MA5204 Commutative and Homological Algbera

this is my notes for MA5204 Commutative and Homological Algbera. growing up hating algebra, recently I started to appreciate the beauty of algebra. 16/01/2024, I overcomed my fear, my shyness, my anxiety, I asked my teacher to enrol me in an graduate algebra class. this course is taught by Assoc Professor David Hansen (and his postdoc Alexander Youcis and Finn Wiersig on chapter9_morering, chapter10_projective_module) in NUS AY2024-2025. The main reference of the course is (1) Atiyah Macdonald - Introduction to Commutative Algebra, (2) Matsumura - Commutative Ring Theory, and (3) Matsumura - Commutative Algebra

Nguyen Ngoc Khanh

May 21, 2025

Contents

1 CATEGORY THEORY **4**

1.1 CATEGORY THEORY . . . 4

1.2 CATEGORICAL CONSTRUCTION OF HOMOLOGICAL ALGEBRA . . . 4

1.3 UNIVERSAL COEFFICIENT THEOREM FOR CHAIN COMPLEXES OF R-MODULES . . . 12

1.4 KÜNNETH THEOREM FOR CHAIN COMPLEXES OF R-MODULES . . . 15

1.5 REAL-WORLD APPLICATIONS . . . 17

1.5.1 UNIVERSAL COEFFICIENT THEOREM FOR TOPOLOGICAL SPACES . . . 17

1.5.2 EILENBERG-ZILBER THEOREM . . . 18

1.5.3 KÜNNETH THEOREM FOR TOPOLOGICAL SPACES . . . 19

2 RING AND IDEAL **21**

2.1 RING HOMOMORPHISM, IDEALS, QUOTIENT RING . . . 21

2.1.1 RING AND RING HOMOMORPHISM . . . 21

2.1.2 IDEAL AND QUOTIENT RING . . . 22

2.2 PRIME IDEAL AND MAXIMAL IDEAL . . . 23

2.2.1 PRIME IDEAL AND DOMAIN . . . 23

2.2.2 MAXIMAL IDEAL AND FIELD, LOCAL RING . . . 24

2.3 RADICAL . . . 25

2.3.1 RADICAL . . . 25

2.3.2 NILRADICAL . . . 26

2.3.3 JACOBSON RADICAL . . . 27

2.4 OPERATION ON IDEAL . . . 27

2.4.1 IDEAL GENERATED BY SET . . . 27

2.4.2 OPERATION ON IDEAL . . . 27

2.5 EXTENSION AND CONTRACTION . . . 30

2.6 SPECTRUM OF RING . . . 30

3 MODULES **32**

3.1 MODULE AND MODULE HOMOMORPHISM . . . 32

3.2 SUBMODULE AND QUOTIENT MODULE . . . 33

3.3 OPERATION ON SUBMODULE . . . 34

3.4 DIRECT SUM AND DIRECT PRODUCT . . . 35

3.5 EXACT SEQUENCE . . . 36

3.6 FINITELY GENERATED MODULE
FINITELY PRESENTED MODULE . . . 37

4 LOCALIZATION **42**
4.1 LOCALIZATION OF RING . . . 42
4.2 EXTENSION AND CONTRACTION . . . 45
4.3 LOCALIZATION OF MODULE . . . 47
4.4 LOCAL PROPERTIES . . . 48

5 TENSOR PRODUCT **51**
5.1 TENSOR PRODUCT OF MODULES . . . 51
5.2 EXACTNESS OF TENSOR PRODUCT . . . 54
5.3 TENSOR PRODUCT OF ALGEBRAS . . . 58
5.4 TEASER . . . 60

6 NOETHERIAN RING **61**
6.1 NOETHERIAN RING . . . 61
6.2 A PREVIEW OF DIMENSION THEORY . . . 64

7 INTEGRAL DEPENDENCE **65**
7.1 INTEGRAL DEPENDENCE . . . 65
7.2 THE LYING-OVER THEOREM
THE GOING-UP THEOREM . . . 68
7.3 INTEGRALLY CLOSED DOMAIN
THE GOING-DOWN THEOREM . . . 70

8 COMPLETION **72**
8.1 LINEAR TOPOLOGY AND COMPLETION . . . 72
8.2 I-ADIC COMPLETION . . . 76
8.3 MORE I-ADIC COMPLETION . . . 77

9 SOME OTHER CLASSES OF RINGS **83**
9.1 ARTINIAN RING . . . 83
9.2 LENGTH AND ARTINIAN RING . . . 85
9.3 EUCLIDEAN DOMAIN
PRINCIPAL IDEAL DOMAIN
UNIQUE FACTORIZATION DOMAIN . . . 87
9.4 PRIMARY IDEAL . . . 88
9.5 DISCRETE VALUATION RING . . . 90
9.6 DEDEKIND DOMAIN . . . 92
9.7 FRACTIONAL IDEAL, INVERTIBLE IDEAL . . . 93
9.8 PROJECTIVE MODULE . . . 96
9.9 GEOMETRY . . . 97

10 HOMOLOGICAL ALGEBRA 100
10.1 BASIC HOMOLOGICAL ALGEBRA . . . 100
10.2 COMOLOGICAL INVARIANT OF MODULES . . . 104
10.3 ANOTHER PREVIEW OF DIMENSION THEORY . . . 106

11 DIMENSION THEORY 109
11.1 NOETHERIAN RING . . . 109
11.1.1 CONSEQUENCES OF KRULL HEIGHT THEOREM FOR LOCAL RING . . . 110
11.1.2 CONSEQUENCES OF KRULL HEIGHT THEOREM FOR NON-LOCAL RING . . . 111
11.2 REGULAR NOETHERIAN LOCAL RING . . . 112
11.2.1 AUSLANDER-BUCHSBAUM-SERRE THEOREM . . . 112
11.2.2 REGULAR IMPLIES FINITE PROJECTIVE DIMENSION . . . 115
11.3 REGULAR NOETHERIAN RING . . . 115

12 HOMEWORK 1 117

13 HOMEWORK 2 126

14 HOMEWORK 3 145

15 HOMEWORK 4 152
15.1 PROBLEM 1 2 3 . . . 152
15.2 PROBLEM 4 . . . 155
15.3 PROBLEM 5 . . . 160
15.4 PROBLEM 6 . . . 160
15.5 PROBLEM 7 . . . 164
15.6 PROBLEM 8 . . . 164

