Ring Theory (MA4H8)

Charudatta Hajarnavis
Notes by Florian Bouyer

Contents

1 Chapter 1: Rings **4**
1.1 Rings . . . 4
1.2 Properties of Addition and Multiplication . . . 4
1.3 Subrings and Ideals . . . 5
1.4 Cosets and Homomorphism . . . 5
1.5 The Isomorphism Theorems . . . 6
1.6 Direct Sums . . . 7
1.7 Division Rings . . . 7
1.8 Modules . . . 7
1.9 Factor Modules and Homomorphisms . . . 8
1.10 The Isomorphism Theorem . . . 9
1.11 Direct Sums of Modules . . . 9
1.12 Products of subsets . . . 9
1.13 A construction . . . 10
1.14 Zorn's Lemma, Well-ordering Principle, The Axiom of Choice . . . 10

2 Chapter 2: The Jacobson Radical **11**
2.1 Quasi-regularity . . . 11
2.2 Commutative Local Rings . . . 12

3 Chapter 3: Chain conditions **13**
3.1 Finitely Generated Modules . . . 13
3.2 Finiteness Assumption . . . 13
3.3 Nil and Nilpotent Ideals . . . 14
3.4 Nakayama's Lemma and an Application . . . 16

4 Commutative Noetherian Rings **17**
4.1 Primary Decomposition . . . 17
4.2 Decomposition of 0 . . . 18
4.3 Localisation [Commutative Algebra Section 3] . . . 20
4.4 Localisation of a Module [Commutative Algebra 3.1] . . . 22
4.5 Symbolic Powers . . . 22
4.6 The Rank of a Prime Ideal . . . 22
4.7 Regular Local Ring . . . 24

5 Projective Modules **25**
5.1 Free Modules . . . 25
5.2 Exact Sequences . . . 25
5.3 Projective Resolutions and Projective Dimension . . . 29
5.4 Localization and Global Dimension . . . 34

6 Global Dimension of Regular Local Rings **35**
6.1 Change of Rings Theorems . . . 35
6.2 Regular Local Ring . . . 37

7 Unique Factorization **39**
7.1 Unique Factorization Domain . . . 39
7.2 Stably Free Modules . . . 40

Any reference to Commutative Algebra refer to the 2011-2012 Commutative Algebra Lecture notes.

Rings studied will be mostly commutative. We aim to prove:

Theorem (Auslander - Buschsbaum 1959)**.** *A regular local ring is a unique factorization domain.*

Reason for selecting this theorem as our destination:

1. It requires sophisticated results from the theory of commutative Noetherian rings.

2. It requires methods from homological algebra. All known proofs require this.

3. At a crucial stage it helps to think in terms of non-commutative rings.

Prerequisite: MA3G6 Commutative Algebra

Topics assumed:

1. Basic properties of Noetherian rings and modules.

2. Primary decomposition

3. Technicality of localization

Definition. Let R be a commutative Noetherian local ring with 1 and unique maximal ideal M. Let $M = a_1R + \cdots + a_nR$ ($a_i \in M$) be chosen such that n is as minimal as possible. Construct a chain of prime ideals $M \supsetneq P_1 \supsetneq \cdots \supsetneq P_r$ (P_i prime) such that r is greatest possible. Then R is *regular* if $r = n$ (note that $r \leq n$ always in a Noetherian ring)

Local rings arise naturally in geometry. In algebraic geometry points correspond to local rings.

Existence of an identity is not part of our definition of a ring. For us a right, left or (two sided) ideal is a subring (Note that in a non-commutative ring, by ideal we will mean a two sided ideal). So for a right R-module M, $m \cdot 1 = m \, \forall m \in M$ is not a part of our definition. **But** whenever R has 1, we shall assume this.

1 Chapter 1: Rings

1.1 Rings

Definition 1.1. Let R be a non-empty set which has tow law of composition defined on it. (we call these law "addition" and "multiplication" respectively and use the familiar notation). We say that R is a *ring* if the following hold:

1. $a+b \in R$ and $ab \in R\ \forall a,b \in R$
2. $a+b=b+a\,\forall a,b \in R$ (Commutativity of addition)
3. $a+(b+c)=(a+b)+c\,\forall a,b,c \in R$ (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 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"

1.2 Properties of Addition and Multiplication

The following can be deduced from the axioms for a ring:

1. The element 0 is unique
2. Given $a \in R$, $-a$ is uniquely
3. $-(-a)=a$ for all $a \in R$
4. $a+b=a+c$ if and only if $b=c$ for $a,b,c \in R$
5. Given $a,b \in R$, the equation $x+a=b$ has a unique solution $x=b+(-a)$

   Notation. We write $a-b$ to mean $a+(-b)$
6. $-(a+b)=-a-b$ for all $a,b \in R$
7. $-(a-b)=-a+b$ for all $a,b \in R$
8. $a \cdot 0 = 0 \cdot a = 0$ for all $a \in R$
9. $a(-b)=(-a)b=-ab$ for all $a,b \in R$
10. $(-a)(-b)=ab$ for all $a,b \in R$
11. $a(b-c)=sb-ac$ for all $a,b,c \in R$

Notation. $\mathbb{Z}$, the integers. $\mathbb{Q}$, the rational numbers. $\mathbb{R}$, the real numbers. $\mathbb{C}$, the complex numbers. $M_n(R)$, the ring of $n \times n$ matrices whose entries are from the ring R.

1.3 Subrings and Ideals

Definition 1.2. A subset S of a ring R is called a *subring* of R if S itself is a ring with respect to the laws of composition of R

Proposition 1.3. *A non-empty subset S of a ring R is a subring of R if and only if $a-b \in S$ and $ab \in S$ whenever $a, b \in S$*

Proof. If S is a subring then obviously the given condition is satisfied. Conversely, suppose that the condition holds. Take any $a \in S$. We have $a - a \in S$ hence $0 \in S$. Hence for any $x \in S$ we have $0 - x \in S$ so $-x \in S$. Finally, if $a, b \in S$ then by the above $-b \in S$. Therefore $a - (-b) \in S$, i.e., $a + b \in S$. So S is closed with respect to both addition and multiplication. Thus S is a subring since all the other axioms are automatically satisfied. □

Definition 1.4. A subset I of a ring R is called an *ideal* if

1. I is a subring of R
2. For all $a \in I, r \in R$ $ar \in I$ and $ra \in I$

If I is an ideal of R we denote this fact by $I \lhd R$.

Proposition 1.5. *A non-empty subset I of a ring R is an ideal of R if and only if $a - b \in I, ar \in I$ and $ra \in I$ whenever $a, b \in I$ and $r \in R$*

Proof. Exercise □

1.4 Cosets and Homomorphism

Definition 1.6. Let I be an ideal of a ring R and $x \in R$. Then the set of elements $\{x + i : i \in I\}$ is called the *coset* of x in R with respect to I. It is denoted by $x + I$

When dealing with cosets, it is more important to realise that, in general, a given coset can be represented in more than one way. The next lemma shows how the coset representatives are related.

Lemma 1.7. *Let R be a ring with an ideal I and $x, y \in R$. Then $x + I = y + I \iff x - y \in I$*

Proof. Exercise □

We denote the set of all cosets of R with respect to I by R/I. We can give R/I the structure of a ring as follows: Define $(x + I) + (y + I) = (x + y) + I$ and $(x + I)(y + I) = xy + I$ for $x, y \in R$.

The key point here is that the sum and the product of R/I are well-defined, that is, they are independent of the coset representatives chosen. Check this and make sure that you understand why the fact that I is an ideal is crucial to the proof.

Definition 1.8. R/I is called the *residue class ring* of R with respect to I

The zero element of R/I is $0 + I = i + I$ for any $i \in I$. If S is a subset of R with $S \supseteq I$ we denote by S/I the subset $\{s + I : s \in S\}$ of R/I.

Proposition 1.9. *Let I be an ideal of a ring R. Then*

1. *Every ideal of the ring R/I is of the form K/I where $K \lhd R$ and $K \supseteq I$. Also conversely, $K \lhd R, K \supseteq I \Rightarrow K/I \lhd R/I$*
2. *There is a one to one correspondence between ideals of the ring R/I and the ideals of R containing I*

Proof.
1. If $K^* \lhd R/I$, define $K]\{x \in R : x + I \in K^*\}$. Then $K \lhd R, K \supseteq I$ and $K/I = K^*$
2. The correspondence is given by $K \leftrightarrow K/I$ where $K \lhd R$, $K \supseteq I$

□

Definition 1.10. A mapping θ of a ring R into a ring S is said to be a (ring) *homomorphism* if $\theta(x+y) = \theta(x) + \theta(y)$ and $\theta(xy) = \theta(x)\theta(y)$ for all $x, y \in R$.

θ defined by $\theta(r) = 0$ for all $r \in R$ is a homomorphism. It is called the *zero homomorphism.*

ϕ defined by $\phi(r) = r$ for all $r \in R$ is also a homomorphism. It is called the *identity homomorphism*

Let $I \lhd R$. Then $\sigma : R \to R/I$ defined by $\sigma(x) = x + I$ for all $x \in R$ is a homomorphism of R onto R/I. This is called the *natural* (or *canonical*) *homomorphism.*

Proposition 1.11. *Let R, S be rings and $\theta : R \to S$ a homomorphism. Then :*

1. $\theta(0_R) = 0_S$
2. $\theta(-r) = -q(r)$ *for all* $r \in R$
3. $K = \{x \in R : q\theta(x) = 0_S\}$ *is an ideal of* R
4. $\theta R = \{\theta(r) : r \in R\}$ *is subring of* S

Proof. Exercise $\square$

K is called the *kernel* of θ and θR is called the (homomorphic) *image* of R. The ideal K is sometimes denoted by $\ker\theta$.

Definition 1.12. Let θ be a homomorphism of a ring R into a ring S. Then θ is called an *isomorphism* if θ is a one to one and onto map. We say that R and S are isomorphic rings and denote this by $R \cong S$.

1.5 The Isomorphism Theorems

Question: Given a ring R, what rings can occur as its homomorphic images?

The importance of the first isomorphism theorem lies in the fact that it shows the answer to lie with R itself. It tells us that if we know all the ideals of R then we know all the homomorphic images of R.Only the first isomorphism theorem contains new information. The other two are simply its application.

Theorem 1.13. *Let θ be a homomorphism of a ring R into a ring S. Then $\theta R \cong R/I$ where $I = \ker\theta$*

Proof. Defined $\sigma : R/I \to R$ by $\sigma(x + I) = \theta(x)$ for all $x \in R$. The map σ is well defined since for $x, y \in R$, $x + I = y + I \Rightarrow x - y \in I = \ker\theta \Rightarrow \theta(x - y) = 0 \Rightarrow \theta(x) = \theta(y)$. θ is easily seen to be the required isomorphism. $\square$

Theorem 1.14. *Let I be an ideal and L a subring of a ring R. Then $L/(L \cap I) \cong (L + I)/I$*

Proof. Let σ be the natural homomorphism $R \to R/I$. Restrict σ to the ring L. We have $\sigma L = (L + I)/I$. The kernel of σ restricted to L is $L \cap I$. Now apply previous theorem. $\square$

Theorem 1.15. *Let I, K be ideals of a ring R such that $I \subseteq K$. Then $(R/I)/(K/I) \cong R/K$*

Proof. $K/I \lhd R/I$ and so $(R/I)/(K/I)$ is defined. Define a map $\gamma : R/I \to R/K$ by $\gamma(x + I) = x + K$ for all $x \in R$. The map γ is easily seen to be well defined and a homomorphism onto R/K. Further,

$$\begin{aligned} \gamma(x + I) = K &\iff x + K = K \\ &\iff x \in K \\ &\iff x + I \in K/I \end{aligned}$$

Therefore $\ker\gamma = K/I$. Now apply the first isomorphism theorem. $\square$

1.6 Direct Sums

Definition 1.16. *The internal direct sum:* Let $\{I_\lambda\}_{\lambda\in\Lambda}$ be a collection of ideals of a ring R. We define their *sum* to be $\sum_{\lambda\in\Lambda} I_\lambda = \{x \in R : x = x_1 + \cdots + x_k, x_i \in I_{\lambda_i}, k = 1, 2, 3, \ldots\}$. That is the sum is the collection of finite sums of elements of the I_λ's.

We say that the sum of the I_λ's is *direct* if each element of $\sum_{\lambda\in\Lambda} I_\lambda$ is uniquely expressible as $x_1 + \cdots + x_k$ with $x_i \in I_{\lambda_i}$. In this case we denote this sum as $\sum_{\lambda\in\Lambda} \oplus I_\lambda$ or $I_1 \oplus \cdots \oplus I_n$ if Λ is finite.

Proposition 1.17. *The sum $\sum_{\lambda\in\Lambda} I_\lambda$ is direct if and only if $I\mu \cap (\sum_{\lambda\in\Lambda,\lambda\neq\mu} I_\lambda) = 0$ for all $\mu \in \Lambda$*

Proof. Exercise □

Definition 1.18. *The external direct sum*: Let $R_1, \ldots, R_n$ be rings. We define the *external direct sum* S to be the set of all n-tuples $\{(r_1, \ldots, r_n) : r_i \in R_i\}$. On S we define addition and multiplication component wise. This makes S a ring. We write $S = R_1 \oplus \cdots \oplus R_n$.

The set $(0, \ldots, 0, R_j, 0, \ldots, 0)$ is an ideal of S. Clearly S is the internal direct sum of these ideals. But $(0, \ldots, R_j, \ldots 0) \cong R_j$. Because of this S can be considered as a ring in which the R_j are ideals and S is their internal direct sum. Also in internal direct sum we can consider $I_1 \oplus \cdots \oplus I_n$ to be the external direct sum of the rings I_j. Hence, in practice, we do not need to distinguish between external and internal direct sums.

1.7 Division Rings

Definition 1.19. Let R be a ring with 1. An element $u \in R$ is said to be a *unit* if there exists an element $v \in R$ such that $uv = vu = 1$. The element v is called the *inverse* of u and is denoted by u^{-1}

A ring D with at least two elements is called a *division ring* (or a *skew field*) if D has an identity and every non-zero element of D has an inverse in D

A division ring in which the multiplication is commutative is called a *field-discriminant*

Example. The Quaternions: Let D be the set of all symbols $a_0 + a_1 i + a_2 j + a_3 k$ where $a_i \in \mathbb{R}$. Two such symbols are considered to be equal if and only if $a_i = b_i$ for $i = 0, 1, 2, 3$. We make the ring as follows: Addition is component-wise. Two such symbols are multiplied term by term using the relations $i^2 = j^2 = k^2 = -1$ and $ij = -jk = k, jk = -kj = i, ki = -ik = j$. Then D is a non-commutative ring with zero and identity. Let $a_0 + a_1 i + a_2 j + a_3 k$ be a non-zero element of D. Then not all the a_i are zero. We have

$$(a_0 + a_1 i + a_2 j + a_3 k)(a_0 - a_1 i - a_2 j - a_3 k) = a_0^2 + a_1^2 + a_2^2 + a_3^2 \neq 0$$

. So letting $n = a_0^2 + a_1^2 + a_2^2 + a_3^2$, the element $(a_0/n) + (a_1/n)i + (a_2/n)j + (a_3/n)k$ is the inverse of $a_0 + a_1 i + a_2 j + a_3 k$. Thus D is a division ring. It is called the division ring of *real quaternions. Rational quaternions* can be defined similarly where the coefficients are from $\mathbb{Q}$.

1.8 Modules

Definition 1.20. Let R be a ring. A set M is called a *right R-module if:*

1. M is an additive abelian group
2. A law of composition $M \times R \to M$ is defined, which satisfies for $x, y \in M$ and $r_1, r_2 \in R$
3. $(x + y)r_1 = xr_1 + yr_1$
4. $x(r_1 + r_2) = xr_1 + xr_2$
5. $x(r_1 r_2) = (xr_1)r_2$

A *left* R-module is defined analogously. Here the product of $m \in M$ and $r \in R$ is denoted by rm.

Example.
1. R and $\{0\}$ are left R-modules. They are also right R-modules.
2. Let V be a vector space over a field F. Then V is a left F-module. The module axioms are part of the vector space axioms

3. Any abelian group can be considered a left $\mathbb{Z}$-module:

   Let $g \in A$ and $k \in \mathbb{Z}$. We defined $kg = \underbrace{g + \cdots + g}_{k \text{ times}}$ if $k > 0$, $0_{\mathbb{Z}}g = 0_A$ and $kg = -[(-k)g]$ if $k < 0$.

4. Let R be a ring. Then $M_n(R)$ becomes a left R-module if we define for $r \in R$ and $X \in M_n(R)$

$$rX = \begin{pmatrix} r & 0 & 0 & \cdots & 0 \\ 0 & r & 0 & \cdots & 0 \\ 0 & 0 & r & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \\ 0 & 0 & 0 & & r \end{pmatrix} X$$

   Clearly, we can also make $M_n(R)$ a right R-module.

The symbol M_R will denote M is a right R-module, while the symbol ${}_RM$ will denote M is a left R-module. For technical reason it is sometimes easier to work with right R-modules while dealing with non-commutative rings (when we choose to write maps on the left). We say simply say that M is a module if the other details are clear from the context.

Proposition 1.21. *Let M be a right R-module. Then:*

1. $0_M r = 0_M$ *for all* $r \in R$
2. $m0_R = 0_M$ *for all* $m \in M$.
3. $(-m)r = m(-r) = -mr$ *for all* $m \in M$ *and* $r \in R$

Proof. Exercise □

Definition 1.22. Let K be a subset of a right R-module M. Then K is called a *right R-submodule* (or just submodule) if K is also a right R-module under the laws of composition defined on M.

Proposition 1.23. *Let K be a non-empty subset of M_R. Then K is a submodule of M $\iff$ $x - y \in K$ and $xr \in K$ for all $x, y \in K$ and $r \in R$*

Proof. Exercise □

Definition 1.24. Submodules of R_R are called *right ideals* of R and submodules of ${}_RR$ are called *left ideals* of R.

1.9 Factor Modules and Homomorphisms

Let K be a submodule of a right R-module M. Consider the facto group M/K. Elements of M/K are cosets of the form $m + K$ with $m \in M$. We can make M/K a right R-module by defining $[m + K]r = mr + K$ for all $m \in M$ and $r \in R$. Check that this action is well defined and the module axioms are satisfied to make M/K a right R-module.

Proposition 1.25. *Let K be a submodule of M_R. Then*

1. *every submodule of M/K has the form A/K where A is a submodule of M and $A \supseteq K$.*
2. *There is a one to one correspondence between the submodules of M/K and the submodules of M containing K*

Definition 1.26. Let M and M' be right R-modules. A mapping $\theta : M \to M'$ is called an *R-homomorphism* if:

1. $\theta(x + y) = \theta(x) + \theta(y)$ for all $x, y \in M$
2. $\theta(xr) = \theta(x)r$ for all $x \in M$ and $r \in R$

If K is a submodule of M_R then the map $\sigma : M \to M/K$ defined by $\sigma(m) = m + K$ for all $m \in M$ is an R-homomorphism of M onto M/K. It is called the *canonical R-homomorphism*

Proposition 1.27. *Let $\theta : M_R \to M'_R$ be an R-homomorphism. Then:*

1. $\theta(0_M) = 0_{M'}$
2. $K = \{x \in M : \theta(x) = 0_{M'}\}$ *is a submodule of* M
3. $\theta M = \{\theta(m) : m \in M\}$ *is a submodule of* M'

Proof. Exercise □

K is called the *kernel* of θ and θM is called the *image* of θ. θ is a one to one correspondence map if and only if $\ker\theta = 0$

Definition 1.28. Let $\theta : M_R \to M'_R$ be an R-homomorphism. Then θ is called an *R-isomorphism* if it is in addition a one to one correspondence and onto map. In this case we write $M \cong M'$

1.10 The Isomorphism Theorem

There are similar to those for rings

Theorem 1.29. *Let M and M' be right R-modules and $\theta : M \to M'$ and R-homomorphism. Then $\theta M \cong M/K$ where $K = \ker\theta$*

Theorem 1.30. *Let L, K be submodules of M_R. Then $(L + K)/K \cong L/(L \cap K)$*

Theorem 1.31. *If K, L are submodules of M_R and $K \subseteq L$ then L/K is a submodule of M/K and $(M/K)/(L/K) \cong M/L$.*

The proofs of these theorems are similar to those for rings

1.11 Direct Sums of Modules

Let $M_1, \dots, M_n$ be right R-modules. The set of n-tuples $\{(m_1, \dots, m_n) : m_i \in M_i\}$ becomes a right R-modules if we define $(m_1, \dots, m_n) + (m'_1, \dots, m'_n) = (m_1 + m'_1, \dots, m_n + m'_n)$ and $(m_1, \dots, m_n)r = (m_1 r, \dots, m_n r)$. This is the *external direct sum* of the M_i and is denoted $\sum_{i=1}^n \oplus M_i$ or $M_1 \oplus \cdots \oplus M_n$.

