$\bigcap_{n=1}^{\infty} J^n \subseteq \bigcap_{\substack{F\text{-essential} \\ \text{right ideal}}} F = 0$$

□

Theorem 7.2.5 (Theorem of Lenagan)**.** *Let R be Noetherian and K.dim(R) ≤ 1. Then $\bigcap_{n=1}^{\infty} J^n = 0$*

Unfortunately there is not enough time to cover the proof during this course.

Question. In the above theorem, how about if K.dim(R) ≤ 2. Does the result still hold?

This problem is still open.

[1] To check this a useful fact is: $I \triangleleft_r R, R/I \cong cR/cI$ if $r(c) = 0$