16 HOMEWORK 5 166

Chapter 1

CATEGORY THEORY

this was written when I studied MA5209 - Algebraic Topology by Dr Charmaine Sia

1.1 CATEGORY THEORY

1.2 CATEGORICAL CONSTRUCTION OF HOMOLOGICAL ALGEBRA

Definition 1.2.1 (initial object, terminal object, pointed category, zero map, kernel, cokernel)
Given a category C, an object 0 is initial if for all $X \in \operatorname{ob} C$, there is only one map in $\operatorname{Hom}(0, X)$, an object $*$ is terminal if for all $X \in \operatorname{ob} C$, there is only one map in $\operatorname{Hom}(X, *)$. Category C is called pointed if it has initial and terminal objects and the unique map $0 \to *$ is an isomorphism. If C is a pointed category, we use the same symbol 0 for both initial object and terminal object. In a pointed category, there exists a zero map between any two objects $M, N \in \operatorname{ob} C$, defined by

$$\begin{tikzcd} M \arrow[r] \arrow[dr, "0"'] & 0 \arrow[d] \\ & N \end{tikzcd}$$

the composition of $M \to 0$ and $0 \to N$. Moreover, let $f : M \to N$ be a morphism in C, a kernel of f is a map $i : K \to M$ such that $fi = 0$ and such map is universal, that is, if $j : L \to M$ with $fj = 0$, then it factors through $i : K \to M$, a cokernel of f is a map $k : N \to Q$ such that $kf = 0$ and such map is universal, that is, if $l : M \to P$ with $lf = 0$, then it factor through $k : N \to Q$

$$\begin{tikzcd} K \arrow[r, "i"] \arrow[rr, bend left, "0"] & M \arrow[r, "f"] & N \\ L \arrow[u, dashed] \arrow[ur, "j"'] \arrow[urr, bend right, "0"'] & & \end{tikzcd} \qquad \begin{tikzcd} M \arrow[r, "f"] \arrow[rr, bend left, "0"] \arrow[drr, bend right, "0"'] & N \arrow[r, "k"] \arrow[dr, "l"'] & Q \arrow[d, dashed] \\ & & P \end{tikzcd}$$

A category C has kernels if every morphism has a kernel. A category C has cokernels if every morphism has a cokernel.

Definition 1.2.2 (preadditive category, Ab-enriched category)
A category C is called **preadditive category** (or Ab-enriched category) if for any two objects $M, N \in \operatorname{ob} C$, $\operatorname{Hom}(M, N)$ is an abelian group and composition is bilinear, that is, if f, g, h are morphisms in C

$$f(g+h) = fg + fh$$
$$(f+g)h = fh + gh$$

The collection of morphisms on a preadditive category *resembles* a monoid

Definition 1.2.3 (additive category)
A category C is additive if

1. C is pointed
2. C is preadditive
3. C admits finite biproduct

biproduct is when product and coproduct coincide. finite biproduct is the product/coproduct of finitely many objects

Definition 1.2.4 (abelian category)
A category C is abelian if

1. C is additive
2. every map in C has kernel and cokernel
3. every monomorphism in C is the kernel of its cokernel
4. every epimorphism in C is the cokernel of its kernel

Remark 1.2.5
The category of R-modules is an abelian category, given any submodule N of M

1. every monomorphism in C is the kernel of its cokernel says that any map $M \to Q$ that sends N to zero factors through M/N
2. every epimorphism in C is the cokernel of its kernel says that any map $L \to M$ that is zero on M/N factor through N

Definition 1.2.6 (projective class)
Let C be a **pointed category with kernels**. A **projective class** in C is a pair $(\mathcal{P}, \mathcal{E})$ where $\mathcal{P}$ is a collection of objects (called **projectives**) and $\mathcal{E}$ is a collection of morphisms (called **epimorphisms**) such that

1. An object P is **projective** if and only if P has the universal lifting property against every **epimorphism** $M \to N$, that is, given any **epimorphism** $M \to N$, if there is a map $P \to N$, then it factors through M

$$\begin{tikzcd} M \arrow[r, two heads, "epi"] & N \\ & P \arrow[u] \arrow[ul, dashed] \end{tikzcd}$$

2. A morphism $f : M \to N$ is an **epimorphism** if and only if every **projective** has the universal lifting property against f, that is, given any **projective** P, if there is a map $P \to N$, then it factors through M

$$\begin{tikzcd} M \arrow[r, two heads, "f"] & N \\ & P \arrow[u] \arrow[ul, dashed] \end{tikzcd}$$

3. C has enough **projectives**, that is, given any object $M \in \operatorname{ob} C$, for every **projective** P, there exists an **epimorphism** $P \to M$.

A similar definition for **injective class**

Remark 1.2.7
In the category of R-modules, an evidental projective class is the pair $(\mathcal{P}, \mathcal{E})$ where $\mathcal{E}$ is the collection of surjective maps and $\mathcal{P}$ is the collection of projective modules

Definition 1.2.8 (chain complex, exact sequence)
In a **pointed category with kernels**, a **chain complex** is a sequence such that given any subsequence $A \to B \to C$, $A \to B$ factors through $\ker(B \to C)$, that is, there exists a map $A \to \ker(B \to C)$ such that the diagram below commutes

$$\begin{tikzcd} \dots \arrow[r] & A \arrow[r] \arrow[d, dashed] & B \arrow[r] & C \arrow[r] & \dots \\ & \ker(B \to C) \arrow[ur] \end{tikzcd}$$

Equivalently, the composition $A \to B \to C$ is the zero map. If there is a notion of epimorphism and the map $A \to \ker(B \to C)$ is an epimorphism, then the sequence is called **exact** at B. A sequence is called exact sequence or an acyclic chain complex if it is exact everywhere, possibly except the two ends.
Similar definition for **cochain complex**

Definition 1.2.9 (chain map)

Given two chain complexes $C_\bullet, D_\bullet$ in a **pointed category with kernels**, for each $n \in \mathbb{Z}$, there is a map $f_n : C_n \to D_n$ such that the diagram below commutes, then $f_\bullet$ is called a **chain map**

$$\begin{tikzcd}
\dots & C_{n-1} \arrow[l] \arrow[d, "f_{n-1}"] & C_n \arrow[l] \arrow[d, "f_n"] & C_{n+1} \arrow[l] \arrow[d, "f_{n+1}"] & \dots \arrow[l] \\
\dots & D_{n-1} \arrow[l] & D_n \arrow[l] & D_{n+1} \arrow[l] & \dots \arrow[l]
\end{tikzcd}$$

Chain complexes and chain maps form a category and it is called the category of chain complexes.