Let $\{M_\lambda\}_{\lambda\in\Lambda}$ be a collection of submodules of a right R-modules M. We define their *sum* $\sum_{\lambda\in\Lambda} M_\lambda$ to be $\{m_{\lambda_1} + \cdots + m_{\lambda_k} : m_{\lambda_i} \in M_{\Lambda_i}$ for all possible subsets $\{\lambda_1, \dots, \lambda_k\}$ of $\Lambda\}$. Thus $\sum_{\lambda\in\Lambda} M_\lambda$ is the set of all finite sums of elements of the M_λ's. It is easy to see that this is a submodule of M.

$\sum_{\lambda\in\Lambda} M_\lambda$ is said to be *direct* if each $\sum_{\lambda\in\Lambda} M_\lambda$ has a unique expression as $m_{\lambda_1} + \cdots + m_{\lambda_k}$ for some $m_{\lambda_i} \in M_{\lambda_i}$. As in 1.6 we can show that $\sum_{\lambda\in\Lambda} M_\lambda$ is direct $\iff$ $M_\mu \cap \{\sum_{\lambda\in\Lambda,\lambda\neq\mu} M_\lambda\} = \{0\}$ for all $\mu \in \Lambda$. If $\sum_{\lambda\in\Lambda} M_\Lambda$ is direct, we denote it by $\sum_{\lambda\in\Lambda} \oplus M_\lambda$ or $M_1 \oplus \cdots \oplus M_n$ if Λ is a finite set. As explained for rings in 1.6, there is no real difference between (finite) external and internal direct sums of modules.

Definition 1.32. Let R be a ring with 1. A module M_R is said to be *unital* if $m1 = m$ for all $m \in M$

We shall assume that all modules considered are unital whenever R is a ring with identity.

1.12 Products of subsets

Let M be a right R-module. Let K, S be non-empty subsets of M and R respectively. We defined their *products* KS to be $\{\sum_{i=1}^n k_i s_i | k_i \in K, s_i \in S; i = 1, 2, \dots\}$. Thus KS consists of all possible finite sums of elements of the type ks with $k \in K$ and $s \in S$. If K is a non-empty subset of M and S is a right ideal of R then KS is a submodule of M. (Check that we require finite sums in our definition to make this work)

The above definition applies, in particular, when $M = R$. Thus if S is a non-empty subset of R then $S^2 = \{\sum_{i=1}^n s_i t_i : s_i, t_i \in S; n = 1, 2, \dots\}$. Extending inductively, S^nconsist of all finite sums of elements of the type $x_1 x_2 \dots x_n$ with $x_i \in S$.

Note that if S is a right ideal of R then so is S^n

1.13 A construction

Let R be a ring with an ideal I and M a right R-module. In general, M need not be a right R/I-module. However, we can give M a right R/I-module structure if $MI = 0$. In this case we define $mr = m[r + I]$ for all $m \in R$ and $r \in R$. It can be checked that this is well-defined right R/I-module action. Further, under this action the R and R/I submodules of M coincide.

In particular, I/I^2 is naturally a right (and left) R-module. This fact will be used repeatedly. In general same for I^n/I^{n+1}.

1.14 Zorn's Lemma, Well-ordering Principle, The Axiom of Choice

Definition 1.33. 1. A non-empty set $\mathscr{S}$ is said to be *partially ordered* if there exists a binary relation $\leq$ in $\mathscr{S}$ which is defined for certain pairs of elements in $\mathscr{S}$ and satisfies:

   (a) $a \leq a$

   (b) $a \leq b,\ b \leq c \Rightarrow a \leq c$

   (c) $a \leq b,\ b \leq a \Rightarrow a = b$

2. Let $\mathscr{S}$ be a partially ordered set. A non-empty subset τ is said to be *totally ordered* if for every pair $a, b \in \tau$ we have either $a \leq b$ or $b \leq a$

3. Let $\mathscr{S}$ be a partially ordered set. An elements $x \in \mathscr{S}$ is called a *maximal element* if $x \leq y$ with $y \in \mathscr{S} \Rightarrow x = y$. Similarly, for a *minimal* element

4. Let τ be a totally ordered subset of a partially ordered set $\mathscr{S}$. We say that τ has an *upper bound* in $\mathscr{S}$ if there exists $c \in \mathscr{S}$ such that $x \leq c$ for all $x \in \tau$.

Zorn's Lemma (Axiom). *If a partially ordered set $\mathscr{S}$ has the property that every totally ordered subset of $\mathscr{S}$ has an upper bound in $\mathscr{S}$, then $\mathscr{S}$ contains a maximal element.*

A non-empty set $\mathscr{S}$ is said to be *well-ordered* if it is totally ordered and every non-empty subset of $\mathscr{S}$ has a minimal element.

The Well ordering Principle. *Any non-empty set can be well-ordered.*

Axiom (The Axiom of Choice)**.** *Given a class of sets, there exists a "choice function", i.e., a function which assigns to each of these sets one of its elements.*

It can be shown that Axiom of Choice is logically equivalent to Zorn's Lemma which is logically equivalent to the Well-ordering Principle.

2 Chapter 2: The Jacobson Radical

All rings considered in this chapter are assumed to have an identity.

2.1 Quasi-regularity

Definition 2.1. Let M be a right ideal of R. M is said to be a *maximal right ideal* if $M \neq R$ and $M' \supsetneq M$ with $M' \lhd_r R \Rightarrow M' = R$.

Similar definition is applied for a maximal two-sided ideal, and maximal left ideal.

Proposition 2.2. *Let $I \neq R$ be a right ideal of a ring R. Then there exists a maximal right ideal M of R such that $M \supseteq I$.*

c.f. Commutative Algebra, Theorem 1.4. By Zorn's Lemma. Let $\mathscr{S}$ be the set of all proper right ideals of R containing I. Partially order $\mathscr{S}$ by inclusion. Let $\{T_\alpha\}_{\alpha\in\Lambda}$ be a totally ordered subset of $\mathscr{S}$. Let $T = \cup_{\alpha\in\Lambda} T_\alpha$. Then $T \lhd_r R$ and $T \supseteq I$. Moreover T is proper since $T = R \Rightarrow 1 \in T \Rightarrow 1 \in T_\alpha$ for some $\alpha \in \Lambda \Rightarrow T_\alpha = R$. Thus $T \neq R$ and so $T \in \mathscr{S}$. Thus $T \neq R$ and so $T \in \mathscr{S}$. Now $T \supseteq T_\alpha$ for all $\alpha \in \Lambda$. Hence Zorn's Lemma applies and $\mathscr{S}$ contains a maximal element, say M. Clearly M is a maximal right ideal and $M \supseteq I$. □

Corollary 2.3. *A ring with identity contains a maximal right ideal.*

Proof. Take $I = 0$ in the above theorem. □

Remark. This is not true for rings without 1

Definition 2.4. The intersection of all maximal right ideals of a ring R is called its *Jacobson radical*. It is usually denoted by $J(R)$ (or simply J)

Remark. Strictly speaking the above definition was for the right Jacobson radical. However we shall show that this is the same as the left Jacobson radical.

Theorem 2.5 (Crucial Lemma)**.** *Let M be a maximal right ideal of a ring R and let $a \in R$. Define $K = \{r \in R : ar \in M\}$. Then $K \lhd_r R$ and:*

1. *if $a \in M$ then $K = R$*
2. *if $a \notin M$ then K is also a maximal right ideal.*

Proof. Clear that $K \lhd_r R$, Now assume that $a \notin M$ so that $M + aR = R$ $(*)$. Define an R-module homomorphism $\theta : R \to R/M$ by $r \mapsto ar + M\, \forall r \in R$. Check that this is a homomorphism of right R-modules. By $(*)$, θ is an onto map. So by the isomorphism theorem for modules: $R/M \cong R/\ker\theta = R/K$. It follows that K is a maximal right ideal. □

Theorem 2.6. $J \lhd R$

Proof. Clearly $J \lhd_r R$. Now let $j \in J$ and $a \in R$ and suppose $aj \notin J$. Then by definition there exists a right ideal M such that $aj \notin M$. Define $K = \{r \in R : ar \in M\}$. By the previous theorem K is a maximal right ideal. But $j \notin K$ since $aj \notin M$ hence $j \notin J$. This is a contradiction. Hence $aj \in J$ for all $j \in J$ and $r \in R$. Thus $J \lhd R$. □

Definition 2.7. Let x be an element of a ring R. We say that x is a *right quasi-regular* (rqr) if $1 - x$ has a right inverse, i.e., if $\exists y \in R$ such that $(1 - x)y = 1$

A subset S of R is called *right quasi-regular* if every elements of S is rqr

Left quasi-regular (lqr) is defined analogously

We call an element or set *quasi-regular* if it is both lqr and rqr.

Lemma 2.8. *Let I be a rqr right ideal of R. Then $I \subseteq J$*

Proof. Let M be a maximal right ideal of R. If $I \nsubseteq M$ then $I + M = R$, so $1 = x + m$ for some $x \in I$ and $m \in M$. Hence $1 - x \in M$, now there exits $y \in R$ such that $(1 - x)y = 1$, so $1 \in M$ hence $M = R$. A contradiction, thus $I \subseteq J$ as required. □

Lemma 2.9. *Let R be a ring, $J(R)$ is a right quasi-regular ideal.*

Proof. Let $j \in J$. Suppose that $1-j$ has no right inverse. Then $(1-j)R \neq R$ so by Theorem 2.2 there exists a maximal right ideal M such that $(1-j)R \subseteq M$. But $j \in M$ by definition of $J(R)$ so $1 = 1-j+j \in M$, hence $M = R$. This is a contradiction, hence $1-j$ has a right inverse for all $j \in J$. So J is a rqr. $\square$

Lemma 2.10. *Let I be an ideal of a ring R. Then I rqr if and only if I lqr.*

Proof. Suppose that I is rqr. Let $x \in I$, then there exists $a \in R$ such that $(1-x)(1-a) = 1$. So $a = xa - x \in I$ since $I \lhd_r R$. Hence there exists $t \in R$ such that $(1-a)(1-t) = 1$, so $1-x = (1-x)1 = (1-x)(1-a)(1-t) = 1(1-t) = 1-t$. Hence $(1-a)(1-x) = 1$, thus x is lqr. By symmetry we can run the converse argument. $\square$

Theorem 2.11. *The (right) Jacobson radical is a qr ideal and contains all the rqr right ideals.*

Proof. This is what we have proved above. $\square$

Corollary 2.12. *The Jacobson radical of a ring R is left right symmetric, i.e., left Jacobson radical J_l is equal to the right Jacobson radical J_r*

Proof. J_l is a qr ideal by the left hand version of the theorem, so $J_l \subseteq J_r$. Similarly $J_r \subseteq J_l$, hence $J_r = J_l$. $\square$

Theorem 2.13. *Let R be a ring with Jacobson radical J. Then $J(R/J) = 0$*

Proof. The maximal right ideals of the right R/J are precisely the right ideals of the form M/J where M is a maximal right ideal of R $\square$

Remark. The theory can be adjusted to deal with rings without an identity.

2.2 Commutative Local Rings

Definition 2.14. Let R be a commutative ring, R is said to be a *local ring* if R has a unique maximal ideal

Note. This terminology is slightly different from Kaplansky's

Let R be a commutative local ring with 1. Let M be the maximal ideal of R, then:

1. M is the Jacobson radical of R
2. R/M is a field
3. If $x \in R$, $x \notin M$ then x is a unit of R.

Example. Let $R = \left\{ \frac{a}{b} | a, b \in \mathbb{Z}, b \text{odd} \right\}$

Check that R is a local ring. Find its unique maximal ideal. In fact $R = \mathbb{Z}_{(2)}$, i.e., the ring $\mathbb{Z}$ localised at the prime ideal $2\mathbb{Z}$

Remark. There exists a non-commutative ring with unique maximal ideal (in fact the only proper non-zero ideal) which is <u>not</u> its Jacobson radical.

3 Chapter 3: Chain conditions

Rings need not have 1 in this chapter

3.1 Finitely Generated Modules

Definition 3.1. Let Tbe a subset of M_R. The "smallest" submodule of M containing T is called *the submodule of M generated by T,* i.e., it is the intersection of all submodules of M containing T.

By convention we take $\{0\}$ to be the submodule generated by the empty set $\emptyset$.

Of particular importance is the case when T consists of a singles element $a \in M$. In general the submodule generated by a is $\{ar + \lambda a | r \in R, \lambda \in \mathbb{Z}\}$. This equals aR when R has 1 and M is unital.

Definition 3.2. If M_R is generated by a single element then we say that M is a *cyclic module*

A right R-module M is said to be *finitely generated* (f.g.) if it is the module generated by a finite subset. If R has 1 and M is a finitely generated module then $\exists a_1, \ldots, a_n \in M$ such that $M = a_1R + \cdots + a_nR$.

Cyclic submodules of R_R $[{}_RR]$ are called *principle right (left) ideals.*

3.2 Finiteness Assumption

Definition 3.3. Let $\mathscr{S}$ be a non-empty collection of submodules of a right R-module M.

1. An element $K \in \mathscr{S}$is said to be *maximal* in $\mathscr{S}$ if $\nexists K' \in \mathscr{S}$ such that $K' \supsetneq K$.

   Similarly for a *minimal* element of $\mathscr{S}$

2. A is said to have the *ascending chain condition* (ACC) for submodules in $\mathscr{S}$ if every chain of submodules $A_1 \subseteq A_2 \subseteq \ldots$ with $A_i \in \mathscr{S}$ has equal terms after a finite number of terms.

3. M is said to have the *maximum condition* on submodules in $\mathscr{S}$ if every non-empty collection of submodules in $\mathscr{S}$ has a submodules maximal in this collection.

   The *descending chain condition* (DCC) and *minimum condition* are defined analogously.

Proposition 3.4. *Let $\mathscr{S}$ be a non-empty collection of submodules of M_R then the following are equivalent:*

1. *M has ACC [DCC] on submodules in $\mathscr{S}$*

2. *M has the maximum [minimum] condition on submodules in $\mathscr{S}$*

Proof. Exercise $\square$

Particularly important is the case when $\mathscr{S}$ consists of all submodules in M_R. The abbreviation "M has ACC" will mean that M has ACC on the set of all submodules of M. Similarly for the other conditions.

Proposition 3.5. *The following are equivalent for a right R-module M.*

1. *M has ACC*

2. *M has the maximal condition*

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

Proof. This is Commutative Algebra Proposition 5.1 $\square$

Example. $\mathbb{Z}_{\mathbb{Z}}$ has ACC since every ideal is principle (this follows from the Euclidean Algorithm)

Remark. 1. ACC does not imply the existence of an integer n such that all chains stop after n steps. This is easily checked on $\mathbb{Z}$

2. Similarly with DCC. Examples are harder but they do exists.

3. However if M_R has both ACC and DCC then such an integer does exists. This follows from the theory of composition series.

Lemma 3.6 (Dedekind Modular Law). *Let A, B, C be submodules of M_R such that $A \supseteq B$. Then $A \cap (B + C) = B + (A \cap C)$.*

Proof. Elementary $\square$

Proposition 3.7 (Commutative Algebra 5.4). *Suppose that K is a submodule of M_R. Then M has ACC [DCC] if and only if both K and M/K have ACC [DCC]*

Proof. $\Rightarrow$: Straightforward

$\Leftarrow$: Let $M_1 \subseteq M_2 \subseteq \dots$ be an ascending chain of submodules of M. 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 of K. So there exists $k \geq 1$ such that $M_k \cap K = M_{k+i} \cap K$ for all $i \geq 1$. The second chain stops since it consists of submodules of M which are in 1 to 1 correspondence with those of M/K. So there exists an l such that $M_l + K = M_{l+i} + K$ for all $i \geq 1$. Let $n = \max\{k, l\}$. Then $M_{n+i} = M_{n+i} \cap (M_{n+i} + K) = M_{n+i} \cap (M_n + K) = M_n + (M_{n+i} \cap K)$ by the Modular Law (since $M_{n+i} \supseteq M_n$). And $M_n + (M_{n+i} + K) = M_n + M_n \cap K = M_n$, and this is true $\forall i \geq 1$. So M_R has ACC

Similarly for DCC $\square$

This important proposition has many consequences

Corollary 3.8 (Commutative Algebra 5.5). *Let $M_1, \dots, M_n$ be submodules of a right R-modules M. If each M_i has ACC [DDC] then so does their sum $M_1 + \dots + M_n = K$.*

Proof. Take $K_1 = M_1 + M_2$. We have $K_1/M_1 = \frac{M_1+M_2}{M_1} \cong \frac{M_2}{M_1 \cap M_2}$. So $\frac{K_1}{M_1}$ has ACC [DCC] since $\frac{M_2}{M_1 \cap M_2}$ is a factor modules of M_2 and M_2 has ACC. Also M_1 has by assumption ACC [DCC]. So by the proposition 3.7, K_1 has ACC [DCC].

This can easily be extended by induction. $\square$

Corollary 3.9. *Let R be a ring with 1. Suppose that R has ACC [DCC] on right ideals. Let M_R be a finitely generated unital right R-module. Then M_R has ACC [DCC] on submodules.*

Proof. Since M_R is finitely generated and unital, there exists $m_1, \dots, m_k$ such that $M = m_1R + \dots m_kR$. So by Corollary 3.8 it is enough to show that each m_iR has ACC [DCC]. The map $r \to m_ir$ for all $r \in R$ is an R-homomorphism of R_R onto m_iR. So m_iR is isomorphic to a factor of R_R. So m_iR has ACC [DCC] on submodules. $\square$

Remark. If R does not have 1, the ACC part of the corollary still holds but the DCC part is false! This is because $(m_i) = \{m_ir + \lambda m_i | r \in R, \lambda \in \mathbb{Z}\}$ and $\mathbb{Z}$ has ACC but not DCC

Definition 3.10. A modules with ACC on submodules is called a *Noetherian module.* A modules 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 ACC on left ideals is called a *left Noetherian ring.*

A ring with 1 and DCC on right ideals is called a *right Artinian ring.* A ring with 1 and DCC on left ideals is called a *left Artinian ring.*

3.3 Nil and Nilpotent Ideals

Definition 3.11. Let S be non-empty subset of a ring R. S is said to be *nil* if given any $s \in S$ there exists an integer $k \geq 1$ (which depends on s) such that $s^k = 0$. S is said to be *nilpotent* if there exists an integer $k \geq 1$ such that $S^k = 0$

If S consists of a single element, there is no difference between nil and nilpotent and we normally say that the element is nilpotent.

Proposition 3.12. *Let R be a ring with 1. Every nil one sided ideal of R is 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 $(1-x)(1+x+\cdots+x^{k-1}) = 1$ so x is r.q.r. so $x \in J(R)$. Thus $I \subseteq J(R)$. $\square$

Remark. This is also true without 1.

Lemma 3.13. *Let R be a ring:*

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

Proof. Suppose that $I^k = 0$ and $K^l = 0$, $k, l \geq 1$. Then $(I+K)^{k+l-1} = 0$ since every term in the expansion lies in either I^k or K^l and hence is zero. So $I+K$ is nilpotent. $(RI)^k = (RI)(RI)\dots(RI) \subseteq R(IR)^{k-1}I \subseteq RI^k = 0$. So RI is nilpotent.

Suppose that I is a nilpotent right ideal. Then $I \subseteq I + RI$. Now $I + RI \lhd R$ and is nilpotent by the first part. $\square$

Definition 3.14. The sum of all nilpotent ideals of R is called the *Nilpotent radical* (or the Wedderburn radical). It is usually denoted by $N(R)$.

Note. $N(R) \subseteq J(R)$ always.

It follows from Lemma 3.13 that $N(R) = \sum$ nilpotent right ideals $= \sum$ nilpotent left ideals. Clearly $N(R)$ is a nil ideal. It is in general not itself nilpotent.

Example (Zassenhaus's Example)**.** Let F be a field, I the open interval $(0,1)$ and R a vector space over F with basis $\{x_i | i \in I\}$. Define a multiplication on F by extending the following product of basis elements $x_i x_j = \begin{cases} x_{i+j} & \text{if } i+j<1 \\ 0 & \text{if i + j} \geq 1 \end{cases}$. Thus 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 except a finite number of i. Check that $N(R) = R$ but R is not nilpotent.

Proposition 3.15. *Let R be a commutative ring. Then $N(R)$ equals the set of all nilpotent elements of R.*

Proof. Let n be a nilpotent element. This implies that the principle ideal generated by n is nilpotent. (Prove!) $\square$

Example. The above is false for non-commutative rings. e.g, let R be the ring of 2×2 matrices over $\mathbb{Q}$. Then R has only two ideals 0 and R. So $N(R) = 0$ but $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = 0$.

Definition 3.16. An ideal P of a ring R is said to be a *prime ideal* if $AB \subseteq P$, $A, B \lhd R$ implies $A \subseteq P$ or $B \subseteq P$. We exclude R itself from the set of prime ideals.

Proposition 3.17. *Let R be a commutative ring and $P \lhd R$. Then P is a prime ideal if and only if $(a, b \in R)$ we have $ab \in P \Rightarrow a \in P$ or $b \in P$.*

Proof. Trivial if R has 1. Not so trivial but still true if R does not have 1. $\square$

Proposition 3.18 (Commutative Algebra 1.10)**.** *Let R be a ring. The intersection of all prime ideals of R is a nil ideal.*

Proof. We shall show that if $x \in R$ is not nilpotent then there exists a prime ideal excluding it. Suppose that $x \in R$ is not nilpotent. Let $\mathscr{S}$ be the set of ideals which contains no power of x. $\mathscr{S} \neq 0$ since $\{0\} \in \mathscr{S}$. Check that Zorn's lemma applies. So $\mathscr{S}$ contains a maximal element, say P. Claim: P is a prime ideal. If not then $\exists$ ideals A and B of R such that $AB \subseteq P$ but $A \nsubseteq P$ and $B \subseteq P$. Then $A + P \supsetneq P$ and $B + P \supsetneq P$. So $x^k \in A + P$ and $x^l \in B + P$ for some integers k, l. But then $x^{k+l} \in (A+P)(B+P) \subseteq P$ which is a contradiction. Thus P is a prime ideal proving the proposition. $\square$

Corollary 3.19. *In a commutative ring $N(R)$ equals the intersection of all prime ideals of R.*

Proof. This follows from Theorem 3.15 and the previous theorem. □

Corollary 3.20. *In a commutative ring with* 1 *a finitely generated nil ideal is nilpotent. In particular when* R *is Noetherian* $N(R)$ *is nilpotent.*

Proof. Let K be a finitely generated ideal of R. Let $K = k_1R + \cdots + k_sR$ with $k_i \in K$. Each k_i is nilpotent hence so is the ideal. The result follows by 3.13. When R is Noetherian $N(R)$ is finitely generated and so nilpotent by above. □

3.4 Nakayama's Lemma and an Application

Definition 3.21. Let $I \lhd_r R$. We say that $a_1, \ldots, a_n$ is *minimal generated set* for I if:

1. $a_1, \ldots, a_n$ generate I
2. No proper subset of $\{a_1, \ldots, a_n\}$ generates I.

Nakayama's Lemma. *Let* R *be a ring with* 1 *and* M_R *a finitely generated module. Let* I *be a subset of* $J(R)$ *Then* $MI = M \Rightarrow M = 0$.

Proof. Let $MI = M$. Then we have $MJ = M$. Suppose that $M \neq 0$. Let $a_1, \ldots, a_n$ be a minimal generated set for M. We have $M = a_1R + \cdots + a_nR$ so that $MJ = a_1J + \cdots + a_nJ$. Now $a_1 \in M = MJ$ so $a_1 = a_1x + \cdots + a_nx_n$ for some $x_i \in J$. Now $a_1(1-x) = a_2x_2 + \cdots + a_nx_n$ ($a_1(1-x_1) = 0$ if $n = 1$). So $a_1 = a_2x_2(1-x_1)^{-1} + \cdots + a_nx_n(1-x_1)^{-1}$ ($a_1 = 0$ if $n = 1$). This contradicts the minimality of n. Hence $M = 0$ □

Remark. This is also valid for rings without 1.

Let R be a commutative local ring with 1 with unique maximal ideal J. Then R/J is a field. So J/J^2 is an R/J-module, i.e., J/J^2 is a vector space over the field R/J. If $x \in R$ let $\overline{x}$ denote the coset $x + J^2$. So $\overline{x} \in R/J^2$.

Lemma 3.22 (Commutative Algebra 2.17)**.** *Let* R *be a commutative local ring with* 1*. Let* J *be the maximal ideal of* R*. Suppose that* J *is finitely generated and* $x_1, \ldots, x_k \in J$*. Then* $x_1, \ldots, x_k$ *generate* J *(as an* R*-module)* $\iff$ $\overline{x_1}, \ldots, \overline{x_k}$ *is a set which spans the vector space* J/J^2 *(over the field* R/J*)*

Proof. $\Rightarrow$) $\overline{x_1}, \ldots, \overline{x_k}$ generate J/J^2 as an R-module so $\overline{x_1}, \ldots, \overline{x_k}$ generate J/J^2 as an R/J-module, i.e., they span the vector space J/J^2.

$\Leftarrow$) Let $I = x_1R + \cdots + x_kR$. Then $I \subseteq J$, $\overline{x_1}, \ldots, \overline{x_k}$ generates J/J^2 as an R-module, hence $I + J^2 = J$. This implies that $(J/I)J = J/I$ where J/I is considered as an R-module. So $J/I = 0$ by Nakayama's lemma, so $J \subseteq I$. Hence $J = x_1R + \cdots + x_kR$. □

Corollary 3.23. *In the above ring* $x_1, \ldots, x_k$ *is a minimal generated set for* J $\iff$ $\overline{x_1}, \ldots, \overline{x_k}$ *is a basis for the vector space* J/J^2 *over* R/J*.*

Proof. Follows from above □

Theorem 3.24. *Let* R *be a commutative Noetherian local ring with* 1*. Let* J *be the maximal ideal of* R*. Then any two minimal generating set of* J *contain the same number of elements.*

Proof. This is a direct consequence of the corollary □

Notation. We shall denote this common number by $V(R)$. Thus $V(R) = \dim J/J^2$ as a vector space over the field R/J.

4 Commutative Noetherian Rings

All rings considered in this chapter are assumed to be commutative rings 1.

4.1 Primary Decomposition

Definition 4.1. An ideal Q is said to be *primary* if $ab \in Q$ $(a, b \in R)$ implies that $a \in Q$ or $b^n \in Q$ for some integer n.

Clearly a prime ideal is primary.

Definition 4.2. R is called a *primary ring* if 0 is a primary ideal.

Clearly an ideal Q is primary if and only if R/Q is a primary ring.

Definition 4.3. We say that R has *primary decomposition* if every ideal of R is expressible as a finite intersection of primary ideals.

Definition 4.4. An ideal is said to be *meet-irreducible* if $I = A \cap B$, $A, B \lhd R$ implies $I = A$ or $I = B$.

Note. The two different definitions: M_R is *irreducible* if $\{0\}$ and M are the only submodules. $I \lhd R$ is *meet-irreducible* if $I = A \cap B$ implies $I = A$ or $I = B$

Lemma 4.5 (Commutative Algebra 6.18)**.** *Let R be a Noetherian ring. Then every ideal of R is expressible as a finite intersection of meet-irreducible ideals.*

Proof. Suppose not. Let $A \lhd R$ be a maximal counterexample. Then A is not meet-irreducible. So $A = B \cap C$, $B, C \lhd R$, $B \supsetneq A, C \supsetneq A$. By maximality of A, both B and C are finite intersection of meet-irreducible ideals. Hence so is A. Contradiction hence the result holds. □

Notation. Let M be a subset of M_R. The *annihilator* of S in R is $\operatorname{ann}(S) = \{r \in R | Sr = 0\}$. For R is non-commutative $\operatorname{ann}(S) \lhd_r R$. If S is a submodule then typically S is a subset of R.

Theorem 4.6 ((Noether) Commutative Algebra 6.20)**.** *A Noetherian ring has primary decomposition*

Proof. By the previous lemma it is enough to show that a meet-irreducible ideal is primary. Without loss of generality assume 0 to be meet-irreducible. Suppose that $ab = 0$, $a, b \in R$.

Claim: There exists an integer $n \geq 1$ such that $b^n R \cap \operatorname{ann}(b^n) = 0$.

Since the chain $\operatorname{ann}(b) \subseteq \operatorname{ann}(b^2) \subseteq \ldots$ stops there is an integer $n \geq 1$ such that $\operatorname{ann}(b^n) = \operatorname{ann}(b^{2n})$. Now $z \in b^n R \cap \operatorname{ann}(b^n) \Rightarrow x = b^n t$ for some $t \in R$ and $b^z = 0$. So $b^{2n} t = 0 \Rightarrow b^n t = 0 \Rightarrow z = 0$. Since 0 is meet-irreducible either $b^n R = 0$ or $\operatorname{ann}(b^n) = 0$. Thus $b^n = 0$ or $a = 0$ and 0 is a primary ideal □

Definition 4.7. Let Q be a primary ideal. Let P/Q be the nilpotent radical of the ring R/Q. P is called the *radical* of Q and we say that Q is *P-primary.*

Notation. We denote the radical of Q by $\sqrt{Q}$.

Recall that for a commutative ring R, $N(R)$ =set of all nilpotent elements of R.

Proposition 4.8. *Let Q be a primary ideal and let $P = \sqrt{Q}$. Then:*

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. Hence $b \in P$. Thus P is a prime ideal/
2. P/Q is a nil ideal of R/Q. If R/Q is Noetherian, P/Q is nilpotent (by Proposition 3.13 ?(check reference maybe)). Hence $P^k \subseteq Q$ for some $k \geq 1$.

□

Theorem 4.9 (Commutative Algebra 6.24)**.** *Let R be a commutative Noetherian ring. Then $\cap_{n=1}^{\infty} J^n = 0$ where $J = J(R)$.*

Proof. Let $X = \cap_{n=1}^{\infty} J^n$. Let $XJ = Q_1 \cap \cdots \cap Q_n$ be a primary decomposition for X. Fix i and let $P_i = \sqrt{Q_i}$, if $X \nsubseteq Q_i$ then $J \subseteq P_i$. So $J^{k_i} \subseteq Q_i$ for some $k_i \geq 1$ by the previous proposition. Thus $X \subseteq Q_i$ or $J^{k_i} \subseteq Q_i$. So $X \subseteq Q_i$ for all $i = 1 \dots, n$ in any case. Hence $X \subseteq XJ$. So $X = XJ$ hence by Nakayama's lemma $X = 0$. □

This is a surprisingly useful result.

Remark. For a right Noetherian ring this is false (Proven by Herstein in 1965). While for left and right Noetherian rings the result is still an open problem.

Definition 4.10. A ring is called an *integral domain* if the product of any two non-zero elements of the ring is non-zero.

Theorem 4.11. *Let R be a commutative, local, Noetherian ring. Suppose that $J = J(R)$ is a principle ideal. Then every non-zero ideal of R is a power of J. In particular, R is a principal ideal ring.*

Proof. Let $0 \neq I \lhd R$, $I \neq R$. Then $I \subseteq J$. Since $\cap_{n=1}^{\infty} J^n = 0$ there exists an integer $k \geq 1$ such that $I \subseteq J^k$ but $I \nsubseteq J^{k+1}$. Let $J = aR$ $(a \in J)$, then $J^m = a^m R \forall m \geq 1$. Now there exists an element x such that $x \in I$ but $x \notin a^{k+1}R$ $(*)$. Since $x \in a^k R$ we have $x = a^k t$ for some $t \in R$. Now $t \notin J = aR$ by $(*)$. So t must be a unit of R. So $a^k = xt^{-1} \in I$. Hence $J^k = a^k R \subseteq I$. It follows that $I = J^k$ proving the theorem. □

Corollary 4.12. *Let R be a commutative, local, Noetherian ring.*

1. *If J is not nilpotent then R is an integral domain and 0 and J are the only prime ideals of R.*
2. *If J is nilpotent then R is Artinian and J is the only prime ideal of R.*

Proof. Exercise. (Note that in 2. $J^s = 0$ for some $s \geq 1$ so $R, J, J^2, \dots, J^s = 0$ are the only ideals. □

4.2 Decomposition of 0

Definition 4.13. Let $I = Q_1 \cap \cdots \cap Q_n$ be a primary decomposition for an ideal I. Suppose that Q_i are P_i-primary. We say the decomposition is *normal* [Commutative Algebra: minimal] if

1. No Q_i is superfluous
2. $P_i \neq P_j$ for all $i \neq j$

Given that I has a primary decomposition, we can arrange a normal decomposition for I by:

1. Removing any superfluous primary ideals and
2. By applying the following:

Lemma 4.14. *If Q_1 and Q_2 are P-primary ideals then so is $Q_1 \cap Q_2$*

Proof. Let $ab \in Q_1 \cap Q_2$, $a, b \in R$. If $a \notin Q_1 \cap Q_2$ then $a \notin Q_1$ say. Then $b^n \in Q_1$ for some $n \geq 1$. So $b \in P$. Hence $b^s \in Q_2$ for some $s \geq 1$ since Q_2 is P-primary. Let $k = \max(n, s)$ then $b^k \in Q_1 \cap Q_2$. Now $p \in P$ implies $p^t \in Q_1 \cap Q_2$ for sufficiently large $t \geq 1$. Hence $P \subseteq \sqrt{Q_1 \cap Q_2}$. But $Q_1 \cap Q_2 \subseteq Q_1$ so $\sqrt{Q_1 \cap Q_2} \subseteq \sqrt{Q_1} = P$, thus $P = \sqrt{Q_1 \cap Q_2}$. □

Thus whenever necessary we shall assume that the primary decomposition being considered is normal.

Remark. We may still have $\sqrt{Q_i} \supsetneq \sqrt{Q_j}$ with a normal primary decomposition [Commutative Algebra, example before 6.8]

Definition 4.15. Let R be a ring. We say that a prime ideal P is a *minimal* prime ideal of R if $Q \subseteq P$ with Q prime implies $Q = P$.

Lemma 4.16. *Let R be a commutative Noetherian ring. Suppose that $0 = Q_1 \cap \cdots \cap Q_n$ be a primary decomposition of 0. Let $P_i = \sqrt{Q_i}$ and suppose (after possible renumbering) that $P_1, \dots, P_k$ are minimal in the set $\{P_1, \dots, P_n\}$. Then $P_1, \dots, P_k$ are precisely the minimal primes of R.*

Proof. It is enough to show that if P is a prime ideal of R then $P \supseteq P_j$ for some $1 \leq j \leq k$. By Theorem 4.6 (? check reference) there exists integers $k_i \geq 1$ such that $P_i^{k_i} \subseteq Q_i$ for $i = 1, \ldots, n$. Then $P_1^{k_1} P_2^{k_2} \ldots P_n^{k_n} \subseteq Q_1 \cap \cdots \cap Q_n = 0$. In particular, $P_1^{k_1} \ldots P_n^{k_n} \subseteq P$ hence $P_m \subseteq P$ for some m with $1 \leq m \leq n$. But since $P_1, \ldots, P_k$ are minimal in the set $\{P_1, \ldots, P_n\}$ we have $P_j \subseteq P_m$ for some j, $1 \leq j \leq m$. Thus $P \supseteq P_j$ with $1 \leq j \leq m$ as required. □

Definition 4.17. Let $c \in R$, we say that c is *regular* if $cx = 0, x \in R \Rightarrow x = 0$

An element which is not regular is called a *zero-divisor*.

Notation. Let $I \lhd R$. Write $\mathscr{C}(I) = \{x \in R | x + I \text{ is regular in the ring } R/I\}$

Clearly $\mathscr{C}(0) = \{\text{regular elements of } R\}$. If P is a prime ideal, in a commutative ring then $\mathscr{C}(P) = R \setminus P$.

Proposition 4.18. *Let R be a Noetherian ring and $0 = Q_1 \cap \cdots \cap Q_n$ a normal primary decomposition. Let $P_i = \sqrt{Q_i}$ and suppose that $P_1, \ldots, P_k$ are the minimal primes of R. Then:*

1. $N(R) = P_1 \cap \cdots \cap P_k$.
2. $\mathscr{C}(0) = R \setminus \cup_{i=1}^n P_i$
3. $\mathscr{C}(N) = R \setminus \cup_{i=1}^k P_i$

Proof.
1. Clearly $N \subseteq P_1 \cap \cdots \cap P_k$. Now $P_1 \cap \cdots \cap P_k \subseteq P_j$ for all $1 \leq j \leq n$. By Proposition 4.8 there exists an integer t_i such that $(P_1 \cap \cdots \cap P_k)^{t_i} \subseteq Q_i$. Let $t = \max\{t_i\}$, then $(P_1 \cap \cdots \cap P_k)^t \subseteq Q_1 \cap \cdots \cap Q_n = 0$. Thus $P_1 \cap \cdots \cap P_k \subseteq N$ and so $P_! \cap \cdots \cap P_k = N$.
2. Let $c \in R \setminus \cup_{i=1}^n P_i$. Then $cx = 0, x \in R \Rightarrow x \in Q_i$ for all i $1 \leq i \leq n$, since c belong to no P_i. Hence $x \in Q_1 \cap \cdots \cap Q_n = 0$, so $c \in \mathscr{C}(0)$.

   Now $P_i^{n_i} \subseteq Q_i$ for some n_i. So $P_i^{n_i}[Q_1 \cap \cdots \cap Q_{i-1} \cap Q_{i+1} \cap \cdots \cap Q_n] \subseteq Q_1 \cap \cdots \cap Q_n = 0$. Now $Q_1 \cap \cdots \cap Q_{i-1} \cap Q_{i+1} \cap \cdots \cap Q_n \neq 0$ since our decomposition is normal. So P_i is does not contain a regular elements and hence $\cup_{i=1}^n P_i$ does not contain a regular element. Hence $\mathscr{C}(0) = R \setminus \cup_{i=1}^n P_i$
3. Exercise

□

Lemma 4.19. *Let R be a commutative ring. Let $P_1, \ldots, P_n$ be ideals of R, at least $n-2$ of which are prime. Let S be a subring of R. Suppose that $S \subseteq \cup_{i=1}^n P_i$, then $S \subseteq P_k$ for some k, $1 \leq k \leq n$.*

Remark. Note that S does not (necessarily) contain 1, since our definition of rings did not include 1

Proof. Proof by induction on n. For $n = 1$, result is trivial.

For $n = 2$ if $S \nsubseteq P_1$ and $S \nsubseteq P_2$ then choose $x_1, x_2 \in S$ such that $x_1 \notin P_2$ and $x_2 \notin P_1$. Then $x_1 + x_2 \in S$ but $x_1 + x_2 \notin P_i, i = 1, 2$.

Now assume $n > 2$ and that the result holds for values $< n$.