Similar definition for **cochain map**

Remark 1.2.10 (homology)

Let $\operatorname{im} f = \ker \operatorname{coker} f$ and $\operatorname{coim} f = \operatorname{coker} \ker f$. The main axiom of abelian category states that the canonical map $\hat{f} : \operatorname{coim} f \to \operatorname{im} f$ is an isomorphism.

$$\begin{tikzcd}
 & A \arrow[rrr, "f"] \arrow[dr] & & & B \arrow[dr] & \\
\ker f \arrow[ur] & & \operatorname{coim} f \arrow[r, dashed, "\hat{f}"] & \operatorname{im} f \arrow[ur] & & \operatorname{coker} f
\end{tikzcd}$$

Given a complex $L \to M \to N$ in an abelian category if $gf = 0$, one can define homology in three ways

$$\begin{tikzcd}
 & \operatorname{im} f \arrow[rr, "\phi"] \arrow[dr] & & \ker g \arrow[dl] & \\
L \arrow[ur] \arrow[rr, "f"] & & M \arrow[rr, "g"] \arrow[dl] \arrow[dr] & & N \\
 & \operatorname{coker} f \arrow[rr, "\psi"] & & \operatorname{im} g \arrow[ur] &
\end{tikzcd}$$

1. $\operatorname{coker}(\operatorname{im} f \to \ker g)$
2. $\ker(\operatorname{coker} f \to \operatorname{coim} g)$
3. $\operatorname{im}(\ker g \to \operatorname{coker} f)$

The first of these corresponds to the usual $\ker / \operatorname{im}$ and it is not very hard to show that all three ways give canonically isomorphic objects in an abelian category. It is essential to require the category to be abelian here, the three possibilities are distinct in a general additive category (with kernels and cokernels). https://math.stackexchange.com/a/18112/700122

Definition 1.2.11 (chain homotopy)
Given two chain complexes $C_\bullet, D_\bullet$ in a **pointed preadditive category with kernels**. Let $f_\bullet, g_\bullet : C_\bullet \to D_\bullet$ be two chain maps. A **homotopy** from $f_\bullet$ into $g_\bullet$ is a collection of maps $h_n : C_{n-1} \to D_n$ such that $\partial h_{n+1} + h_n \partial = f_n - g_n$

$$\begin{tikzcd}
\dots & C_{n-1} \arrow[l, "\partial"'] \arrow[dr, "h_n"] & C_n \arrow[l, "\partial"'] \arrow[dr, "h_{n+1}"] & C_{n+1} \arrow[l, "\partial"'] & \dots \arrow[l, "\partial"'] \\
\dots & D_{n-1} \arrow[l, "\partial"] & D_n \arrow[l, "\partial"] & D_{n+1} \arrow[l, "\partial"] & \dots \arrow[l, "\partial"]
\end{tikzcd}$$

If there exists a homotopy from $f_\bullet$ into $g_\bullet$, then $f_\bullet$ and $g_\bullet$ are called **homotopic** and denoted by $f_\bullet \sim g_\bullet$. Being homotopic is an equivalence relation.

Definition 1.2.12 (homotopy equivalent)
Two chain complexes $C_\bullet, D_\bullet$ are called **homotopy equivalent** if there exists chain maps $f : C_\bullet \to D_\bullet$ and $g : D_\bullet \to C_\bullet$ so that $gf \sim 1_{C_\bullet}$ and $fg \sim 1_{D_\bullet}$. Being homotopy equivalent is an equivalence relation and each equivalence class is called a **homotopy type**

Theorem 1.2.13 (fundamental theorem of homological algebra - FTHA)
Let C be a **pointed category with kernels** and $(\mathcal{P}, \mathcal{C})$ be a projective class in C. Given $f : M \to M'$ in C and the diagram below

$$\begin{tikzcd}
0 & M \arrow[l] \arrow[d, "f"] & P_0 \arrow[l, "\epsilon"'] \arrow[d, dashed, "f_0"] & P_1 \arrow[l, "d"'] \arrow[d, dashed, "f_1"] & \dots \arrow[l, "d"'] \\
0 & M' \arrow[l] & P'_0 \arrow[l, "\epsilon'"'] & P'_1 \arrow[l, "d'"'] & \dots \arrow[l, "d'"']
\end{tikzcd}$$

where both chains are chain complexes, the top chain consists of projectives P_n and the bottom chain is exact. Then,

- There exists a chain map defined by $f_n : P_n \to P'_n$ for every $n \in \mathbb{N}_0$
- If C is preadditive, the lift is unique upto chain homotopy.

Proof.

1. The first statement is proved by induction

$$\begin{tikzcd}
P_{n-2} \arrow[d, "f_{n-2}"'] & P_{n-1} \arrow[l] \arrow[d, "f_{n-1}"'] & & P_n \arrow[ll] \arrow[dl, dashed] \arrow[d, dashed, "f_n"] \\
& & K'_{n-1} \arrow[dl] & \\
P'_{n-2} & P'_{n-1} \arrow[l] & & P'_n \arrow[ll] \arrow[ul, two heads]
\end{tikzcd}$$

Suppose there exist maps $f_{n-1} : P_{n-1} \to P'_{n-1}$ and $f_{n-2} : P_{n-2} \to P'_{n-2}$. Let $K'_{n-1} = \ker(P'_{n-1} \to P'_{n-2})$.

Since the bottom chain is acyclic, the map $P'_n \to P'_{n-1}$ factors through K'_{n-1} by an epimorphism.