Clearly any selection of $n-1$ of the P_i at most 2 will be non-prime. Suppose that $S \subseteq \cup_{i=1}^n P_i$ but $S \notin P_i$ for any i $(i = 1, 2, \ldots, n)$. Then $S \nsubseteq P_1 \cup \cdots \cup P_{k-1} \cup P_{k+1} \cup \cdots \cup P_n$ by induction hypothesis (as k varies). Now choose $x_k \in S$ such that $x_k \notin P_1 \cup \cdots \cup P_{k-1} \cup P_{k+1} \cup \cdots \cup P_n$. Thus $x_k \in P_k$. Since $n > 2$ at least of the P_i must be prime, say P_1. Let $y = x_1 + x_2 \ldots x_n$, then $y \notin P_i$ for any $i = 1, \ldots, n$. This is a contradiction. This completes the induction. □

Proposition 4.20. *Let R be a commutative Noetherian ring. Let $I \lhd R$, then I contains a regular element if and only if* $\operatorname{ann} I = 0$.

Proof. $\Rightarrow$: Trivial

$\Leftarrow$: Suppose that every element of I is a zero divisor. Then by the Proposition 4.18 part 2) $I \subseteq \cup_{i=1}^n P_i$ (where the P_i are as in Proposition 4.18. So $I \subseteq P_j$, for some j, $1 \leq j \leq n$. We have $\operatorname{ann} I \supseteq \operatorname{ann} P_j \neq 0$. This completes the proof. □

Proposition 4.21. *Let R be a commutative Noetherian ring and $I \lhd R$. Suppose that I contains a regular element. Then $I = c_1 R + \cdots + c_n R$ where each c_i is regular.*

Proof. Let K be the right ideal generated by the regular elements in I. So $I \setminus K$ is either empty or consists of zero divisors. Let $P_1, \dots, P_n$ be the primes associated with a primary decomposition of 0 (as in Proposition 4.18). So $I \setminus K \subseteq P_1 \cup \dots \cup P_n$ by Proposition 4.18 part 2, so $I \subseteq K \cup P_1 \cup \dots \cup P_n$. Hence $I \subseteq K$ or $I \subseteq P_i$ for some i (by Lemma 4.19). But $I \nsubseteq P_i$ for any i since I contains a regular element but all P_i contains zero-divisors. Hence $I \subseteq K$ and so $I = K$. Since R is Noetherian it follows that we can find a finite generating set consisting of regular elements. □

4.3 Localisation [Commutative Algebra Section 3]

Definition 4.22. Let S be a non-empty subset of a ring R. We say that S is *multiplicatively closed* if $s_1, s_2 \in S \Rightarrow s_1 s_2 \in S$.

Typical example: $\mathscr{C}(P) = R \setminus P$ where P is a prime ideal in a commutative ring. We shall always assume $0 \notin S$ and $1 \in S$.

Define an equivalence relation $\sim$ on $R \times S$ as follows: $(a, s) \sim (b, t)$ if there exists $s' \in S$ such that $(at - bs)s' = 0$ (where $(a, s), (b, t) \in R \times S$)

Let $\frac{a}{c}$ be the equivalence class of (a, b) and let R_S denote the set of all such equivalence classes. For $\frac{a}{s}, \frac{b}{t} \in R_S$ define $\frac{a}{s} + \frac{b}{t} = \frac{at+bs}{st}$ and $\frac{a}{s} \times \frac{b}{t} = \frac{ab}{st}$.

Check that this is well-defined and that R_S is a ring. We have a natural ring homomorphism $\phi : R \to R_S$ given by $\phi(r) = \frac{r}{1}$ for all $r \in R$

Definition 4.23. R_S constructed above is called a *localizations of R at S*

Let A, B be rings with 1 and $\phi : A \to B$ a homomorphism of rings. In this context we shall always assume $\phi(1_A) = 1_B$

The Universal Mapping Property.

$$\begin{tikzcd} A \arrow[d, "\phi"'] \arrow[dr, "\theta"] & \\ B & A_S \arrow[l, dashed, "\psi"] \end{tikzcd}$$

Let A, B be rings and S a multiplicatively closed subset of A. Suppose that $\phi : A \to B$ is a ring homomorphism such that $\phi(s)$ is a unit in B for all $s \in S$. Then there exists a unique ring homomorphism $\psi : A_S \to B$ such that $\phi = \psi\theta$

Proof. See Commutative Algebra 3.2-point □

The ring homomorphism $\theta : R \to R_S$ has the following properties:

1. $s \in S$ implies $\theta(s)$ is a unit in R_S
2. Given $a \in R, \theta(a) = 0$ if and only if $as = 0$ for some $s \in S$
3. Every element of R_S is expressible as $\theta(a)[\theta(s)]^{-1}$ for some $a \in R$, $s \in S$.

These three properties determine R_S to within isomorphism.

Theorem 4.24. *Let A, B be rings and S a multiplicatively closed subset of A. Suppose that $\alpha : A \to B$ is a ring homomorphism such that:*

1. *$s \in S$ implies $\alpha(s)$ is a unit of B*
2. *$\alpha(a) = 0$ implies $as = 0$ for some $s \in S$*
3. *Every element of B is expressible as $\alpha(a)[\alpha(s)]^{-1}$ for some $a \in A, s \in S$.*

Then there exists a unique isomorphism $\psi : A_S \to B$ such that $\alpha = \psi\theta$, where θ is the natural map $A \to A_S$.

$$\begin{tikzcd} A \arrow[d, "\alpha"'] \arrow[dr, "\theta"] & \\ B & A_S \arrow[l, dashed, "\exists!\,\psi"] \end{tikzcd}$$

Proof. By the universal mapping property there is a unique homomorphism $\psi : A_S \to B$ such that $\alpha = \psi\theta$, where ψ is given by $\psi(as^{-1}) = \alpha(a)[\alpha(s)]^{-1}$ (used property 1.) Then use property 2 and 3 to check that ψ is an isomorphism. □

In view of this we speak of the localization of R at S. Also since $\frac{a}{s} = \frac{a}{1} \cdot \frac{1}{s}$ we usually write as^{-1} rather than $\frac{a}{s}$ for elements of R_S.

Particularly important is the case when elements of S are regular, in this case the natural map $R \to R_S$ is a monomorphism. We identity R with its image in R_S. Thus we may assume that R is a subring of R_S, we write r instead of $\frac{r}{1}$ for elements of R. In particular when R is an integral domain and $S = R \setminus \{0\}$ then R_S is just the field of fractions of R.

Lemma 4.25. *Let R be a ring and S a multiplicatively closed subset such that $S \subseteq \mathscr{C}(0)$. Then:*

1. *if $I \lhd R \Rightarrow IR_S \lhd R_S$ and every element of IR_S is expressible as xd^{-1} for some $x \in I$ and $d \in S$.*
2. *$K \lhd R_S \Rightarrow K \cap R \lhd R$ and $(K \cap R)R_S = K$.*

Proof. We are assuming that R is a subring of R_S. So a typical element of IR_S is $x_1r_1c_1^{-1} + \cdots + x_nr_nc_n^{-1}$ for some $x_i \in I, r_i \in R$ and $c_i \in S$. Let $d = c_1c_2 \ldots c_n$ and $d_i = c_1c_2 \ldots c_{i-1}c_{i+1} \ldots c_n$ then $x_1r_1c_1^{-1} + \cdots + x_nr_nc_n^{-1} = (x_1r_1d_1 + \cdots + x_nr_nd_n)d^{-1} = xd^{-1}$ where $x = x_1r_1d_1 + \cdots + x_nr_nd_n \in I$.

The rest is an exercise. □

Remark. If $I \lhd R$ we have $IR_S \cap R \supseteq I$ but we do not have equality in general. E.g. $R = \mathbb{Z}$ and $R_S = \mathbb{Q}$.

However, see Lemma 4.27 part 2 below.

Corollary 4.26. *If R is a Noetherian ring then so is the ring R_S.*

Proof. Clear from the previous lemma (part 2) □

Lemma 4.27. *Let R be a ring and S a multiplicatively closes subset. Suppose that the elements of S are regular. Then*

1. *If Π is a prime ideal of R_S then $\Pi \cap R$ is a prime ideal of R*
2. *If P is a prime ideal of R and $P \cap S = \emptyset$ then PR_S is a prime ideal of R_S and $PR_S \cap R = P$*

Proof.

1. Easy
2. We shall first need to show that $PR_S \cap R = P$. Clearly $PR_S \cap R \supseteq P$. Let $z \in PR_S \cap R$, then $z = ps^{-1}$ for some $p \in P$ and $s \in S$ Lemma 4.25 part 1. So $zs = p \in P$ with $z, s \in R$. Now $z \in P$ since $s \notin P$ and P is prime. Thus $PR_S \cap R = P$. Now let $\alpha\beta \in PR_S$ with $\alpha, \beta \in R_S$. Then $\alpha = ac^{-1}$ and $\beta = bd^{-1}$ where $a, b \in R$, $c, d \in S$. So $abc^{-1}d^{-1} \in PR_S$ hence $ab \in PR_S \cap R = P$. So $\alpha \in PR_S$ or $\beta \in PR_S$, hence PR_S is a prime ideal of R_S. (Note: $PR_S \neq R_S$ since $P \neq R$) □

Theorem 4.28. *Let R, S be as above. Then there is a one to one order preserving correspondence between the prime ideals of R which do not intersect S and the prime ideals of R_S*

Proof. This follows from the previous lemma. The correspondence is $P \leftrightarrow PR_S$. □

Remark. Theorems analogous to the above hold even when the elements of S are not assumed to be regular.

Notation. Of special importance is the case when P is a prime ideal and $S = R \setminus P = \mathscr{C}(P)$. In this case it is customary to write R_P instead of $R_{\mathscr{C}(P)}$ or $R_{R\setminus P}$.

Proposition 4.29. *Let P be a prime ideal of a ring R and suppose that the elements of $\mathscr{C}(P)$ are regular. Then PR_P is the unique maximal ideal of R_P and thus R_P is a local ring.*

Proof. Let $I \lhd R_P$, $I \neq R_P$. Then I does not contain a unit of R_P. $[I \cap R] \cap \mathscr{C}(P) = \emptyset$, i.e., $I \cap R \subseteq P$. So $I = (I \cap R)R_P \subseteq PR_P$, since $P \cap \mathscr{C}(P) = \emptyset$, $PR_P \neq R_P$. It follows that PR_P is the unique maximal ideal of R_P. □

Remark. Hence the name "localization"

Example. $R = \mathbb{Z}, P = 2\mathbb{Z}$, then $Z_{(2)} = \left\{\frac{a}{b} | a, b \in \mathbb{Z}, b \,\text{odd}\right\}$

4.4 Localisation of a Module [Commutative Algebra 3.1]

Let M be an R-module and S a multiplicatively closed subset of R such that $0 \notin S$, $1 \in S$. Define an equivalence relation on $M \times S$ as follows: $(m, s) \sim (m', s')$ if there exists $t \in S$ such that $(ms' - m's)t = 0$. Check that $\sim$ is an equivalence relation. Denote equivalence class of (m, s) by m/s. Let M_S be the collection of all such equivalence classes. Define

$$\frac{m}{s} + \frac{m'}{s} = \frac{ms' + m's}{ss'}, \frac{m}{s} \cdot \frac{r}{t} = \frac{mr}{st}, m, m' \in M, s, s', t \in S, r \in R$$

Check that this turns M_S into an R_S-module. Uniqueness corresponding to Theorem 4.24 can also be proved. We call M_S the *localization of M at S*.

Note that if A is an R_S-module then A can be considered an R-module via the action $a \cdot r = a \cdot \frac{r}{1} \forall a \in A, r \in R$. In this case $A \cong A_S$ as R_S-module [Check that $\frac{a}{c} \to a \cdot \frac{1}{c}$ is an isomorphism $A_S \to S$]

4.5 Symbolic Powers

Let P be a prime ideal. Then the powers of P need not be P-primary [Commutative Algebra Example after 6.3]

$P^{(n)} = \{x \in R | xc \in P^n$ for some $c \in \mathscr{C}(P\}$. Check that $P^{(n)} \lhd R$.

Definition 4.30. $P^{(n)}$ is called the n^{nt} *symbolic power of P*

Clearly $P^{(1)} = P$ and $P^{(n)} \subseteq P$ for all n.

Lemma 4.31. *$P^{(n)}$ is P-primary*

Proof. Let $ab \in P^{(n)}$, $a, b \in R$. Then $abc \in P^n$ for some $c \in \mathscr{C}(P)$. If no power of b lies in $P^{(n)}$ then $b \notin P$, i.e., $b \in \mathscr{C}(P)$, We have $a(bc) \in P^n$ with $bc \in \mathscr{C}(P)$. Hence $a \in P^{(n)}$ and $P^{(n)}$ is primary. It is easy to see that $\sqrt{P^{(n)}} = P$ □

Lemma 4.32. *Let P be a prime ideal and suppose that elements of $\mathscr{C}(P)$ are regular. Then fro every $n \geq 1$:*

1. $(PR_P)^n = P^n R_P$
2. $P^n R_P \cap R = P^{(n)}$
3. $P^{(n)} R_P = P^n R_P$

Proof.

1. $(PR_P)^n = P^n R_P^n = P^n R_P$
2. $x \in P^{(n)} \Rightarrow xc \in P^n$ for some $c \in \mathscr{C}(P)$. So $xcR_P \subseteq P^n R_P \Rightarrow xR_P \subseteq P^n R_P$ since c is a unit of R_P. Hence $x \in P^n R_P \cap R$.

   Conversely: $q \in P^n R_P \cap R \Rightarrow q = pc^{-1}$ with $p \in P^n$ and $c \in \mathscr{C}(P)$. Hence $qc = p \in P^n$, so $q \in P^{(n)}$ and noting that $q \in R$, we have$P^{(n)} = P^n R_P \cap R$
3. Exercise

□

4.6 The Rank of a Prime Ideal

Definition 4.33. A prime ideal P is said to have *rank r* (or *height r*) if there exists a chain of prime ideals $P_1 \subsetneq P_2 \subsetneq \cdots \subsetneq P_r \subsetneq P$ but none longer. If there does not exists a maximal finite chain of primes then we say $\operatorname{rk} P = \infty$. If P contains no other primes, we define $\operatorname{rk} P = 0$

Note that $\operatorname{rk} P = 0$ if and only if P is a minimal prime.

Definition 4.34. Let $a_1, \ldots, a_n \in R$, we say that prime P is *minimal over* $a_1, \ldots, a_n$ if $P/(a_1 R + \cdots + a_n R)$ is a minimal prime of the ring $R/(a_1 R + \cdots + a_n R)$.

Lemma 4.35. *Let R be a Noetherian ring, $A \lhd R$. Suppose that R/A is an Artinian ring. Then R/A^n is Artinian for all $n \geq 1$.*

Proof. $R/A \cong \frac{R/A^2}{A/A^2}$ (by the third isomorphism theorem). Note A/A^2 is finitely generated as an R/A-module, so by Corollary 3.9 A/A^2 is Artinian. Since R/A and A/A^2 are Artinian, it follows from Proposition 3.7 that R/A^2 is Artinian. The proof then extends by induction. □

Krull's Principal Ideal Theorem. *Let R be a Noetherian Ring. Let $a \in R$ be a non-unit, suppose that P is a prime ideal minimal over a. Then* $\operatorname{rk} P \leq 1$.

Proof. We shall first deal with the case when P is the unique maximal ideal of R, i.e., when R is a local ring with Jacobson radical P. Suppose we have $Q_1 \subseteq Q \subsetneq P$. Factoring out by Q_1 we may without loss of generality assume that R is an integral domain. In the ring R/aR, P/aR is both the unique maximal ideal and a minimal prime. Hence by Proposition 4.18 we have $P/aR = N(R/aR)$. By Proposition 3.20(Check this reference) there exists an integer $n \geq 1n$ such that $P^n \subseteq aR$.

Now R/P is a field so by Lemma 4.35 R/P^n is Artinian. Hence R/aR is an Artinian ring. Hence there exists $k \geq 1$ such that $Q^{(k)} + aR = Q^{(k+1)} + aR$. So $Q^{(k)} \subseteq Q^{(k+1)} + aR$. Let $x \in Q^{(k)}$, then $x = y + at$ for some $y \in Q^{(k+1)}$, $t \in R$. Hence $at = x - y \in Q^{(k)}$. Now $a \notin Q$ since P is minimal over a. So $t \in Q^{(k)}$, thus $Q^{(k)} \subseteq Q^{(k+1)} + aQ^{(k)}$. Hence $Q^{(k)} = Q^{(k+1)} + aQ^{(k)}$ (since the other containment is true trivially). Hence $\left[\frac{Q^{(k)}}{Q^{(k+1)}}\right] = \left[\frac{Q^{(k)}}{Q^{(k+1)}}\right] aR$ where [] is viewed as an R-module.

So $\frac{Q^{(k)}}{Q^{(k+1)}} = 0$ by Nakayama's Lemma since $aR \subseteq J(R)$, so $Q^{(k)} = Q^{(k+1)}$. Now localize at Q. So $Q^{(k)}R_Q = Q^{(k+1)}R_Q$ and $Q^kR_Q = Q^{k+1}R_Q$ by Lemma 4.32 part 3. So $(QR_Q)^k = (QR_Q)^{k+1}$ by Lemma 4.32 part 1. So $(QR_Q)^k = 0$ by Nakayama's Lemma since $QR_Q = J(R_Q)$. Hence $Q^k = 0$ and hence $Q = 0$ since R is a domain.

Now in the general case again suppose that $Q_1 \subseteq Q \subsetneq P$. Factor out Q_1 and assume that R is an integral domain. Now localize at P. Factor out Q_1 and assume that R is an integral domain. Now localise at P, by Theorem 4.28, there exists an inclusion preserving one to one correspondence between primes of R lying inside P and primes of the ring R_P. Use this and the first part of the proof applied to the ring R_P to finish the proof. □

The Generalised Principal Ideal Theorem. *Let R be a commutative Noetherian ring. Suppose that P is a prime ideal minimal over the elements $x_1, \ldots, x_r \in R$. Then* $\operatorname{rk} P \leq r$.

Proof. We prove this by induction

For $r = 1$ we use Krull's Principal Ideal Theorem.

Now assume the result is true for primes minimal over $\leq r-1$ elements. Suppose that P is minimal over $x_1, \ldots, x_r$ and suppose that we can construct a chain of primes $P = P_0 \supsetneq P_1 \supsetneq \cdots \supsetneq P_{r+1}$. If $x_1 \in P_r$ then in the ring R/x_1R we have a chain of primes $P_0/x_1R \supsetneq P_1/x_1R \supsetneq \cdots \supsetneq P_r/x_1R$ $(*)$ But P_0/x_1R is minimal over the images of $x_2, \ldots, x_r$ in the ring R/x_1R. So $(*)$ contradicts the induction. So $x_1 \notin P_r$.

Let k be such that $x_1 \in P_k$ but $x_1 \notin P_{k+1}$. So we have $P_k/P_{k+2} \supseteq \frac{P_{k+2}+x_1R}{P_{k+2}} \supsetneq P_{k+2}/P_{k+2}$. By Krull's Principal Ideal Theorem P_k/P_{k+2} can not be minimal over $[x_1 + P_{k+2}]$ (since otherwise we have $P_k/P_{k+2} \supsetneq P_{k+1}/P_{k+2} \supsetneq P_{k+2}/P_{k+2}$). So there exists a prime ideal P'_{k+1} such that $P_k \supsetneq P'_{k+1} \supseteq P_{k+2} + x_1R \supsetneq P_{k+2}$. Proceeding this way we can build a new chain $P = P_0 \supsetneq P_1 \supsetneq \cdots \supsetneq P_k \supsetneq P'_{k+1} \supsetneq \cdots \supsetneq P'_r \supsetneq P_{r+1}$. Now we have $x_1 \in P'_r$ and this leads to a contradiction as in $(*)$. □

Definition 4.36. Let R be a commutative ring. We define the *Krull dimension* of R by $K\dim(R) = \sup_{P \text{ prime}} \operatorname{rk} P$.