Since the top chain is a chain complex, the composition $P_n \to P_{n-1} \to P'_{n-1} \to P'_{n-2}$ equals $P_n \to P_{n-1} \to P_{n-2} \to P'_{n-2}$ and equals 0 zero, so $P_n \to P_{n-1} \to P'_{n-1}$ factors through K'_{n-1}

Since P_n is projective and $P'_n \to K'_{n-1}$ is an epimorphism, $P_n \to K'_{n-1}$ factors through P'_n by a map $f_n : P_n \to P'_n$

Base case: $n = 0$, let $P_{n-1} = M, P'_{n-1} = M'$, $P_{n-2} = 0, P'_{n-2} = 0$ and $f_{n-1} = f, f_{n-2} = 0$

2. Let $f_\bullet^{(1)}, f_\bullet^{(2)} : P_\bullet \to P'_\bullet$ be any two lifts from $f : M \to M'$

$$\begin{tikzcd} M \arrow[d, "f"'] & P_\bullet \arrow[l, "\epsilon"'] \arrow[d, dashed, bend right, "f_\bullet^{(1)}"'] \arrow[d, dashed, bend left, "f_\bullet^{(2)}"] \\ M' & P'_\bullet \arrow[l, "\epsilon'"] \end{tikzcd}$$

We will prove that $g_\bullet = f_\bullet^{(1)} - f_\bullet^{(2)}$ is chain homotopic to zero, that is to find maps $h_{n+1} : P_n \to P'_{n+1}$ such that $d'h + hd = g$

$$\begin{tikzcd} 0 \arrow[d, "0"'] & P_0 \arrow[l, "d"'] \arrow[d, "g_0"'] & P_1 \arrow[l, "d"'] \arrow[d, "g_1"'] & \dots \arrow[l, "d"'] \\ 0 & P'_0 \arrow[l, "d'"] & P'_1 \arrow[l, "d'"] & \dots \arrow[l, "d'"] \end{tikzcd}$$

Suppose there exists map $h_{n-1} : P_{n-2} \to P'_{n-1}$ and $h_{n-2} : P_{n-3} \to P'_{n-2}$ such that

$$g_{n-2} - h_{n-2}d = d'h_{n-1}$$

$$\begin{tikzcd} P_{n-3} \arrow[dr, "h_{n-2}"] & P_{n-2} \arrow[l, "d"'] \arrow[dr, "h_{n-1}"] & P_{n-1} \arrow[l, "d"'] \\ P'_{n-3} & P'_{n-2} \arrow[l, "d'"] & P'_{n-1} \arrow[l, "d'"] \end{tikzcd}$$

Consider the map $g_{n-1} - h_{n-1}d : P_{n-1} \to P'_{n-1}$,

$$\begin{aligned} d'(g_{n-1} - h_{n-1}d) &= d'g_{n-1} - d'h_{n-1}d && \text{(preadditive)} \\ &= d'g_{n-1} - (g_{n-2} - h_{n-2}d)d && \text{(induction)} \\ &= d'g_{n-1} - g_{n-2}d && \text{(preadditive, } dd = 0) \\ &= 0 && (g_\bullet \text{ is a chain map}) \end{aligned}$$

Let $K'_{n-1} = \ker(d' : P'_{n-1} \to P'_{n-2})$.

Since the bottom chain is acyclic, the map $d' : P'_n \to P'_{n-1}$ factors through K'_{n-1} by an epimorphism.

$$\begin{tikzcd} P_{n-2} \arrow[ddr, "h_{n-1}"] & P_{n-1} \arrow[l, "d"'] \arrow[d, dashed] \arrow[ddr, dashed, "h_n"] & \\ & K'_{n-1} \arrow[d] & \\ P'_{n-2} & P'_{n-1} \arrow[l, "d'"] & P'_n \arrow[l, "d'"] \arrow[ul, dashed, two heads] \end{tikzcd}$$

As $d'(g_{n-1} - h_{n-1}d) = 0$, $g_{n-1} - h_{n-1}d$ factors through K'_{n-1}, that is, $g_{n-1} - h_{n-1}d$ equals the composition $P_{n-1} \to K'_{n-1} \to P'_{n-1}$

Since P_{n-1} is projective and $P'_n \to K'_{n-1}$ is an epimorphism, $P_{n-1} \to K'_{n-1}$ factors through P'_n by a map $h_n : P_{n-1} \to P'_n$, that is, the $d'h_n$ equals the composition $P_{n-1} \to P'_n \to K'_{n-1} \to P'_{n-1}$ and equals the composition $P_{n-1} \to K'_{n-1} \to P'_{n-1}$, hence

$$d'h_n = g_{n-1} - h_{n-1}d$$

Base case: $n = 0$, let $P_{n-2} = 0, P'_{n-2} = 0$, $P_{n-1} = M, P'_{n-1} = M'$, $h_{n-1} = 0$, then

$$d'(g_{n-1} - h_{n-1}d) = 0 \qquad (d' : P'_{n-1} \to P'_{n-2} \text{ is the zero map } M' \to 0)$$

□

Definition 1.2.14 (resolution, projective resolution)
Let M be an object in a **pointed category with kernels**. A **resolution** of M is an exact sequence

$$0 \longleftarrow M \xleftarrow{\epsilon} P_0 \xleftarrow{d} P_1 \xleftarrow{d} \dots$$

If P_n are projectives in a projective class $(\mathcal{P}, \mathcal{E})$, then the sequence is called $\mathcal{P}$-**projective resolution**.
Similar definition for **injective resolution**

Corollary 1.2.15
Let M be an object in a **pointed preadditive category with kernels**. Any two projective resolutions of M are of the same chain homotopy type.

Definition 1.2.16 (additive functor)
Let C, D be **preadditive categories**, a functor $F : C \to D$ is additive if for every $M, N \in \operatorname{ob} C$,

$$\operatorname{Hom}(M, N) \to \operatorname{Hom}(F(M), F(N))$$

is a homomorphism of abelian . In other words, if $f, g : M \to N$, then $F(f+g) = F(f) + F(g)$. Moreover, since F is a functor if $h : N \to Q$, then $F(hf) = F(h)F(f)$. Hence, additive functor on a preadditive category resembles a morphism between two monoids

Remark 1.2.17 (additive functor preserves chain complex)
Additive functor preserves chain complex. That is, if $C_\bullet$ is a chain complex, then

$$\dots \xleftarrow{d} C_{n-1} \xleftarrow{d} C_n \xleftarrow{d} C_{n+1} \xleftarrow{d} \dots$$

$$\dots \xleftarrow{Fd} FC_{n-1} \xleftarrow{Fd} FC_n \xleftarrow{Fd} FC_{n+1} \xleftarrow{Fd} \dots$$

the bottom sequence is also a chain complex.