Note. $K\dim$ can be infinite in a Noetherian ring even thought the rank of each prime ideal is finite.

Proposition 4.37. *Let R be a commutative Noetherian local ring with Jacobson radical J. Then $K\dim(R) = \operatorname{rk} J < \infty$.*

Proof. Since R is local, $K\dim(R) = \operatorname{rk} J$, and $\operatorname{rk} J < \infty$ by the Generalised Principal Ideal Theorem as it is minimal over its generators. □

Lemma 4.38. *Let R be a commutative Noetherian local ring with $K\dim(R) = n$. Then $K\dim(R/cR) \geq n-1$. Further, if c is regular then equality holds.*

Proof. Let J be the maximal ideal of R. Then $\operatorname{rk} J = n$, so there exists a chain of primes $J = P_0 \supsetneq P_1 \supsetneq \cdots \supsetneq P_n$. As in the Generalised Principal Ideal Theorem we can construct a new chain of primes, $J = Q_0 \supsetneq Q_1 \supsetneq \cdots \supsetneq Q_{n-1}$ with $c \in Q_{n-1}$. Hence $\operatorname{rk}(J/cR) \geq n-1$ $(*)$.

Now assume that c is regular. If $J/cR = T_0/cR \supsetneq \cdots \supsetneq T_k/cR$ is a chain of primes in R/cR then $J = T_0 \supsetneq T_1 \supsetneq \cdots \supsetneq T_k$ is a chain of primes in R. Since c is regular by Proposition 4.18 T_k can not be a minimal prime of R since $c \in T_k$. So $n = \operatorname{rk} J \geq \operatorname{rk} J/cr + 1$. Hence $\operatorname{rk} J/cR = n-1$ from $(*)$ when c is regular. □

4.7 Regular Local Ring

Let R be a Noetherian local ring with Jacobson radical J. We have $V(R) = \dim J/J^2$ as a vector space over the field R/J. So $V(R)$ =the number of elements in a minimal generator set for J by Corollary 3.23. By The Generalised Principal Ideal Theorem we have $\operatorname{rk} J \leq V(R)$

Definition 4.39. A Noetherian local ring is called a *regular local ring* if $\operatorname{rk}(J) = V(R)$.

A local principal ideal domain is regular by Theorem 4.12

Lemma 4.40. *Let R be a Noetherian local ring with Jacobson radical J (R not a field). Suppose that $x \in J \setminus J^2$, let $R^* = R/xR$. Then $V(R^*) = V(R) - 1$.*

Proof. Note that R^* is a Noetherian local ring with Jacobson radical $J^* = J/xR$. Let $y_1^*, \ldots, y_k^*$ be a minimal generating set for J^*. Choose $y_1, \ldots, y_k \in J$ such that $y_i \mapsto y_i^*$ under the natural homomorphism $R \to R/xR$. Claim $x, y_1, \ldots, y_k$ is a minimal generating set for J. We shall now show that the homomorphic images of $x, y_1, \ldots, y_k$ in the vector space J/J^2 are linearly independent. Suppose that $xr + y_1r_1 + \cdots + y_kr_k \in J^2$ $(*)$. So $y_1^*r_1^* + \cdots + y_k^*r_k^* \in (J^*)^2$ where r_i^* are the homomorphic images of r_i under $R \to R/xR$. It follows that $r_i^* \in J^*$ since $y_1^*, \ldots, y_k^*$ is a minimal generating set for J^* and $\dim J^*/(J^*)^2 = k$. So $r_i \in J$ for all i. It follows from $(*)$ that $xr \in J^2$ since $r_i, y_i \in J$. So $r \in J$ since $x \notin J^2$. (Note that J^2 is J-primary check!) This completes the proof. □

Theorem 4.41. *Let R be a regular local ring with Jacobson radical J. Suppose that $x \in J \setminus J^2$. Then the ring $R^* = R/xR$ is also regular local.*

Proof.

$$\begin{aligned}
V(R) - 1 &= V(R^*) && \text{by the previous lemma} \\
&\geq \operatorname{rk} J^* && \text{where } J^* = J/xR \text{ by the General Principal Ideal Theorem} \\
&\geq \operatorname{rk} J - 1 && \text{by Theorem 4.38} \\
&= V(R) - 1
\end{aligned}$$

So $V(R^*) = \operatorname{rk} J^*$. Thus R^* is a regular local ring □

Remark. We have also shown that $\operatorname{rk} J^* = \operatorname{rk} J - 1$.

Lemma 4.42. *Let R be a Noetherian local ring which is not an integral domain. Let $P = pR$ ($p \in P$) be a prime ideal. Then* $\operatorname{rk} P = 0$.

Proof. Suppose that $Q \subsetneq P$ where Q is a prime ideal. Then $p \notin Q$. Now $q \in Q$ implies $q = pt$ for some $t \in R$. Hence $pt \in Q \Rightarrow t \in Q$ since $p \notin Q$. So $q \in pQ \subseteq P^2 \subseteq p^2R$. Preceding this way we have $Q \subseteq P^n$ for all $n \geq 1$, so $Q \subsetneq \cap_{n=1}^{\infty} P^n \subseteq \cap_{n=1}^{\infty} J$ where $J = J(R)$. But by Theorem 4.9 $\cap_{n=1}^{\infty} J^n = 0$, so $Q = 0$ which is a contradiction since R is not a domain. Hence $\operatorname{rk} P = 0$ □

Theorem 4.43. *A regular local ring is an integral domain.*

Proof. By induction on $K\dim R = \operatorname{rk} J$. If $\operatorname{rk} J = 0$ then R must be a field.

Suppose now that $\operatorname{rk} J = n > 0$ and assume result for rings of $K\dim < n$. Since $J \neq J^2$ by Nakayama's lemma choose $x \in J \setminus J^2$. By Theorem 4.41, $R^* = R/xR$ is regular local. Also $K\dim R^* = K\dim R - 1$. By induction hypothesis R^* is an integral domain, i.e., xR is a prime ideal. Suppose that R is not an integral domain, then by Lemma 4.42 xR is a minimal prime. Let $P_1, \ldots, P_k$ be the minimal primes of R. We have show that $J \setminus J^2 \subseteq P_1 \cup \cdots \cup P_k$. So $J \subseteq J^2 \cup P_1 \cup \cdots \cup P_2$. So $J \subseteq P_j$ for some j by Lemma 4.19 hence $J = P_j$. So $\operatorname{rk} J = 0$, which is a contradiction. So R is an integral domain. □

5 Projective Modules

All rings in this chapter are assumed to have 1 but need not be commutative.

Suppose R is regular local and P prime. How about the ring R_P?

5.1 Free Modules

Definition 5.1. A right R-module M is said to be *free* if:

1. M is generated by a subset $S \subseteq M$
2. $\sum_{\text{finite}} a_i r_i = 0$ if and only if $r_i = 0 \forall r_i \in R, a_i \in S$.

Then S is called a *free basis for* M.

Remark. 1. R_R is free with free basis 1

2. In a free module not every minimal generating set is a free basis. e.g: in the ring of 2×2 matrices over $\mathbb{Q}$, $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ is a minimal generating set but not a free basis.
3. By convention, 0 is considered to be a free module on the empty free basis.

Lemma 5.2. *Let R be a commutative ring, then any two free basis of a free R-module have the same cardinality.*

Proof. By Theorem 2.2, R contains a maximal ideal, M say. Then R/M is a field. Let A be a free R-module with a free basis $\{x_\lambda\}_{\lambda \in \Lambda}$. We claim: $\frac{x_\lambda R}{x_\lambda M} \cong \frac{R}{M}$ (as R and hence as R/M-modules). To see this, define $\theta : R \to \frac{x_\lambda R}{x_\lambda M}$ by $\theta(r) = x_\lambda r + x_\lambda M$. Then θ is an R-homomorphism and $\ker \theta \supseteq M$. But M is maximal, so $\ker(\theta) = M$, proving our claim.

Write $B_\lambda = \frac{x_\lambda R}{x_\lambda M}$, since $B_\lambda \cong R/M$ each B_λ is a 1-dimensional vector space over the field R/M. From the external direct sum $\sum_{\lambda \in \Lambda} \oplus B_\lambda$. Now A/AM is an R/M-module. (see Section 1.11). We have $A/AM \cong \sum_{\lambda \in \Lambda} \oplus B_\lambda$ (as R-modules and hence also as R/M-modules). Hence dimension of A/AM as a vector space is $|\Lambda|$. The dimension of A/AM is invariant by vector space theory, hence the result. $\square$

Remark. Over a non-commutative ring it is possible to have $R \cong R \oplus R$ as right R-modules.

The Free Module F_A. Let A be a set indexed by Λ. We define F_A to be the set of all symbols $\sum a_\lambda r_\lambda$ with $a_\lambda \in A, r_\lambda \in R, \lambda \in \Lambda$, where all but a finite number of r_λ are zero. We further require these expression to satisfy $\sum a_\lambda r_\lambda = \sum a_\lambda s_\lambda \iff r_\lambda = s_\lambda \, \forall \lambda \in \Lambda$. We can make F_A a right R-module by defining $\sum a_\lambda r_\lambda + \sum a_\lambda s_\lambda = \sum a_\lambda (r_\lambda + s_\lambda)$ and $(\sum a_\lambda r_\lambda) r = \sum a_\lambda (r_\lambda r)$ (for all $r_\lambda, s_\lambda, r \in R$)

A is a free basis for F_A (identifying $a \in A$ with $a \cdot 1 \in F_A$)

Proposition 5.3. *Every right R-module is a homomorphism image of a free right R-module*

Proof. Let M be a right R-module. Index the elements of M and form the free right R-module F_M. Elements of F_M are formal sums of the form $\sum (m_i) r_i$, $m_i \in M, r_i \in R$. Define $F_M \to M$ by $\sum (m_i) r \mapsto \sum m_i r_i \in M$. This map is well-defined and is an R-homomorphism by the definition of F_M. $\square$

5.2 Exact Sequences

Let M_i be right R-modules and f_i R-homomorphism of M_i into M_{i-1}. The sequence (which maybe finite or infinite) $\cdots \xrightarrow{f_{i+2}} M_{i+1} \xrightarrow{f_{i+1}} M_i \xrightarrow{f_i} M_{i-1} \xrightarrow{f_{i-1}} \cdots$ is said to be *exact* if $\operatorname{im} f_{i+1} = \ker f_i$ for all i.

A *short exact sequence* (s.e.s.) is an exact sequence of the form $0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$. Note that since $0 \longrightarrow M' \xrightarrow{f} M$ is exact we have $\ker(f) = 0$, i.e., f is a monomorphism. Similarly we have $M \xrightarrow{g} M'' \longrightarrow 0$ is exact so $M'' = \operatorname{im}(g)$, i,e, g is an epimorphism. We have $M' \cong f(M')$, i.e., M' is isomorphic to a submodule of M. Also $M'' \cong M/\ker(g) = M/f(M')$.

Given modules $B \subseteq A$, we can construct the short exact sequence $0 \longrightarrow B \xrightarrow{i} A \xrightarrow{\pi} A/B \longrightarrow 0$ where i is the inclusion map and π the canonical homomorphism.

Proposition 5.4 (c.f. Graduate Algebra Theorem 5.3)**.** *Given a short exact sequence*
$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, shift left, "\alpha"] & B \arrow[l, shift left, dashed, "\delta"] \arrow[r, shift left, "\beta"] & C \arrow[l, shift left, dashed, "\gamma"] \arrow[r] & 0 \end{tikzcd},$$
the following conditions are equivalent.

1. $\operatorname{im}\alpha$ *is a direct summand of* B
2. *There exists a homomorphism* $\gamma : C \to B$ *such that* $\beta\gamma = 1_C$
3. *There exists a homomorphism* $\delta : B \to A$ *such that* $\delta\alpha = 1_A$

Proof. 1. $\Rightarrow$ 2.) Let $B = \operatorname{im}(\alpha) + B_1 = \ker\beta + B_1$. Let β_1 be the restriction of β to B_1. We have $\beta B = \beta_1 B_1 = C$, so β_1 is an epimorphism. Also $\ker\beta_1 \subseteq \operatorname{im}\alpha \cap B_1 = 0$. Hence β_1 is an isomorphism and $C \cong B_1$. Define $\gamma : C \to B$ to be the inverse of β_1. It follows that γ

2. $\Rightarrow$ 1.) We shall show that $B = \alpha(A) + \gamma\beta(B) = \ker\beta + \gamma\beta(B)$. Let $b \in B$, then $b = (b - \gamma\beta b) + \gamma\beta b$. Now $b - \gamma\beta b \in \ker\beta$ since $\beta(b - \gamma\beta b) = \beta b - \beta\gamma\beta b = \beta b - 1_C\beta b = \beta b - \beta b = 0$. If $z \in \ker\beta \cap \gamma\beta B$ means $z = \gamma\beta b$ for some $b \in B$ and $\beta(z) = 0$. This means $0 = \beta(x) = \beta\gamma\beta b = \beta b \Rightarrow x = 0$. Thus $B = \ker(\beta) \oplus \gamma\beta(B)$

Similarly we can show $1 \iff 3$. $\square$

Definition 5.5. We say that the short exact sequence *split* if any (and hence all) of the above condition holds.

Note that if the above short exact sequence split then we have $B = \operatorname{im}\alpha \oplus B_1 \cong A \oplus C$ (external direct sum)

Definition 5.6. A right R-module P is said to be *projective* if every diagram of the from

$$\begin{tikzcd} & P \arrow[d, "\mu"] & \\ A \arrow[r, "\pi"] & B \arrow[r] & 0 \text{ exact} \end{tikzcd}$$

can be embedded in he diagram

$$\begin{tikzcd} & P \arrow[d, "\mu"] \arrow[dl, dashed, "\overline{\mu}"'] & \\ A \arrow[r, "\pi"] & B \arrow[r] & 0 \end{tikzcd}$$

in such a way that $\pi\overline{\mu} = \mu$. ("the diagram commutes")

Lemma 5.7. *A free module is projective.*

Proof. Let F be a free right module with a free basis $\{e_\alpha\}$. Consider

$$\begin{tikzcd} & F \arrow[d, "\mu"] \arrow[dl, dashed, "\overline{\mu}"'] & \\ A \arrow[r, "\pi"] & B \arrow[r] & 0 \text{ exact} \end{tikzcd}$$

Let $b_\alpha = \mu e_\alpha$. As π is an epimorphism, we can choose $a_\alpha \in A$ such that $\pi a_\alpha = b_\alpha$. Now define $\overline{\mu} : F \to A$ by $\overline{\mu}(\sum e_\alpha r_\alpha) = \sum a_\alpha r_\alpha$, $r_\alpha \in R$. Then $\overline{\mu}$ is an R-homomorphism $F \to A$ and $\pi\overline{\mu}(\sum e_\alpha r_\alpha) = \pi(\sum a_\alpha r_\alpha) = \sum \pi(a_\alpha) r_\alpha = \sum b_\alpha r_\alpha = \sum \mu(e_\alpha) r_\alpha = \mu(\sum e_\alpha r_\alpha)$. Therefore $\pi\overline{\mu} = \mu$. $\square$

A projective module need not be free. To be shown later.

Lemma 5.8. *Let* P_α $(\alpha \in \Lambda)$ *be right* R*-modules. Then* $\sum_{\alpha\in\Lambda} \oplus P_\alpha$ *is projective if and only if all* P_α *are projective*

Proof. Let i_α be the injection map $P_\alpha \to \sum_{\alpha\in\Lambda} \oplus P_\alpha$ and let p_α be the projection map $\sum_{\alpha\in\Lambda} \oplus P_\alpha \to P_\alpha$

$\Leftarrow$ Consider the diagram

$$\begin{tikzcd} & \sum \oplus P_\alpha \arrow[d, "f"] & \\ A \arrow[r, "\pi"] & B \arrow[r] & 0 \end{tikzcd}$$

Restrict f to P_α, $f|_{P_\alpha} = f_\alpha$ say. Then $f_\alpha = f i_\alpha$. Since each P_α is projective, there exists maps $\overline{f_\alpha} : P_\alpha \to A$ such that $\pi\overline{f_\alpha} = f_\alpha$. Define $\overline{f} = \sum_{\alpha\in\Lambda} \overline{f_\alpha} p_\alpha$. Then $\pi\overline{f} = \sum_{\alpha\in\Lambda} \pi\overline{f_\alpha} p_\alpha = \sum_{\alpha\in\Lambda} f_\alpha p_\alpha = \sum_{\alpha\in\Lambda} f i_\alpha p_\alpha = f$. So $\sum_{\alpha\in\Lambda} \oplus P_\alpha$ is projective.

$\Rightarrow$ For any $\beta \in \Lambda$ consider

$$\begin{tikzcd} & P_\beta \arrow[d, "f_\beta"] & \\ A \arrow[r, "\pi"] & B \arrow[r] & 0 \end{tikzcd}$$

This gives rise to

$$\begin{tikzcd} & \sum \oplus P_\alpha \arrow[dl, "\overline{f}"'] \arrow[d, "f_\beta p_\beta"] & \\ A \arrow[r, "\pi"] & B \arrow[r] & 0 \end{tikzcd}$$

So there exists $\overline{f} : \sum_{\alpha\in\Lambda} \oplus P_\alpha \to A$ such that $\pi\overline{f} = f_\beta p_\beta$. Hence $\pi\overline{f} i_\beta = f_\beta p_\beta i_\beta = f_\beta$ and $\overline{f} i_\beta$ maps $p_\beta \to A$.

□

Proposition 5.9. *The following conditions are equivalent:*

1. *P is a projective right R-module*
2. *P is a direct summand of a free module*
3. *Every short exact sequence* $0 \longrightarrow M' \longrightarrow M \longrightarrow P \longrightarrow 0$ *splits.*

Proof. $3 \Rightarrow 2$ Consider the short exact sequence $0 \longrightarrow K_P \longrightarrow F_p \longrightarrow P \longrightarrow 0$ where K_P is the kernel of the map $F_P \to P$. Since this sequence splits, $F_P \cong P \oplus K_P$

$2 \Rightarrow 1$ Follows from Lemma 5.7 and Lemma 5.8

$1 \Rightarrow 3$ Consider

$$\begin{tikzcd} & & & P \arrow[dl, dashed, "\overline{\mu}"'] \arrow[d, "1_P"] & \\ 0 \arrow[r] & M' \arrow[r, "f"] & M \arrow[r, "g"] & P \arrow[r] & 0 \end{tikzcd}$$

Since P is projective, there exists $\overline{\mu} : P \to M$ such that $g\overline{\mu} = 1_P$. Thus the short exact sequence splits.

□

Example. Projective does not imply Free. Let $R = \mathbb{Z}/6\mathbb{Z}$, $A = 2\mathbb{Z}/6\mathbb{Z}$ and $B = 3\mathbb{Z}/6\mathbb{Z}$, then $A, B \lhd R$ and $R = A \oplus B$. A being a direct summand of R is projective, but is not free since it has fewer elements than R

Theorem 5.10. *Over a commutative local ring, finitely generated projective modules are free.*

Proof. Let R be a commutative local ring with unique maximal ideal J. Let M be a finitely generated R-module. Let $\{a_1, \ldots, a_n\}$ be a minimal set of generators for M. Then there exists a free module with a free basis $\{x_1, \ldots, x_n\}$ and an R-homomorphism $\phi : F \overset{\text{onto}}{\to} M$ such that $\phi(x_i) = a_i$ (See note on page 25, Question 1 on Exercise sheet 6 or Commutative Algebra). Thus we have $0 \longrightarrow K \longrightarrow F \xrightarrow{\phi} M \longrightarrow 0$ where $K = \ker(\phi)$.

Claim: $K \subseteq FJ$. If not there exists an element $k = x_1r_1 + \cdots + x_nr_n$ ($r_i \in R$) of F such that $k \in K$ but $r_i \notin J$ for some i. Say $r_1 \notin J$. Since R is local, r_1 must be a unit. Since $k \in \ker\phi$, $a_1r_1 + \cdots + a_nr_n = 0$. So $a_1 = -r_1^{-1}(a_2r_2 + \cdots + a_nr_n)$ contradiction the fact that $\{a_1, \ldots, a_n\}$ was a minimal generating set. Thus $K \subseteq FJ$.