$$(Fd)(Fd) = F(dd) = F(0) = 0$$

Remark 1.2.18 (additive functor preserves chain homotopy)
Additive functor preserves chain homotopy. That is, if $f, g : C_\bullet \to D_\bullet$ are chain homotopic by a chain homotopy h, then, $F(h)$ is a chain homotopy from Ff to Fg

$$\begin{aligned}(Fd)(Fh) + (Fh)(Fd) &= F(dh) + F(hd) && (F \text{ is a functor})\\ &= F(dh + hd) && (F \text{ is additive})\\ &= F(f - g) && (f \simeq g \text{ by } h)\\ &= F(f) - F(g) && (F \text{ is a functor})\end{aligned}$$

Remark 1.2.19
a functor between additive categories is additive if and only if it preserves finite coproducts - Mac Lane's "Categories for the working mathematician"

TODO - https://math.stackexchange.com/questions/793029/do-covariant-functors-preserve-direct-sums

Definition 1.2.20 (left derived functor)
Let C be a **pointed preadditive category with kernels**, a projective class $(\mathcal{P}, \mathcal{E})$. Let $F : C \to \mathrm{Ab}$ be an additive functor, then the **left derived functor** of F with respect to $(\mathcal{P}, \mathcal{E})$ are $L_n F : C \to \mathrm{Ab}$ defined by

$$(L_n F)(X) = H_n(FP_\bullet)$$

where $X \leftarrow P_0 \leftarrow P_1 \leftarrow \ldots$ is a $\mathcal{P}$-projective resolution.

Remark 1.2.21
One can define the dual notion of right derived functor that is left derived functor by cohomology of injective resolution.

Remark 1.2.22
As F is additive and any two projective resolutions of an object are chain homotopic, the left derived functor is well-defined.

Remark 1.2.23
$\mathrm{Tor}_n^A(M, -)$ is a left derived functor in the cateogry of R-modules

Proposition 1.2.24

For any short exact sequence

$$0 \to L \to M \to N \to 0$$

There exists a natural long exact sequence

$$\begin{tikzcd} & & L_2FN \arrow[dll] \\ L_1FL \arrow[r] & L_1FM \arrow[r] & L_1FN \arrow[dll] \\ FL \arrow[r] & FM \arrow[r] & FN \arrow[r] & 0 \end{tikzcd}$$

Remark 1.2.25

If F is an exact functor, then $L_1FN = 0$. L_n measures how far F from being exact.

Proof. *Proof using fundamental lemma of HA* □

1.3 UNIVERSAL COEFFICIENT THEOREM FOR CHAIN COMPLEX OF R-MODULES

Remark 1.3.1 (R-Mod is abelian)

If R is a commutative ring, the category of R-modules is abelian

Remark 1.3.2 (projective module, projective class in R-Mod)

In the category R-Mod, there is a projective class $(\mathcal{P}, \mathcal{E})$ defined by epimorphism being surjective homomorphism. Then, the following are equivalent

1. $P \in \text{ob}\,\text{R-Mod}$ is projective
2. Every short exact sequence $0 \to M \to N \to P \to 0$ splits
3. P is a direct summand of a free R-module, that is, there exists $Q \in \text{ob}\,\text{R-Mod}$ such that $P \oplus Q$ is a free R-module.

Proof. *TODO* □

Definition 1.3.3 (Tor functor)

In the category R-Mod, define $\text{Tor}_n : \text{R-Mod} \times \text{R-Mod} \to \text{Ab}$ such that $\text{Tor}(-, M)$ is the n-th left derived functor of $(- \times M)$

$$\text{Tor}_n(N, M) = (L_n(- \otimes M))(N) = H_n(P_\bullet \otimes M)$$

where $N \leftarrow P_0 \leftarrow P_1 \leftarrow ...$ is a projective resolution of N

Remark 1.3.4 (some properties of Tor)

$$\begin{aligned}\mathrm{Tor}_n(A,B) &= \mathrm{Tor}_n(B,A)\\ \mathrm{Tor}_n(\varinjlim_\alpha A_\alpha, B) &= \varinjlim_\alpha \mathrm{Tor}_n(A_\alpha, B)\\ \mathrm{Tor}_n(P,B) &= 0 && \text{(if } P \text{ is projective)}\end{aligned}$$

TODO

Definition 1.3.5 (direct sum of chain complexes of R-module - product, coproduct, biproduct)
In the category $\mathrm{Ch}(\text{R-Mod})$, the direct sum $\oplus : \mathrm{Ch}(\text{R-Mod}) \times \mathrm{Ch}(\text{R-Mod}) \to \mathrm{Ch}(\text{R-Mod})$ is defined as follows:

$$(C_\bullet \oplus D_\bullet)_n = C_n \oplus D_n$$

where $C_\bullet, D_\bullet \in \mathrm{ob}\,\mathrm{Ch}(\text{R-Mod})$ and the boundary map $\partial : (C_\bullet \oplus D_\bullet)_n \to (C_\bullet \oplus D_\bullet)_{n-1}$ is defined by

$$\begin{aligned}\partial : (C \oplus D)_n &\to (C \oplus D)_{n-1}\\ c \oplus d &\mapsto \partial c \oplus \partial d\end{aligned}$$

Definition 1.3.6 (tensor product of chain complexes of R-module)
In the category $\mathrm{Ch}(\text{R-Mod})$, the tensor product $\otimes : \mathrm{Ch}(\text{R-Mod}) \times \mathrm{Ch}(\text{R-Mod}) \to \mathrm{Ch}(\text{R-Mod})$ is defined as follows:

$$(C_\bullet \otimes D_\bullet)_n = \bigoplus_{p+q=n} C_p \otimes D_q$$

where $C_\bullet, D_\bullet \in \mathrm{ob}\,\mathrm{Ch}(\text{R-Mod})$ and the boundary map $\partial : (C_\bullet \otimes D_\bullet)_n \to (C_\bullet \otimes D_\bullet)_{n-1}$ is the linear extension of $\partial : C_p \otimes D_q \to (C_\bullet \otimes D_\bullet)_{n-1}$ where

$$\partial(c \otimes d) = \partial c \otimes d + (-1)^p c \otimes \partial d$$

Proof. *TODO - bilinear chain map factors through tensor product* □

Lemma 1.3.7 (on the spot categorical lemma)
Let $F, G : C \to D$ be functors that are natural to the identity functor. Let $f : A \to B$ be a morphism in C, if $FA = GA$ and $FB = GB$, then $Ff = Gf$ *if $C = D$, then it produces a bunch of commutative squares, easy to prove*

$$\begin{tikzcd} A \arrow[d, "f"] & FA \arrow[r, "="] \arrow[d, "Ff"] & GA \arrow[d, "Gf"] \\ B & FB \arrow[r, "="] & GB \end{tikzcd}$$