Now since M is projective, the above short exact sequence split. So $F = K \oplus M'$ where $M' \cong M$. Hence $FJ = KJ \oplus M'J$. So $K = FJ \cap K = K \cap (KJ \oplus M'J) = KJ \oplus (K \cap M'J)$ by the modular law. But $K \cap M'J \subseteq K \cap M' = 0$, so $K = KJ$. Now K is finitely generated (check this!). By Nakayama's Lemma $K = 0$, thus M' and hence M is free. □

Remark. Kaplansky has shown that the result is true even without the finitely generated assumption.

The Dual Basis Lemma

Let R be a commutative integral domain with a field of fraction K. Let $0 \neq A \lhd R$ and define $A^* = \{k \in K : kA \subseteq R\}$. Then A^* is an R-module.

Lemma 5.11. *Let R,K, A be as above. Let $\theta : A \to R$ be an R-homomorphism. Then there exists $q \in A^*$ such that $\theta(x) = qx$ for all $x \in A$.*

Proof. $AK = K$. So a typical element of K is expressible as ac^{-1} with $a, c \in R$, $c \neq 0$. Now θ can be extended to a K-homomorphism, $\theta^* : K \to K$ by $\theta^*(ac^{-1}) = \theta(a)c^{-1}$. Check that θ^* is well defined and K-homomorphism. Let $\theta^*(1) = q \in K$. Then for $x \in A$, $\theta(x) = \theta^*(x) = \theta^*(1x) = \theta^*(1)x = qx$. Clearly $q \in A^*$. □

Proposition 5.12 (The Dual Basis Lemma - Special Case)**.** *With the notation as above: A_R is projective if and only if $1 = x_1q_1 + \cdots + x_nq_n$ for some $x_i \in A$, $q_i \in A^*$. (Or equivalently $A^*A = R$)*

Proof. $\Rightarrow$) Let F be a free module with an R-homomorphism $\phi : F \twoheadrightarrow A$. Since A is projective, there exists an R-homomorphism $\psi : A \to F$ such that $\phi\psi = 1_A$

$$F \underset{\psi}{\overset{\phi}{\rightleftarrows}} A\,.$$

Let $\{f_\alpha\}$ be a free basis for F. Then for each $y \in A$, we have $\psi(y) = f_1r_1 + \cdots + f_nr_n$ uniquely for some $f_i \in \{f_\alpha\}$ and $r_i \in R$. So for each i, $y \to r_i$ is an R-homomorphism $A \to R$. So by the previous lemma, there exists $q_i \in A^*$ such that $\psi(y) = f_1q_1y + \cdots + f_nq_ny$. So

$$\begin{aligned} y &= \phi\psi(y) \\ &= \phi(f_1q_1y + \cdots + f_nq_ny) \\ &= \phi(f_1)q_1y + \cdots + \phi(f_n)q_ny \text{since } q_iy \in R \end{aligned}$$

So $1 = \phi(f_1)q_1 + \cdots + \phi(f_n)q_n = x_1q_1 + \cdots + x_nq_n$, where $x_i = \phi(f_i) \in A$.

$\Leftarrow$) Define $\psi : A \to \underbrace{R \oplus \cdots \oplus R}_{n-\text{times}}$ by $\psi(x) = (q_1x, \ldots, q_nx)$ for all $x \in A$.

$$A \underset{\phi}{\overset{\psi}{\rightleftarrows}} R \oplus \cdots \oplus R$$

Note that $q_ix \in R$ since $q_i \in A^*$. Define $\phi : \underbrace{R \oplus \cdots \oplus R}_{n-\text{times}} \to A$ by $\phi(r_1, \ldots, r_n) = x_1r_1 + \cdots + x_nr_n$, $r_i \in R$Then ϕ is an R-homomorphism and for any $y \in A$

$$\begin{aligned} \phi\psi(y) &= \phi(q_1y, \ldots, q_ny) \\ &= x_1q_1y + \cdots + x_nq_ny \\ &= y \end{aligned}$$

So $\phi\psi = 1_A$, hence A_R is projective.

$\square$

Proposition 5.13. *Let R be a commutative Noetherian integral domain and $I \lhd R$. Suppose that IR_M is a projective R_M-module for each maximal ideal M of R. Then I_R is projective.*

Proof. $I = 0$ is trivial so assume $I \neq 0$.

Proof. Let F be the field of fractions of R. Then F is also the field of fractions of each R_M (check!). Consider a maximal ideal M. Since IR_M is R_M-projective by the Dual Basis Lemma, there exists some $x_i' \in IR_M$ and $q_i \in F$ such that $1 = x_1'q_1 + \cdots + x_n'q_n$ and $q_iI \subseteq R_M$. Now q_iI is a finitely generated R-module. So $q_iI = z_1R + \cdots + z_kR$ with $z_i \in R_M$. Let $a \in R$ be a common denominator of the x_i', let $b \in R$ be a common denominator of the z_j. Let $d = ab$, then $d \in \mathscr{C}(M)$, $d = x_1(q_1b) + \cdots + x_n(q_nb)$ where $x_i = x_i'a \in I$ and $q_ibI \subseteq R\,(\dagger)$.

Now $I^*I \lhd R$, by $(\dagger)$ $I^*I \cap \mathscr{C}(M) \neq \emptyset$. This is true for all maximal ideal M. Hence $I^*I = R$. Thus $1 \in I^*I$ and so I_R is projective by the dual basis lemma. $\square$

$\square$

Remark. This is a special case of a standard result. If A is a finitely generated module over a commutative Noetherian ring R then A_R is projective if and only if A_M is a projective R_M-module for all maximal ideal M. See:

- Marsumura: Commutative ring Theory Theorem 7.12
- Rotman: Intro to homological algebra Exercise 9.22 p258

5.3 Projective Resolutions and Projective Dimension

Definition 5.14. If A is a right R-module, and exact sequence

$$\cdots \longrightarrow P_n \xrightarrow{\partial_n} P_{n-1} \xrightarrow{\partial_{n-1}} \cdots \xrightarrow{\partial_1} P_0 \xrightarrow{\epsilon} A \longrightarrow 0$$

where each P_i is projective is called a *projective resolution* for A. (This sequence may be finite or infinite)

Construction of a Projective Resolution

Let A be a right R-module. A is a homomorphic image of a free module, say F_0 (by Proposition 5.3). So we have the exact sequence $0 \longrightarrow K_0 \xrightarrow{i} F_0 \xrightarrow{\alpha} A \longrightarrow 0$, where α is the homomorphism $F_0 \twoheadrightarrow A$ and $K_0 = \ker\alpha$ and i =inclusion map. If K_0 is projective the above is a projective resolution.

Even if K_0 is not projective it is still a homomorphic image of a free module, say F_1. So we have the exact sequence $0 \longrightarrow K_1 \longrightarrow F_1 \xrightarrow{\beta} K_0 \longrightarrow 0$ where $K_1 = \ker\beta$. Let $i\beta = \gamma$. Thus γ maps $F_1 \to F_0$ and we have $\ker\alpha = K_0 = \operatorname{im}\beta = \operatorname{im}\gamma$. So we have the exact sequence

$$0 \longrightarrow K_1 \longrightarrow F_1 \longrightarrow F_0 \longrightarrow A \longrightarrow 0$$

Here F_1 and F_0 are free and hence projective. If K_1 is not projective the procedure can be repeated. It may happen that after a finite number of steps we get an exact sequence

$$0 \longrightarrow K_n \longrightarrow F_n \longrightarrow F_{n-1} \longrightarrow \cdots \longrightarrow F_1 \longrightarrow F_0 \longrightarrow A \longrightarrow 0$$

where the K_n are projective and all the F_i are free.

Definition 5.15. A right R-module A is said to have *finite projective dimension* if there exists an exact sequence

$$0 \longrightarrow P_k \longrightarrow P_{k-1} \longrightarrow \cdots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow A \longrightarrow 0$$

where each P_i is projective. k is called the *length* of this sequence.

Further, we say that A has *projective dimension* n if n is the least integer for which there exists a projective resolution

$$0 \longrightarrow P_n \longrightarrow P_{n-1} \longrightarrow \dots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow A \longrightarrow 0$$

We denote the projective dimension of A by $\mathrm{pd}_R(A)$ (or simply $\mathrm{pd}(A)$) If A does not have finite projective dimension we write $\mathrm{pd}\, A = \infty$. If $A = 0$ we take $\mathrm{pd}\, A = -1$ conventionally.

It is clear that $\mathrm{pd}\, A = 0$ if and only if A is projective.

Schanuel's Lemma. *Let M be a right R-module and let*

$$0 \longrightarrow K \xrightarrow{\overline{f}} A \xrightarrow{f} M \longrightarrow 0 \qquad 0 \longrightarrow K' \xrightarrow{\overline{g}} Y \xrightarrow{g} M \longrightarrow 0$$

be two short exact sequence. If X and Y are projective then $X \oplus K' \cong Y \oplus K$.

Proof. Define $L = \{(x, y) | x \in X, y \in Y$ such that $f(x) = g(y)\}$. Then L is a submodule of $X \oplus Y$.

$$\begin{tikzcd} & X \arrow[dl, dashed, "\alpha"'] \arrow[d, "f"] & \\ Y \arrow[r, "g"] & M \arrow[r] & 0 \end{tikzcd}$$

Since X is projective there exists an R homomorphism $\alpha : X \to Y$ such that $f = g\alpha$. Define $\theta : X \oplus K' \to X \oplus Y$ by $\theta(x, k') = (x, \alpha(x) + \overline{g}(k')$ with $x \in X, k' \in K'$. θ is clearly an R-homomorphism, also $g(\alpha(x) + \overline{g}(k)) = g\alpha(x) + g\overline{g}(k') = f(x) + 0$. Thus θ is an R-homomorphism $X \oplus K' \to L$. Now $\theta(x, k') = 0 \Rightarrow x = 0$ and $\overline{g}(k') = 0 \Rightarrow x = 0$ and $k' = 0$. Thus θ is a monomorphism.

Finally if $(x, y) \in L$ then $f(x) = g(y)$, so $g\alpha(x) = g(y)$. So $g[-\alpha(x) + y] = 0$. Hence $-\alpha(x) + y \in \ker g = \mathrm{im}(\overline{g}) = \overline{g}(K')$. Hence there exists $k_1' \in K'$ such that $g(k_1') = -\alpha(x) + y$. Thus $\theta(x, k') = (x, y)$ and θ is an epimorphism.

So we have $X \oplus K' \cong L$ and $Y \oplus K \cong L$ and we are done. $\square$

Corollary 5.16. *In the above situation K is projective if and only if K' is projective.*

Remark. For free modules the result corresponding to Schanuel's Lemma does not work.

Generalised Schanuel's Lemma. *Suppose that A is a right R-module and we have two exact sequences of R-modules*

$$0 \longrightarrow K_n \longrightarrow P_n \longrightarrow P_{n-1} \longrightarrow \dots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow A \longrightarrow 0$$

$$0 \longrightarrow K_n' \longrightarrow P_n' \longrightarrow P_{n-1}' \longrightarrow \dots \longrightarrow P_1' \longrightarrow P_0' \longrightarrow A' \longrightarrow 0$$

with P_j, P_j' projective for $j = 1, 2, \dots, n$. Then $K_n \oplus P_n' \oplus P_{n-1} \oplus \dots \oplus \begin{cases} P_0 & n \text{ odd} \\ P_0' & n \text{ even} \end{cases} \cong K_n' \oplus P_n \oplus P_{n-1}' \oplus \dots \oplus \begin{cases} P_0' & n \text{ odd} \\ P_0 & n \text{ even} \end{cases}$.

Proof. By induction on n. If $n = 0$ this is just Schanuel's lemma.

So assume the result for $n = j - 1$, i.e., $K_{j-1} \oplus P_{j-1}' \oplus \dots \cong K_{j-1}' \oplus P_{j-1} \oplus \dots$ where $K_t = \ker$ of map $P_t \to P_{t-1}$ and $K_t' = \ker$ of map $P_t' \to P_{t-1}'$. So we have the exact sequences

$$0 \longrightarrow K_j \longrightarrow P_j \longrightarrow K_{j-1} \longrightarrow 0$$

$$0 \longrightarrow K_j' \longrightarrow P_j' \longrightarrow K_{j-1}' \longrightarrow 0$$

we obtain

$$0 \longrightarrow K_j \longrightarrow P_j \oplus P_{j-1}' \oplus P_{j-2} \oplus \dots \longrightarrow K_{j-1} \oplus P_{j-1}' \oplus P_{j-2} \oplus \dots \longrightarrow 0$$

$$0 \longrightarrow K'_j \longrightarrow P'_j \oplus P_{j-1} \oplus P'_{j-2} \oplus \ldots \longrightarrow K'_{j-1} \oplus P_{j-1} \oplus P'_{j-2} \oplus \ldots \longrightarrow 0$$

In both these sequences the middle terms are projective and the right hand side terms are isomorphic by induction assumption. So by Schanuel's lemma $K_j \oplus P'_j \oplus P_{j-1} \oplus \ldots \cong K'_j \oplus P_j \oplus P'_{j-1} \oplus \ldots$. This completes the proof. $\square$

Corollary 5.17. *With the above notation we have K_n projective if and only if K'_n is projective.*

Corollary 5.18. *If $\operatorname{pd} A_R = m$ and*

$$0 \longrightarrow K \longrightarrow P_m \longrightarrow P_{m-1} \longrightarrow \ldots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow A \longrightarrow 0$$

is an exact short sequence with P_j's projective. Then K is projective.

Example. A module with infinite projective dimension.

Consider $\mathbb{Z}/2\mathbb{Z}$ as a module over the ring $\mathbb{Z}/4\mathbb{Z}$ defined by $[x + 2\mathbb{Z}][a + 4\mathbb{Z}] = [xa + 2\mathbb{Z}]$, $x, a \in \mathbb{Z}$. Look at

$$\begin{tikzcd}
\cdots \arrow[r] & \mathbb{Z}/4\mathbb{Z} \arrow[rr, "d_2"] & & \mathbb{Z}/4\mathbb{Z} \arrow[rr, "d_1"] \arrow[dr] & & \mathbb{Z}/4\mathbb{Z} \arrow[r, "\epsilon"] & \mathbb{Z}/2\mathbb{Z} \arrow[r] & 0 \\
& & 2\mathbb{Z}/4\mathbb{Z} \arrow[ur] & & 2\mathbb{Z}/4\mathbb{Z} \arrow[ur] \arrow[dr] & & & \\
& 0 \arrow[ur] & & 0 \arrow[ur] & & 0 & &
\end{tikzcd}$$

where $\epsilon : [a + 4\mathbb{Z}] \to [a + 2\mathbb{Z}]$ and $d_i : [a + 4\mathbb{Z}] \to [2a + 4\mathbb{Z}]$ for all i. The kernel at each stage is $2\mathbb{Z}/4\mathbb{Z}$ and thus cannot be projective (why?).

Proposition 5.19. *Let $\{A_\lambda\}_{\lambda \in \Lambda}$ be a family of right R-modules. Then* $\operatorname{pd}\left(\sum_{\lambda \in \Lambda} \oplus A_\lambda\right) = \sup_{\lambda \in \Lambda} \operatorname{pd} A_\lambda$

Proof. We shall do this for the direct sum of two modules, the general case just involves more notation. Let

$$\ldots \longrightarrow P_n \xrightarrow{\alpha_n} P_{n-1} \xrightarrow{\alpha_{n-1}} \ldots \xrightarrow{\alpha_2} P_1 \xrightarrow{\alpha_1} P_0 \xrightarrow{\alpha_0} A \longrightarrow 0$$

$$\ldots \longrightarrow Q_n \xrightarrow{\beta_n} Q_{n-1} \xrightarrow{\beta_{n-1}} \ldots \xrightarrow{\beta_2} Q_1 \xrightarrow{\beta_1} Q_0 \xrightarrow{\beta_0} B \longrightarrow 0$$

be projective resolution for A and B. Consider

$$\ldots \longrightarrow P_n \oplus Q_n \xrightarrow{\theta_n} P_{n-1} \oplus Q_{n-1} \longrightarrow \ldots \longrightarrow P_1 \oplus Q_1 \xrightarrow{\theta_1} P_0 \oplus Q_0 \xrightarrow{\theta_0} A \oplus B \longrightarrow 0$$

where $\theta_n(p_n, q_n) = (\alpha_n p_n, \beta_n q_n)$, $p_n \in P_n, q_n \in Q_n$. This is an exact sequence and each $P_i \oplus Q_i$ is projective. It follows $\operatorname{pd}(A \oplus B) \leq \sup(\operatorname{pd} A, \operatorname{pd} B)$

Suppose that $\operatorname{pd}(A \oplus B) = m < \infty$. Consider

$$0 \longrightarrow T_m \longrightarrow P_{m-1} \oplus Q_{m-1} \xrightarrow{\theta_{m-1}} \ldots \longrightarrow P_0 \oplus Q_0 \xrightarrow{\theta_0} A \oplus B \qquad 0$$

where θ_1 are the maps defined above, since $\operatorname{pd}(A \oplus B) \cong m$. But $T_m = \ker \theta_{m-1} \cong \ker \alpha_{m-1} \oplus \ker \beta_{m-1}$. This implies $\operatorname{pd} A \leq \operatorname{pd}(A \oplus B)$ and $\operatorname{pd}(B) \leq \operatorname{pd}(A \oplus B)$.

The above argument shows that if either $\operatorname{pd} A$ or $\operatorname{pd} B = \infty$ then $\operatorname{pd}(A \oplus B) = \infty$ and conversely. This completes the proof. $\square$

Lemma 5.20. *Suppose that*

$$0 \longrightarrow K \longrightarrow P \longrightarrow A \longrightarrow 0$$

is an exact sequence with P projective and A not projective. Then $\operatorname{pd} K < \infty$ if and only if $\operatorname{pd} A < \infty$ and we have in this case $1 + \operatorname{pd} K = \operatorname{pd} A$.

Proof. Follows from definition of projective dimension and generalised Schanuel's Lemma. $\square$

Recall how build our projective resolution for M_k

$$\begin{tikzcd}
 & & & & 0 \arrow[dr] & & 0 & & & & \\
 & & & & & K_1 \arrow[ur] \arrow[dr] & & & & & \\
0 \arrow[r] & P_n \arrow[r] & \dots \arrow[rr] & & P_2 \arrow[ur] \arrow[rr] & & P_1 \arrow[rr] \arrow[dr] & & P_0 \arrow[r] & M \arrow[r] & 0 \\
 & & & K_2 \arrow[ur] & & & & K_0 \arrow[ur] \arrow[dr] & & & \\
 & & 0 \arrow[ur] & & & & 0 \arrow[ur] & & 0 & &
\end{tikzcd}$$

Theorem 5.21. *Let $0 \to B \to A \to C \to 0$ be a short exact sequence. If the projective dimension of any two module is the short exact sequence is finite then so is the third. Furthermore we have*

1. *if* $\operatorname{pd} A > \operatorname{pd} B$ *then* $\operatorname{pd} C = \operatorname{pd} A$
2. *if* $\operatorname{pd} A < \operatorname{pd} B$ *then* $\operatorname{pd} C = \operatorname{pd} B + 1$
3. *if* $\operatorname{pd} A = \operatorname{pd} B$ *then* $\operatorname{pd} C \leq \operatorname{pd} A + 1$.

Proof. To prove the first part we induct on n the sum of the finite projective dimension. If $n = 0$ then both modules must be projective. If one of these is C then the short exact sequence splits. So by Lemma 5.8 if one of A or B is projective then so is the other. On the other hand if A and B are projective then $\operatorname{pd} C \leq 1$.

Now suppose that $n > 0$ and the result is true when the sum of the two projective dimension is $< n$. We may also assume that neither A nor C is projective. Now there exists a projective P such that $0 \to D \to P \to A \to 0$ is exact $(*)$. So $A \cong P/D$. Hence there exists a submodule E with $P \supseteq E \supseteq D$ such that $B \cong E/D$, moreover $C \cong A/B \cong (P/D)/(E/D) \cong P/D$ (by the third isomorphism theorem). Thus we have short exact sequences

$$0 \longrightarrow E \longrightarrow P \longrightarrow C \longrightarrow 0 \qquad (\dagger)$$

$$0 \longrightarrow D \longrightarrow E \longrightarrow B \longrightarrow 0 \qquad (\ddagger)$$

Now $(*)$ and $(\dagger)$ give $\operatorname{pd} D = \operatorname{pd} A - 1$ if $\operatorname{pd} A < \infty$ and $\operatorname{pd} E = \operatorname{pd} C - 1$ if $\operatorname{pd} C < \infty$ (by the previous lemma). So by induction hypothesis $(\ddagger)$ gives that if any two of D, E, B have finite projective dimension then so does the third. Hence the same is true for A, B and C.

Now assume that all the projective dimension are finite. We prove the second part by induction on the sum of all three projective dimension. If $n = 0$, nothing to prove (see the base case of the first part of the proof)

Let $n > 0$. If either A or C is projective, then the result holds. So assume that neither is projective. Induction hypothesis applied to $(\ddagger)$ gives:

- i If $\operatorname{pd} E > \operatorname{pd} D$ then $\operatorname{pd} B = \operatorname{pd} E$
- ii if $\operatorname{pd} E < \operatorname{pd} D$ then $\operatorname{pd} B = \operatorname{pd} D + 1$
- iii if $\operatorname{pd} E = \operatorname{pd} D$ then $\operatorname{pd} B \leq \operatorname{pd} D + 1$

In terms of A, B and C these gives

- a If $\operatorname{pd} C > \operatorname{pd} A$ then $\operatorname{pd} B = \operatorname{pd} C - 1$
- b If $\operatorname{pd} C < \operatorname{pd} A$ then $\operatorname{pd} B = \operatorname{pd} A$
- c If $\operatorname{pd} C = \operatorname{pd} A$ then $\operatorname{pd} B \leq A$.

It can be seen (check!) that a. b. and c. are logically equivalent to 1. 2. and 3. of the theorem. $\square$

Theorem 5.22 (Auslander)**.** *Let M be a right R-module, I a non-empty well-ordered set and $\{M_i\}_{i \in I}$ a family of submodules such that:*

1. $M_i \subseteq M_j$ *if* $i \leq j$

2. $M = \cup_{i \in I} M_i$

3. $\operatorname{pd}(M_i/M_i') \leq n$ *where* $M_i' = \cup_{j<i} M_j$

then $\operatorname{pd} M \leq n$

Proof. By induction on n. If $n = 0$ then for all $i \in I$, $\operatorname{pd}(M_i/M_i') \leq 0$ so M_i/M_i' is projective. So each short exact sequence $0 \to M_i' \to M_i \to M_i/M_i' \to 0$ splits. So there exists submodules C_i of M_i such that $M_i = M_i' \oplus C_i$ where $C_i \cong M_i/M_i'$. So each C_i is projective.

We claim that $M = \sum_{i \in I} \oplus C$. The sum is direct for suppose $c_{i_1} + c_{i_2} + \cdots + c_{i_m} = 0$ where $c_{i_j} \in C_{i_j}$ and $i_1 < i_2 < \cdots < i_m$, then $-c_{i_m} = c_{i_1} + \cdots + c_{i_{m-1}} \in M_{i_m}' \cap C_m = 0$. So $c_{i_m} = 0$ and similarly $c_{i_1} = c_{i_2} = \cdots = c_{i_{m-1}} = 0$. Suppose now that $M \neq \sum_{i \in I} \oplus C_i$, so there exists $i \in I$ such that $M_i \not\subseteq \sum_{i \in I} C_i$. Suppose that j is the least index such that $M_j \not\subseteq \sum_{i \in I} \oplus c_i$. So there exists $m \in M_j$ such that $m \notin \sum_{i \in I} \oplus C_i$. Now $M_j = M_j' \oplus C_j$, so $m = b + c$ for some $b \in M_j'$, $c \in C_j$. But $b \in \sum_{i \in I} \oplus C_i$ by the minimality of j ($b \in M_k$some $k < j$). So $m \in \sum_{i \in I} \oplus C_i$ a contradiction. Thus $M = \sum_{i \in I} \oplus C_i$ as required. Hence $\operatorname{pd} M \leq 0$ since M is a direct sum of projective modules.

Now assume the result for $n - 1$. We are given that $\operatorname{pd}(M_i/M_i') \leq n$ for all $i \in I$. Let F $(= F_M)$ be the free module with free basis M, let F_i be the free module with free basis M_i and let F_i' be the free module with free basis M_i'. We have $F \supseteq F_i \supseteq F_i'$ so we have the short exact sequence $0 \to K \to F \to M \to 0$. Define $K_i = F_i \cap K$ and $K_i' = F_i' \cap K$. From the relations $M_i \supseteq M_i'$, $F_i \supseteq F_i'$ and the short exact sequences $0 \to K_i \to F_i \to M_i \to 0$, it follows that the sequences

$$0 \longrightarrow K_i/K_i' \longrightarrow F_i/F_i' \longrightarrow M_i/M_i' \longrightarrow 0$$

are exact. [Note that $(K_i + F_i)/F_i' \cong K_i/(K_i \cap F_i')$ by the third isomorphism theorem. But this is $K_i/(K_i \cap F_i \cap F_i') = K_i/K_i'$.] Each F_i/F_i' is free since F_i has a set of generators, a subset of which generates F_i'. Hence F_i/F_i' is projective so by Lemma 5.20 $\operatorname{pd} K_i/K_i' \leq n - 1$. It can be checked that:

i $i < j$, $i, j \in I$ implies $K_i \subseteq K_j$

ii $K = \cup_{i \in I} K_i$ and $K_i' = \cup_{j<i} K_j$.

So by Lemma 5.20, we have $\operatorname{pd} M \leq 1 + \operatorname{pd} K \leq n$. This completes our proof. □

Definition 5.23. Let R be a ring. We define $D(R) = \sup_{\{M\}} \operatorname{pd} M$ where M ranges over all right modules of R. $D(R)$ is called the *right global dimension of* R.

Lemma 5.24. *Let M be a cyclic module over a ring R. Then $M \cong R/I$ where I is a right ideal of R.*

Proof. Exercise sheet 2. Q4 i) □

Theorem 5.25. *Let R be a ring. We have*

1. $D(R) = \sup_{\{B\}} \operatorname{pd} B$ *where B runs over all cyclic right R-modules*

2. $D(R) = \sup_{\{I\}} \operatorname{pd} R/I$ *where I runs over all right ideals of R*

3. *Further if $D(R) \neq 0$ then $D(R) = 1 + \sup_{\{I\}} \operatorname{pd} I$ where I runs over all right ideals of R.*

Proof. The equivalence of 1 and 2 follows from the previous lemma. The equivalence of 2 and 3 is clear from Lemma 5.20 using the short exact sequence $0 \to I \to R \to R/I \to 0$. So we prove 1.

Let M be a right R-module. Well order the elements x_i of M ($i \in I$) and denote by M_i [respectively by M_i'] the submodule of M generated by all x_j, $j \leq i$ [respectively $j < i$]. Then M_i/M_i' is either 0 or generated by a single element x_i. So $\operatorname{pd}(M_i/M_i') \leq n$ where $n = \sup_{\{B\}} \operatorname{pd} B$ where B ranges over all cyclic right R-modules. Since the family $\{M_i\}_{i \in I}$ satisfies the hypothesis of Theorem 5.22, we have $\operatorname{pd} M \leq n$, hence $D(R) \leq n$. But by definition $D(R) \geq n$, hence $D(R) = n = \sup_{\{B\}} \operatorname{pd} B$. □

Remark. Auslander has shown that for a (left and right) Noetherian ring R, left global dimension of R is the same as the right global dimension of R

5.4 Localization and Global Dimension

All rings are commutative in this section.

S multiplicative subset of R, $0 \notin S$, $1 \in S$. Let M, K be R-modules and $\phi : M \to K$ and R-homomorphism. Then we can define a corresponding R_S-homomorphism $\phi^* : M_S \to K_S$ by $\phi^*\left(\frac{m}{s}\right) = \frac{\phi(m)}{s}$ with $m \in M, s \in S$. (Check details, c.f. Commutative Algebra). If ϕ is an epimorphism, so is ϕ^*.

Lemma 5.26. *If* $0 \longrightarrow A \xrightarrow{\theta} B \xrightarrow{\phi} C \longrightarrow 0$ *is an exact sequence of R-modules then* $0 \longrightarrow A_S \xrightarrow{\theta^*} B_S \xrightarrow{\phi^*} C_S \longrightarrow 0$ *is an exact sequence of R^*-modules.*

Proof. See Commutative Algebra 3.3 □

Lemma 5.27. *If P is a projective R-module, then P_S is a projective R_S-module.*

Proof. Routine from first principle □

Lemma 5.28. $D(R_S) \leq D(R)$

Proof. If $D(R) = \infty$ there is nothing to prove.

So assume$D(R) < \infty$. Let A be an R_S-module. View A as an R-module. Since $A_S \cong A$ (see section 4.4) using Lemma 5.26 and 5.27 we get $\operatorname{pd}_{R_S} A \leq \operatorname{pd}_R A$. It follows that $D(R_S) \leq D(R)$ □

Example. $D(\mathbb{Z}) = 1$, $D(\mathbb{Z}/4\mathbb{Z}) = \infty$. $D(\mathbb{Z}_{(2)}) = 1$, $D(\mathbb{Z}_{(2)}/4\mathbb{Z}_{(2)}) = \infty$

6 Global Dimension of Regular Local Rings

6.1 Change of Rings Theorems

Theorem 6.1. *Let R be a commutative ring and suppose that x is a regular element of R. Denote the ring R/xR by R^*. Let M be a non-zero R^*-module with $\operatorname{pd}_{R^*} M = n < \infty$. Then $\operatorname{pd}_R M = n+1$*

Proof. By induction on n.

Suppose that $n = 0$, i.e., M is R^*-projective, so there exists a free module F such that $F = M \oplus M'$ (for some submodule M' of F). Now $0 \to xR \to R \to R^* \to 0$ is exact as R-modules. $xR \cong R_R$, so xR is R-projective. Hence $\operatorname{pd}_R(R^*) \leq 1$. By Proposition 5.19, it follows that

$$\operatorname{pd}_R F \leq 1 \, (*)$$

So $\operatorname{pd}_R M \leq 1$. Now x does not annihilate any non-zero elements of R. So x does not annihilate any non-zero elements of a free R-module and hence of a projective R-module. But $Mx = 0$, so it follows that M_R cannot be projective. Thus $\operatorname{pd} M = 1$.

So now let $n > 0$ and assume the result for integers less than n. Now there exists a free R^*-module G such that $0 \to K \to G \to M \to 0$ is exact. Since M is not R^*-projective, $\operatorname{pd}_{R^*}(K) = n-1$. Hence $\operatorname{pd}_R(K) = n$ by induction hypothesis. Also $\operatorname{pd}_R(G) \leq 1$ as in $(*)$. So by Theorem5.21$\operatorname{pd}_R M = n+1$ if $n \neq 1$, and $\operatorname{pd}_R M \leq 2$ if $n = 1$.

In the first case we are done, so now we deal with the case $n = 1$ and we must rule out the possibility that $\operatorname{pd}_R M \leq 1$ when $\operatorname{pd}_{R^*} M = 1$. So assume that $\operatorname{pd}_R M \leq 1$ and $\operatorname{pd}_{R^*} M = 1$. So there exists a free R-module H such that

$$0 \to T \to H \to M \to 0 \, (**)$$

is exact. So T is projective since $\operatorname{pd}_R M \leq 1$. Also $Hx \subseteq T$ since $Mx = 0$. Therefore $(**)$ induces the exact sequence

$$0 \longrightarrow T/Hx \longrightarrow H/Hx \longrightarrow M \longrightarrow 0$$

Now H/Hx is R^*-free (check!) and $\operatorname{pd}_{R^*} M = 1$. Thus T/Hx is R^*-projective. But by the third isomorphism theorem $\frac{T/Tx}{Hx/Tx} \cong T/Hx$ as R^*-modules. Hence Hx/Tx is a direct summand of T/Tx. Since T is R-projective, T/Tx is R^*-projective. [If $\underset{R-\text{free}}{F} = T \oplus K$ then $\underset{R^*-\text{free}}{F/Fx} = T/Tx \oplus K/Kx$]. Hence Hx/Tx is R^*-projective. But $Hx/Tx \cong H/T$ since x is regular. But $H/T \cong M$, so M is R-projective, contradiction. So we have proved that $\operatorname{pd}_{R^*} M = 1$ implies $\operatorname{pd}_R M = 2$ □

Corollary 6.2. *In the above situation if $D(R^*) = n < \infty$, then $D(R) \geq n+1$*

Theorem 6.3. *Let R be a commutative ring. Let M be a right R-module. Suppose that x is a regular element of R such that x annihilates no non-zero elements of M. Write $R^* = R/xR$. Then $\operatorname{pd}_{R^*}(M/Mx) \leq \operatorname{pd}_R M$.*

Proof. If $\operatorname{pd} M_R = \infty$ then nothing to prove. So assume $\operatorname{pd}_R M = n < \infty$. We prove the result by induction on n.

Suppose $n = 0$. If F is R-free then F/Fx is R^*-free. Hence if M is a direct summand of an R-free module, then M/Mx is a direct summand of R^*-free module. (This argument was used before). Thus M/Mx is R^*-projective, as required.

Now suppose that $n > 0$ and the result holds for integers smaller than n. There exists a R-module F such that

$$0 \longrightarrow K \longrightarrow F \longrightarrow M \longrightarrow 0 \quad (*)$$

is exact, so $\operatorname{pd}_R(K) = n-1$. Hence $\operatorname{pd}_{R^*}(K/Kx) \leq n-1$ by induction hypothesis. From $(*)$ we get the exact sequence:

$$0 \longrightarrow \frac{K+Fx}{Fx} \longrightarrow F/Fx \longrightarrow M/Mx \longrightarrow 0$$

so we have

$$0 \longrightarrow \frac{F}{K \cap Fx} \longrightarrow F/Fx \longrightarrow M/Mx \longrightarrow 0$$

is exact. We claim $K \cap Fx = Kx$, clearly $Kx \subseteq K \cap Fx$. Suppose that $k = fx \in K \cap Fx$, where $k \in K$, $f \in F$. But x is not a zero divisor on $F/K \cong M$. Thus we have the exact sequence of R^*-modules

$$0 \longrightarrow K/Kx \longrightarrow F/Fx \longrightarrow M/Mx \longrightarrow 0$$

Since $\mathrm{pd}_{R^*}(K/Kx) \leq n-1$, it follows that $\mathrm{pd}_{R^*}(M/Mx) \leq n$. This completes the proof $\square$

We get equality if R is Noetherian and x lies in the Jacobson Radical of R.

Lemma 6.4. *Let R be a commutative Noetherian ring. Let M be a finitely generated module and suppose that x is a regular element lying in $J(R)$. Suppose that x does not annihilate any non-zero elements of M. Write $R^* = R/xR$.*

Then M/Mx is R^*-projective implies that M is R-projective.

Proof. First suppose that M/Mx is R^*-free. Let $v_1, \dots, v_n$ be a free basis of M/Mx. Let $u_1, \dots, u_n$ be elements of M mapping onto $v_1, \dots, v_n$ under the natural homomorphism $M \to M/Mx$.

Claim: M is R-free with basis $u_1, \dots, u_n$.

Let C be the submodule of M generated by $u_1, \dots, u_n$. Then clearly, $C + Mx = M$. This gives $[M/C]Rx = [M/C]$, so $M/C = 0$ by Nakayama's lemma. Thus $M = C$ and $u_1, \dots, u_n$ generate M.

Suppose that $u_1, \dots, u_n$ is not a free basis for M. Then (after possible renumbering) there exists non-zero $r_1, \dots, r_k \in R$ such that $u_1 r_1 + \dots + u_k r_k = 0$, $k \leq n$ $(*)$. Thus $v_1 r_1 + \dots + v_k r_k \in Mx$. Hence $r_i \in xR$ for all i since $v_1, \dots, v_k$ is part of a free basis of an R^*-module. Say $r_i = xs_i$ for $s_i \in R$. We claim $r_k R \subsetneq s_k R$. Clearly $r_k R \subseteq s_k R$ and $r_k R = s_k R$ would imply $s_k = r_k t_k$ for some $t_k \in R$, i.e., $s_k = xs_k t_k$ and so $s_k(1 - xt_k) = 0$. Hence $x_k = 0$ since $1 - xt_k$ is a unit since $x \in J(R)$. But is $s_k = 0$ then $r_k = 0$ contrary to our assumption. Now cancelling out x, $(*)$ gives $u_1 s_1 + \dots + u_k s_k = 0$ with $s_k \neq 0$ since $r_k \neq 0$. We can write this symbolically as $u_1\left(\frac{r_1}{x}\right) + \dots u_n\left(\frac{r_k}{x}\right) = 0$. Repeating the above process we get an ascending chain of ideals

$$r_k R \subsetneq \left(\frac{r_k}{x}\right) R \subsetneq \left(\frac{r_k}{x^2}\right) R \subsetneq \dots$$

This is a contradiction since R is a Noetherian ring. Hence $u_1, \dots, u_n$ is a free basis for M as claimed. So M is R-free.

Next suppose that M/Mx is R^*-projective. Then there exists a free module F such that

$$0 \longrightarrow K \longrightarrow F \longrightarrow M \longrightarrow 0$$

is exact. As before this induces the exact sequence of R^*-modules

$$0 \longrightarrow K/Kx \longrightarrow F/Fx \longrightarrow M/Mx \longrightarrow 0 \qquad (**)$$

Now write $B = M \oplus K$ $(***)$(external direct sum). Then $Bx = Mx \oplus Kx$. This gives $B/Bx = M/Mx \oplus K/Kx$. Since M/Mx is R^*-projective, $(**)$ splits so $F/Fx \cong M/Mx \oplus K/Kx \cong B/Bx$. Therefore B/Bx is R^*-free and by earlier part of the proof B is R-free. Hence from $(***)$ we have that M is R-projective. $\square$

Theorem 6.5. *Let R be a commutative Noetherian ring, M_R a finitely generated module. Suppose that $x \in R$ is a regular element such that $x \in J(R)$. Suppose also that x does not annihilate any non-zero elements of M. Write $R^* = R/xR$. Then $\mathrm{pd}_{R^*}(M/Mx) = \mathrm{pd}_R(M)$*

Proof. Let $\mathrm{pd}_{R^*}(M/Mx) = n$.

If $\mathrm{pd}_{R^*}(M/Mx) = \infty$ then $\mathrm{pd}_R(M) = \infty$ by Theorem 6.3

So assume that $n < \infty$. We induct on n. For $n = 0$ the result is proved by previous Lemma.