Theorem 1.3.8 (universal coefficient theorem - UCT)
In the category $\mathrm{R\text{-}Mod}$ where R is a PID. Let $C_\bullet$ be a chain complex of free R-modules and N be an R-module. There is a natural short exact sequence (the map $H_n(C_\bullet)\otimes N \to H_n(C_\bullet \times N)$ is natural)

$$0 \longrightarrow H_n(C_\bullet)\otimes N \longrightarrow H_n(C_\bullet \otimes N) \longrightarrow \mathrm{Tor}_1(H_{n-1}(C_\bullet), N) \longrightarrow 0$$

and this sequence splits (but not naturally)

Proof.
We have the short exact sequence of chain complexes of free R-modules

$$0 \longrightarrow Z_\bullet \hookrightarrow C_\bullet \longrightarrow B_{\bullet-1} \twoheadrightarrow 0$$

where $Z_n = \ker(\partial : C_n \to C_{n-1})$ and $B_n = \mathrm{im}(\partial : C_{n+1} \to C_n)$ and the boundary maps on $Z_\bullet$ and $B_{\bullet-1}$ are zeros. Note that, B_{n-1} is free since it is a submodule of free R-module C_n, then the sequence splits. Then, the sequence below is exact and splits

$$0 \longrightarrow Z_\bullet \otimes N \hookrightarrow C_\bullet \otimes N \twoheadrightarrow B_{\bullet-1}\otimes N \longrightarrow 0$$

where the boundary maps on $Z_\bullet \otimes N$ and $B_{\bullet-1}\otimes N$ are zeros and boundary map on $C_\bullet \otimes N$ is $\partial \otimes 1 : c\otimes n \mapsto \partial c \otimes n$
That induces a long exact sequence

$$\begin{tikzcd}
 & \dots \arrow[r] & H_{n+1}(B_{\bullet-1}\otimes N) \arrow[dll, "(i_n)_*"'] \\
H_n(Z_\bullet \otimes N) \arrow[r] & H_n(C_\bullet \otimes N) \arrow[r] & H_n(B_{\bullet-1}\otimes N) \arrow[dll, "(i_{n-1})_*"'] \\
H_{n-1}(Z_\bullet \otimes N) \arrow[r] & \dots &
\end{tikzcd}$$

where the connecting homomorphism $(i_n)_*$ is induced by inclusion map $i_n : B_{n-1}\otimes N \to Z_n \otimes N$

$$\begin{tikzcd}
 & & B_{n-1}\otimes N \arrow[dll, hook', "i_n"'] \arrow[dl, hook'] \\
Z_n \otimes N & C_n \otimes N \arrow[l] &
\end{tikzcd}$$

That induces a short exact sequence

$$0 \longrightarrow \mathrm{coker}(i_n)_* \longrightarrow H_n(C_\bullet \otimes N) \longrightarrow \ker(i_{n-1})_* \longrightarrow 0$$

We have another short exact sequence

$$0 \longrightarrow B_n \overset{j}{\hookrightarrow} Z_n \twoheadrightarrow H_n(C_\bullet) \longrightarrow 0$$

Then, the sequence below is exact (*see the motivation of left derived functor*)

$$\begin{tikzcd}
\dots \arrow[r] & \mathrm{Tor}_1(Z_n, N) \arrow[r] & \mathrm{Tor}_1(H_n(C_\bullet), N) \arrow[dll] & \\
B_n \otimes N \arrow[r, "j\otimes 1 = i_n"'] & Z_n \otimes N \arrow[r, two heads] & H_n(C_\bullet)\otimes N \arrow[r] & 0
\end{tikzcd}$$

Note that, both i_n and $(i_n)_*$ are induced from the inclusion $B_n \to Z_n$ and we have a natural transformation of functors from the category of pairs of a chain complex and an R-module to Ab,

$$(B_\bullet, N) \mapsto H_n(B_\bullet) \otimes N$$
$$(B_\bullet, N) \mapsto H_n(B_\bullet \otimes N)$$

so $(i_n)_* = i_n$

$$B_n \hookrightarrow Z_n$$

$$\begin{tikzcd} B_n \otimes N = H_n(B_\bullet) \otimes N \arrow[r, hook, "j\otimes 1 = i_n"] \arrow[d, "\cong"'] & Z_n \otimes N = H_n(Z_\bullet) \otimes N \arrow[d, "\cong"] \\ H_n(B_\bullet \otimes N) \arrow[r, "(i_n)_*"'] & H_n(Z_\bullet \otimes N) \end{tikzcd}$$

As Z_n is free, $\mathrm{Tor}_1(Z_n, N) = 0$, then

$$\mathrm{coker}(i_n)_* = H_n(C_\bullet) \otimes N$$
$$\ker(i_n)_* = \mathrm{Tor}_1(H_n(C_\bullet), N)$$

We have the short exact sequence

$$0 \longrightarrow H_p(C_\bullet) \otimes N \longrightarrow H_n(C_\bullet \otimes N) \longrightarrow \mathrm{Tor}_1(H_{n-1}(C_\bullet), N) \longrightarrow 0$$

The split of this sequence is from the map $\beta : H_n(C_\bullet \otimes N) \to \mathrm{coker}(i_n)_*$ induced from projection map $C_n \to Z_n$ $\square$

1.4 KÜNNETH THEOREM FOR CHAIN COMPLEXES OF R-MODULES

Theorem 1.4.1 (Künneth theorem)
In the category $\mathrm{R\text{-}Mod}$ where R is a PID, let $C_\bullet, D_\bullet$ be chain complexes of R-modules, and $C_\bullet$ is degree-wise free (each C_n is a free R-module). Then, there is a natural short exact sequence (homology cross product is natural)

$$0 \longrightarrow \bigoplus_{p+q=n} H_p(C_\bullet) \otimes H_q(D_\bullet) \xrightarrow{\times} H_n(C_\bullet \otimes D_\bullet) \longrightarrow \bigoplus_{p+q=n-1} \mathrm{Tor}_1(H_p(C_\bullet), H_q(D_\bullet)) \longrightarrow 0$$

and this sequence splits (but not naturally)

Proof.