Assume that $n > 0$ and the result for values smaller than n. There exists a free module F such that the sequence

$$0 \longrightarrow K \longrightarrow F \longrightarrow M \longrightarrow 0$$

is exact. As before this induces the short exact sequence

$$0 \longrightarrow K/Kx \longrightarrow F/Fx \longrightarrow M/Mx \longrightarrow 0 \qquad (*)$$

Since F/Fx is R^*-free we have that $\operatorname{pd}_{R^*}(K/Kx) = n-1$. Since R is Noetherian and M is finitely generated we have K is finitely generated. Clearly x annihilates no non-zero elements of K. Now $\operatorname{pd}_R(K) = n-1$ by induction hypothesis. So $(*)$ gives $\operatorname{pd}_R M = n$ (unless $\operatorname{pd}_R(M) = 0$ but in this case $\operatorname{pd}_{R^*}(M/Mx) = 0$ by Theorem 6.3) This completes the proof. □

Corollary 6.6. *Let R be a commutative Noetherian ring. Let $x \in J(R)$ be regular and let R^*/xR. If $D(R^*) = n < \infty$ then $D(R) = n+1$.*

Proof. We have $D(R) \geq n+1$ by Corollary 6.2. Now let M be a finitely generated R-module. Let $\operatorname{pd}_R M = k$. We shall not show that $k \leq n+1$. This is clear if $k = 0$, so assume that M is not R-projective. So there exists a free R-module F such that

$$0 \longrightarrow K \longrightarrow F \longrightarrow M \longrightarrow 0$$

is exact. We have $\operatorname{pd}_R K = k = 1$. Since R is Noetherian and F finitely generated, we have K is finitely generated. Also since $K \subseteq F$, x does not annihilate any non-zero elements of K. So by the previous theorem $\operatorname{pd}_R K = \operatorname{pd}_{R^*}(K/Kx) \leq n$. So $\operatorname{pd}_R M = 1 + \operatorname{pd}_R K \leq n+1$. But by Theorem 5.25 $D(R) = \sup_{\{M_R \text{ f.g}\}} \operatorname{pd} M$. Hence $D(R) \leq n+1$. Thus $D(R) = n+1$. □

6.2 Regular Local Ring

Lemma 6.7. *Let R be a regular local ring of Krull dimension n. Then $D(R) = n$.*

Proof. By induction on n. Let J be the Jacobson radical of R. If $n = 0$ we have $J = 0$, i.e., R is a field and the result is true.

Let $n > 0$ and assume the result holds for regular local ring of $K\dim \leq n-1$. Since $n > 0$, $J \neq 0$ and so $J \neq J^2$ by Nakayama's lemma. Let $x_1, \ldots, x_n$ be a minimal generating set for J. Then there exists x_i such that $x_i \notin J^2$. Write $x_i = x$. Since R is an integral domain, x is regular. Let $R^* = R/xR$. By Lemma 4.38 $K\dim R^* = n-1$. Clearly the images of $x_1, x_2, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n$ are a minimal generating set for J/xR. Thus R^* is a regular local ring, hence $D(R^*) = n-1$ by induction hypothesis. Therefore $D(R) = n$ by Corollary 6.6. This completes the proof. □

Lemma 6.8. *Let R be a Noetherian commutative local ring. Suppose that $\operatorname{Ann} J \neq 0$ (where $J = J(R)$). Then $\operatorname{pd} M = 0$ or ∞.*

Proof. If $\operatorname{pd} M \neq 0$ or ∞ then there exists a module B such that $\operatorname{pd} B = 1$. Now consider

$$0 \longrightarrow K \longrightarrow F \longrightarrow B \longrightarrow 0$$

where F is free and $K \subseteq FJ$ (as in Theorem5.10). So $\operatorname{Ann} K \neq 0$. But since $\operatorname{pd} B = 1$, K is projective and hence free. This is a contradiction since a free module cannot have a non-zero annihilator. □

Lemma 6.9. *Let R be a regular local ring with Jacobson radical J. Let $x \in R$ be regular such that $x \in J$ but $x \notin J^2$. Then J/xR is isomorphic to a direct summand of J/xJ.*

Proof. Since $x \notin J^2$ we can choose a minimal generating set $x, y_1, \ldots, y_r$ of J. Write $S = xJ + y_1R + \cdots + y_rR$. Then clearly $S + xR = J$. We claim that $S \cap xR = xJ$, clearly $xJ \subseteq S \cap xR$. Let $z \in S \cap xR$. Then $z = x_j + u_1s_1 + \cdots + y_rs_r = xt$ for some $h \in J, s_i \in R, t \in R$. So $xt - y_1s_1 - \cdots - y_rs_r \in J^2$, since $x, y_1, \ldots, y_r$ is a minimal generating set for J, we have $t \in J$, proving the claim.

Hence we have $J/xJ \cong S/xJ \oplus xR/xJ$ (check!). Now $J/xR \cong \frac{J/xJ}{xR/xJ} \cong S/xJ$ which is a direct summand of J/xJ. □

Proposition 6.10. *Let R be a Noetherian local ring with Jacobian radical J. If $\operatorname{pd} J = m < \infty$ then R is a regular local ring of Krull dimension $m+1$*

Proof. If $J = 0$ then R is a field, $\operatorname{pd} J = -1$ and $K\dim R = 0$, so the result is true.

We now deal with the case $m = 0$. We can assume $J \neq 0$. Since J is projective it is free (Theorem 5.10). So J is a principal ideal generated by a regular element, so by Theorem 4.12, $\operatorname{rk} J = K\dim R = 1$ and the result holds.

We now prove the result by induction on k, the Krull dimension of R.

If $k = 0$ then J is the unique minimal prime of R. Hence $\operatorname{ann} J \neq 0$ (see Proposition 4.18). Then by Lemma 6.8 $\operatorname{pd} J = 0$ and this is dealt with above (we get $J = 0$)

So suppose that $k > 0$ and that the result holds for rings of smaller Krull dimension. Clearly we may also assume $m > 0$. We have $0 < m < \infty$. So by 6.8 $\operatorname{ann} J = 0$. So by Proposition 4.20, J contains a regular element, say x. By Proposition 4.21, we may choose x such that $x \notin J^2$. Write $R^* = R/xR$, $J^* = R/xR$. Since x is regular by Lemma 4.38 we have $K \dim R^* = k - 1$.

Claim: $\operatorname{pd}_{R^*} J^* = m - 1$. We have $\operatorname{pd}_{R^*}(J/xJ) \leq \operatorname{pd}_R J$ by Theorem 6.3, but by Lemma 6.9 J^* is a direct summand of J/xJ, so $\operatorname{pd} J^* < \infty$. Since $m \geq 1$, applying Theorem 5.21 to

$$0 \longrightarrow xR \longrightarrow J \longrightarrow J^* \longrightarrow 0$$

we have $\operatorname{pd}_R J^* = \operatorname{pd}_R J = m$, so by Theorem 6.1 $\operatorname{pd}_{R^*} J^r = m - 1$.

So by induction hypothesis R^* is a regular local ring of Krull dimension m. Hence $K \dim R = m+1$ and R is regular local. (J^* is generating by m elements so J is generated by $m + 1$ elements. But $\operatorname{rk} J = m + 1$) □

Collecting these results together we have

Theorem 6.11 (Serre)**.** *Let R be a commutative Noetherian local ring. Then R is regular local ring of Krull dimension of n if and only if $D(R) = n$.*

Corollary 6.12. *If P is a prime ideal of a regular local ring R then the ring R_P is also regular local*

Proof. R_P is a Noetherian local ring, by the previous theorem $D(R) < \infty$. Hence $D(R_P) < \infty$ by Lemma 5.28. R is regular local by the previous Theorem □

In fact, if S is a multiplicatively closed subset of R and $D(R) < \infty$ then $D(R_S) \leq D(R) < \infty$.

7 Unique Factorization

All rings are commutative with 1

7.1 Unique Factorization Domain

Definition 7.1. An element $0 \neq p \in R$ is said to be a *prime* element if pR is a prime ideal.

Note. If p is a prime element, then so is up where u is a unit.

Definition 7.2. The ring R is called a *unique factorisation domain* (UFD) if R is an integral domain and every non-zero element $a \in R$ is expressible as $a = up_1 \dots p_n$ where u is a unit and the p_i are prime elements.

Proposition 7.3. *If an element of an integral domain is expressible as $p_1 \dots p_n$ where the p_i are primes, then this expression is unique up to a permutation of the p_i's and multiplication by a unit.*

Proof. Algebra II course. (Or Hartley and Hawkes: Rings, Modules and Linear Algebra; Theorem 4.10) □

Definition 7.4. Let R be an integral domain and $a, b \in R$. We say that *a divides b* and write $a|b$ if there exists $c \in R$ such that $b = ac$.

Proposition 7.5. *Let R be a commutative Noetherian integral domain. Then R is a UFD if and only if every rank 1 prime ideal of R is principal.*

Proof. $\Rightarrow$: Let P be a rank 1 prime ideal of R. Let $a \in P$. Then a must be a non-unit, so $a = up_1 \dots p_n$ where u is a unit and the p_j are primes. Hence $p_i \in P$ for some i and so $P = p_iR$ since P is a rank 1 prime ideal and p_iR is a non-zero prime ideal.

$\Leftarrow$: Let S be the set of all elements of R which are expressible in the form $up_1 \dots p_n$ with u a unit and each p_i is prime.

We shall first show that if $a \notin S$ then $aR \cap S = \emptyset$. Suppose not. Let $b \in R$ such that $ab = up_1 \dots p_n$ and n is the least possible, where u is a unit and the p_j are primes. (Note: ab cannot be a unit since a is not a unit). Now $p_i \nmid b$ for any i since if $p_i|b \Rightarrow b = p_it_i$ for some $t_i \in R$. Hence $at_ip_i = up_1 \dots p_n \Rightarrow at_i = up_1 \dots p_{i-1}p_{i+1} \dots p_n$ which contradicts the choice of n. Now $p_1|ab$ so $p_1|a$. Let $a = p_1a_1$ where $a_1 \in R$. Then $p_1a_1b = up_1 \dots p_n$ and so $a_1b = up_2 \dots p_n$. Again $p_2|a_1$ since $p_2 \nmid b$. Proceeding this way we obtain that b is a unit of R. Therefore $a = b^{-1}up_1 \dots p_n$, a contradiction since $a \notin S$.

Now suppose that R is not a UFD. Then there exists a non-zero element $a \in R$ such that $a \notin S$. By the above $aR \cap S = \emptyset$. Choose $P \supseteq aR$ to be an ideal maximal with respect to $P \cap S = \emptyset$. Then P is a prime ideal (check!). However, P will contain a rank 1 prime ideal and hence, by assumption, a prime element. This is a contradiction since $P \cap S = \emptyset$. Thus R must be a UFD.

□

Lemma 7.6. *Let s be a non-zero prime element of a Noetherian local domain R. Let A be a prime ideal with $s \notin A$. Let $S = \{s^n\}$. If AR_S is a principal ideal of R_S then A is a principal ideal of R*

Proof. Let $AR_S = bR_S$. We may assume that $b \in A$ (why?). By Lemma 4.9 $\cap_{n=1}^{\infty} s^nR = 0$. So there exists $k \geq 0$ such that $b \in s^kR$ but $b \notin s^{k+1}R$. Let $b = s^ka$ where $a \in R$. Then $a \notin sR$. We have $AR_S = bR_S = as^kR_S = aR_S$. Also $as^k \in A$ gives $a \in A$ since $s \notin A$ and A is prime

Claim: $A = aR$

Let $x \in A$. Then $x \in aR_S$. So $x = ars^{-m}$ for some m, suppose $m \geq 1$. Hence $xs^m = ar$. Since $a \notin sR$, $r \in sR$ since sR is prime. So $r = sr_1$ for some $r_1 \in R$. Hence $xs^m = asr_1$ and so $xs^{m-1} = ar_1 \in sR$ if $m - 1 > 0$. Proceeding as above we finally obtain $x \in aR$. Thus $A = aR$ as required. □

7.2 Stably Free Modules

Let A, B be $n \times n$ matrices over a commutative integral domain. Then $|AB| = |A| \cdot |B|$ where $|\quad|$ denotes the determinant of the matrix

Notation. Let R be a ring. We write R^n (or sometimes $R^{(n)}$) for $\underbrace{R \oplus \cdots \oplus R}_{n \text{ times}}$

Theorem 7.7 (Kaplansky)**.** *Let R be a commutative integral domain and A a (non-zero) ideal of R such that $A \oplus R^{n-1} \cong R^n$ as R-modules. Then A is a principal ideal of R.*

Proof. The isomorphism shows that $A \oplus R^{n-1}$ has a free basis consisting of n elements, say $\lambda_1, \dots, \lambda_n$. Each λ_j is an n-tuple, so let $\lambda_j = (\alpha_{1j}, \beta_{2j}, \dots, \beta_{nj})$ where $\alpha_{1j} \in A$ and $\beta_{ij} \in R$. Let

$$\Lambda = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1n} \\ \beta_{21} & \beta_{22} & & \beta_{2n} \\ \vdots & & \ddots & \\ \beta_{n1} & \beta_{n2} & & \beta_{nn} \end{pmatrix}$$

Then $\Lambda \in M_n(R)$, note that $|\Lambda| \in A$. Now consider

$$X = \begin{pmatrix} I & I & \dots & I \\ R & R & & R \\ \vdots & & \ddots & \\ R & R & & R \end{pmatrix}$$

Then $X \lhd_r M_N(R)$. Let

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ b_{21} & b_{22} & & b_{2n} \\ \vdots & & \ddots & \\ b_{n1} & b_{n2} & & b_{nn} \end{pmatrix} \in X$$

where $a_{1j} \in A$ and $b_{ij} \in R$ for $2 \leq i \leq n$. Writing the elements of $A \oplus R \oplus \cdots \oplus R$ as columns we have

$$\begin{pmatrix} a_{1j} \\ b_{ij} \\ \vdots \\ b_{nj} \end{pmatrix} = \underbrace{\begin{pmatrix} \alpha_{11} \\ \beta_{21} \\ \vdots \\ \beta_{n1} \end{pmatrix}}_{=\lambda_1} s_{1j} + \underbrace{\begin{pmatrix} \alpha_{12} \\ \beta_{22} \\ \vdots \\ \beta_{n2} \end{pmatrix}}_{=\lambda_2} s_{2j} + \cdots + \underbrace{\begin{pmatrix} \alpha_{1n} \\ \beta_{2n} \\ \vdots \\ \beta_{nn} \end{pmatrix}}_{=\lambda_n} s_{nj}$$

with $s_{ij} \in R$ since $\lambda_1, \dots, \lambda_n$ is a free basis for $A \oplus R^n$. In the matrix from these can be written

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ b_{21} & b_{22} & & b_{2n} \\ \vdots & & \ddots & \\ b_{n1} & b_{n2} & & b_{nn} \end{pmatrix} = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1n} \\ \beta_{21} & \beta_{22} & & \beta_{2n} \\ \vdots & & \ddots & \\ \beta_{n1} & \beta_{n2} & & \beta_{nn} \end{pmatrix} \begin{pmatrix} s_{11} & s_{12} & \dots & s_{1n} \\ s_{21} & s_{22} & & s_{2n} \\ \vdots & & \ddots & \\ s_{n1} & s_{n2} & & s_{nn} \end{pmatrix}$$

Thus $X \subseteq \Lambda M_n(R)$, but $\Lambda M_n(R) \subseteq X$ since $X \lhd R$. Hence $X = \Lambda M_n(R)$. Now let $x \in A$ and consider

$$\begin{pmatrix} x & & & & \\ & 1 & & & 0 \\ & & 1 & & \\ & & & \ddots & \\ & 0 & & & 1 \end{pmatrix} \in X$$

so by above there exists $B \in M_n(R)$ such that

$$\begin{pmatrix} x & & & & \\ & 1 & & & 0 \\ & & 1 & & \\ & & & \ddots & \\ & 0 & & & 1 \end{pmatrix} = \Lambda B$$

Take determinants, we have $x = |\Lambda| \cdot |B|$. Thus $A \subseteq |\Lambda|R$, but $|\Lambda|R \subseteq A$ since $A \lhd R$. Thus $A = |\Lambda|R$ and A is principal. $\square$

Definition 7.8. M_R is said to have a *finite free resolution* if there exists an exact sequence $0 \to F_n \to F_{n-1} \to \cdots \to F_0 \to M \to 0$ with each F_i is free.

Clearly, over a regular local ring each finitely generated module has a finite free resolution

Lemma 7.9. *Let S be a multiplicatively closed subset of a commutative ring R. If M_R has finite free resolution then so does the R_S-module M_S*

Proof. Exercise $\square$

Definition 7.10. An R-module M is called *stably free* if there exists finitely generated free modules F and G such that $G \oplus M \cong F$.

Clearly a stably free module is projective. A stably free module is a finitely generated projective module with a finitely generated free complement

Lemma 7.11. *Let R be a commutative ring. A projective R-module with finite free resolution is stably free*

Proof. We prove this by induction on the length of the finite free resolution. Let M be a finite free resolution module.

For $n = 1$ we have $0 \to F_1 \to F_0 \to M \to 0$. M is projective. So this splits, so $F_0 \cong F_1 \oplus M$ and M is stably free.

Now suppose we have

$$\begin{tikzcd}
0 \arrow[r] & F_n \arrow[r] & \dots \arrow[r] & F_1 \arrow[rr] \arrow[dr] & & F_0 \arrow[r] & M \arrow[r] & 0 \\
& & & & K_0 \arrow[ur] \arrow[dr] & & & \\
& & & 0 \arrow[ur] & & 0 & &
\end{tikzcd}$$

We have $F_0 \cong K_0 \oplus M$ since M is projective. K_0 has finite free resolution of length $n-1$. By induction hypothesis there exists a finitely free module G such that $K_0 \oplus G$ is free. Hence $F_0 \oplus G \cong K_0 \oplus G \oplus M$ with both $F_0 \oplus G$ and $K_0 \oplus G$ free. $\square$

If R is a Noetherian domain and $0 \neq A \lhd R$ such that A is stably free then $A \oplus R^m \cong R^n$. In this case $m = n - 1$ (Q4 on exercise sheet 7)

Theorem 7.12 (Auslander - Buchsbaum 1959)**.** *A regular local ring is a UFD.*

Proof. Let R be a regular local ring of dimension n. We prove the theorem by induction on the (Krull) dimension n.

If $n = 0$ then R is a field and there is nothing to prove.

Assume result for regular local rings of dimension less than n. Let $J = J(R)$, choose $p \in J \setminus J^2$. By Theorem 4.41 R/pR is regular local. By Theorem 4.43 pR is a prime ideal and p is a prime element. Let $S = \{p^n\}$, then clearly $K \dim R_S < K \dim R$.

Now let T be a rank 1 prime of R_S. Let M be a maximal ideal of R_S . Then either $T(R_S)_M = TR_S$ or $T(R_S)_M$ is a rank 1 prime ideal of $(R_S)_M$. By induction hypothesis $(R_S)_M$ is a UFD. So by Proposition 7.5 $T(R_S)$ is principal and hence a projective (free) $(R_S)_M$-module. So by Proposition 5.13 T is a projective R_S-module. Now let A be a rank 1 prime of R. By above AR_S is a projective R_S-module. Since every finitely generated module over R_S has finite free resolution by the previous lemma, AR_S is stably free. So by Theorem 7.7 AR_S is free. Thus AR_S is a principal ideal. So by Lemma 7.6 A is a principal ideal if $p \notin A$. However if $p \in A$ then $pR = A$ since rank A is 1. So by Proposition 7.5 R is a UFD $\square$

Key point. R_S is <u>not</u> local.

Beyond the Course

Theorem 7.13. *Let R be a commutative Noetherian integral domain. The following are equivalent:*

1. *Every ideal of R is a product of prime ideals*
2. *R_M is a PID for each maximal ideal M*
3. *R is integrally closed and $K \dim R = 1$*

(There are various other characterisation) Such a ring is called Dedekind Domain.

Recall that if R is a commutative integral domain, $I \lhd R$, F the field of fraction, then $I^* = \{q \in F | qI \subseteq R\}$. Then $I^*I \subseteq R$, $I^*I \lhd R$.

I is said to be *invertible* if $I^*I = R$. By the dual basis lemma I invertible is the same as I_R projective. So we can add:

4. Every non-zero ideal of R is invertible
5. Every ideal of R is projective.

Proof. 5) $\Rightarrow$ 2), M_R projective implies MR_M projective. So MR_M is free by Theorem 5.10. Thus MR_M is principal, hence by Theorem 4.11 R_M is a PID.

2) $\Rightarrow$ 5). Let $I \lhd R$, then IR_M is principal. So for each maximal ideal M of R. So each IR_M is R_M-projective. Hence by Proposition 5.13 I_R is projective. $\square$

Thus a Dedekind domain is a Noetherian domain R with $D(R) = 1$.