1. **Case 1**: boundary map of $C_\bullet$ is zero

   The boundary map $(C_\bullet \otimes D_\bullet)_n \to (C_\bullet \otimes D_\bullet)_{n-1}$ is the linear extension of

$$\partial : C_p \otimes D_q \to C_p \otimes D_{q-1}$$
$$c \otimes d \mapsto (-1)^{|c|} c \otimes \partial d$$

Hence, we can write the tensor product $C_\bullet \otimes D_\bullet$ as a direct sum of chain complexes

$$C_\bullet \otimes D_\bullet = \bigoplus_p C_p \otimes D_{\bullet - p}$$

We have

$$\begin{aligned}
H_n(C_\bullet \otimes D_\bullet) &= H_n\left(\bigoplus_p C_p \otimes D_{\bullet-p}\right) \\
&= \bigoplus_p H_n(C_p \otimes D_{\bullet-p}) \\
&= \bigoplus_p C_p \otimes H_n(D_{\bullet-p}) && (C_p \text{ is free, cons of UCT}) \\
&= \bigoplus_{p+q=n} C_p \otimes H_q(D_\bullet) && (\text{shifted chain complex})
\end{aligned}$$

2. **Case 2**: $C_\bullet$ is an arbitrary chain complex

   We have the short exact sequence of chain complexes of free R-modules

$$0 \longrightarrow Z_\bullet \hookrightarrow C_\bullet \longrightarrow B_{\bullet-1} \twoheadrightarrow 0$$

   where $Z_n = \ker(\partial : C_n \to C_{n-1})$ and $B_n = \mathrm{im}(\partial : C_{n+1} \to C_n)$ and the boundary maps on $Z_\bullet$ and $B_{\bullet-1}$ are zeros. Note that, B_{n-1} is free since it is a submodule of free R-module C_n, then the sequence splits. Then, the sequence below is exact and splits (*different from the proof of UCT, this uses split, direct sum, tensor product of sequence of chain complexes*)

$$0 \longrightarrow Z_\bullet \otimes D_\bullet \hookrightarrow C_\bullet \otimes D_\bullet \twoheadrightarrow B_{\bullet-1} \otimes D_\bullet \longrightarrow 0$$

   That induces a long exact sequence in homology

$$\begin{tikzcd}
 & \dots \arrow[r] & H_{n+1}(B_{\bullet-1} \otimes D_\bullet) \arrow[dll, "(i_n)_*"'] \\
H_n(Z_\bullet \otimes D_\bullet) \arrow[r] & H_n(C_\bullet \otimes D_\bullet) \arrow[r] & H_n(B_{\bullet-1} \otimes D_\bullet) \arrow[dll, "(i_{n-1})_*"'] \\
H_{n-1}(Z_\bullet \otimes D_\bullet) \arrow[r] & \dots &
\end{tikzcd}$$

   where the connecting homomorphism $(i_n)_*$ are induced by inclusion map $i_n : (B_{\bullet-1} \otimes D_\bullet)_{n+1} \to (Z_\bullet \otimes D_\bullet)_n$

$$\begin{tikzcd}
 & & (B_{\bullet-1} \otimes D_\bullet)_{n+1} \arrow[dll, "i_n"'] \arrow[dl] \\
(Z_\bullet \otimes D_\bullet)_n & (C_\bullet \otimes D_\bullet)_n \arrow[l, hook] &
\end{tikzcd}$$

   That induces a short exact sequence

$$0 \longrightarrow \mathrm{coker}(i_n)_* \longrightarrow H_n(C_\bullet \otimes D_\bullet) \longrightarrow \ker(i_{n-1})_* \longrightarrow 0$$

   We have another short exact sequence

$$0 \longrightarrow B_p \xhookrightarrow{j} Z_p \twoheadrightarrow H_p(C_\bullet) \longrightarrow 0$$

Then, the sequence below is exact (*see the motivation of left derived functor*)

$$\begin{tikzcd}
& \dots \arrow[r] & \mathrm{Tor}_1(Z_p, H_q(D_\bullet)) \arrow[r] & \mathrm{Tor}_1(H_p(C_\bullet), H_q(D_\bullet)) \arrow[dll] & \\
B_p \otimes H_q(D_\bullet) \arrow[r, hook, "j\otimes 1 = i_n"'] & Z_p \otimes H_q(D_\bullet) \arrow[r, two heads] & H_p(C_\bullet) \otimes H_q(D_\bullet) \arrow[r] & 0
\end{tikzcd}$$

Take the direct sum over all pairs $p+q=n$ and note that both i_n and $(i_n)_*$ are induced from the the inclusion $B_p \to Z_p$ we have a natural transformation of functors from the category of pairs of chain complexes to Ab

$$(A_\bullet, B_\bullet) \mapsto H_n(A_\bullet \otimes B_\bullet)$$
$$(A_\bullet, B_\bullet) \mapsto \bigoplus_{p+q=n} H_p(A_\bullet) \otimes H_q(B_\bullet)$$

so $(i_n)_* = i_n$

$$\begin{tikzcd}
B_p \arrow[r, hook] & Z_p
\end{tikzcd}$$

$$\begin{tikzcd}
\bigoplus_{p+q=n} B_p \otimes H_q(D_\bullet) \arrow[r, hook, "j\otimes 1 = i_n"] \arrow[d, "="'] & \bigoplus_{p+q=n} Z_p \otimes H_q(D_\bullet) \arrow[d, "="] \\
H_{n+1}(B_{\bullet-1} \otimes D_\bullet) \arrow[r, "(i_n)_*"'] & H_n(Z_\bullet \otimes D_\bullet)
\end{tikzcd}$$

As Z_p is free, $\mathrm{Tor}_1(Z_p, H_q(D_\bullet)) = 0$, then

$$\mathrm{coker}(i_n)_* = \bigoplus_{p+q=n} H_p(C_\bullet) \otimes H_q(D_\bullet)$$
$$\ker(i_n)_* = \bigoplus_{p+q=n} \mathrm{Tor}_1(H_p(C_\bullet), H_q(D_\bullet))$$

We have the short exact sequence

$$0 \longrightarrow \bigoplus_{p+q=n} H_p(C_\bullet) \otimes H_q(D_\bullet) \xrightarrow{\times} H_n(C_\bullet \otimes D_\bullet) \longrightarrow \bigoplus_{p+q=n-1} \mathrm{Tor}_1(H_p(C_\bullet), H_q(D_\bullet)) \longrightarrow 0$$

The split of this sequence is from the map $\beta : H_n(C_\bullet \otimes D_\bullet) \to \mathrm{coker}(i_n)_*$ induced from projection map $(C_\bullet \otimes D_\bullet)_n \to (Z_\bullet \otimes D_\bullet)_n$

$\square$

1.5 REAL-WORLD APPLICATIONS

1.5.1 UNIVERSAL COEFFICIENT THEOREM FOR TOPOLOGICAL SPACES

Theorem 1.5.1 (universal coefficient theorem - UCT)
Let X be a topological space and $C_\bullet(X)$ be the singular chain complex of X. The singular chain complex with coefficients N be defined by

$$C_\bullet(X, N) = C_\bullet(X) \otimes N$$

The homology group with coefficients N is defined by

$$H_n(X, N) = H_n(C_\bullet(X, N))$$

Then, there is a short exact sequence

$$0 \longrightarrow H_n(X) \otimes N \longrightarrow H_n(X, N) \longrightarrow \mathrm{Tor}_1(H_{n-1}(X), N) \longrightarrow 0$$

and this sequence splits (but not naturally)

1.5.2 EILENBERG-ZILBER THEOREM

Remark 1.5.2 ($\mathrm{Fun}(C, \text{R-Mod})$)
Given a category C, $\mathrm{Fun}(C, \text{R-Mod})$ is a **pointed preadditive category with kernels** (more precisely, abelian category - will define in the future).
Given a morphism $F \to G$ in $\mathrm{Fun}(C, \text{R-Mod})$ (a natural transformation from F to G), then the kernel of $F \to G$ is a morphism $K \to F$ such that $K(X)$ is the kernel of $F(X) \to G(X)$ for all $X \in \mathrm{ob}\, C$

Remark 1.5.3 (models define projective class in $\mathrm{Fun}(C, \text{R-Mod})$)
Let $\mathcal{M}$ be any set of objects in C (called models), then $\mathcal{M}$ defines a projective class $(\mathcal{P}, \mathcal{E})$ in $\mathrm{Fun}(C, \text{R-Mod})$ where a morphism $G \to F$ is an epimorphism (relative to $\mathcal{M}$) if for all $M \in \mathcal{M}$, $G(M) \twoheadrightarrow F(M)$ is surjective. Then, the following are equivalent

1. $P \in \mathrm{ob}\,\mathrm{Fun}(C, \text{R-Mod})$ is projective
2. P is a **retract of coproduct** of $R\,\mathrm{Hom}(M, -)$ for some $M \in \mathcal{M}$ where $\mathrm{Hom}(M, -)$ is a functor $\text{R-Mod} \to \text{Set}$, R is the free R-module functor $\text{Set} \to \text{R-Mod}$. In the case of R-module, **retract of coproduct** is the **direct summand** of a R-module

Proof. *TODO - prove using Yoneda lemma* □

Remark 1.5.4
Let $C = \mathrm{Top}$ and model $\mathcal{M} = \{\Delta^n : n = 0, 1, ...\}$, then for each n, $R\,\mathrm{Hom}(\Delta^n, -)$ is projective. Note that, $R\,\mathrm{Hom}(\Delta^n, -)$ is the n-singular chain complexes with coefficients in R denoted by C_n. Moreover, the sequence below is a projective resolution of the zero-th homology functor H_0

$$0 \longleftarrow H_0 \xleftarrow{\epsilon} C_0 \xleftarrow{\partial} C_1 \xleftarrow{\partial} \ldots$$

Let Ev_X be the evaluation functor of topological space X, then the left derived functor Ev_X on H_0 is the n-th singular homology of X

$$(L_n \mathrm{Ev}_X)(H_0) = H_n(C_\bullet(X)) = H_n(X)$$

Theorem 1.5.5 (Eilenberg-Zilber theorem)
Let X, Y be topological spaces and $C_\bullet$ be the singular chain complex functor from Top to $\mathrm{R\text{-}Mod}$, then there are two chain maps

$$F : C_\bullet(X \times Y) \to C_\bullet(X) \otimes C_\bullet(Y)$$
$$G : C_\bullet(X) \otimes C_\bullet(Y) \to C_\bullet(X \times Y)$$

such that FG and GF are chain homotopic to identity. That is, $C_\bullet(X \times Y)$ and $C_\bullet(X) \times C_\bullet(Y)$ are of the same chain homotopy type.

Proof.
idea of proof
In the category of $\mathrm{Top} \times \mathrm{Top}$, let model $\mathcal{M} = \{(\Delta^p, \Delta^q) : p, q \geq 0\}$. These functors $\mathrm{Top} \times \mathrm{Top} \to \mathrm{R\text{-}Mod}$ are projective

$$C_n(X \times Y) = R[\mathrm{Hom}(\Delta^n, X) \times \mathrm{Hom}(\Delta^n, Y)]$$
$$C_p(X) \otimes C_q(Y) = R[\mathrm{Hom}(\Delta^p, X) \times \mathrm{Hom}(\Delta^q, Y)]$$

As $H_0(X \times Y) \to H_0(X) \to H_0(Y)$ is an isomorphism, by FTHA, that induces a chain homotopy equivalence.

$$\begin{tikzcd}
0 & H_0(X \times Y) \arrow[l] \arrow[d, "="'] & C_0(X \times Y) \arrow[l] \arrow[d, dashed] & C_1(X \times Y) \arrow[l] \arrow[d, dashed] & \dots \arrow[l] \\
0 & H_0(X) \otimes H_0(Y) \arrow[l] & (C_\bullet(X) \otimes C_\bullet(Y))_0 \arrow[l] & (C_\bullet(X) \otimes C_\bullet(Y))_1 \arrow[l] & \dots \arrow[l]
\end{tikzcd}$$

□

Corollary 1.5.6
Same chain homotopy type induces isomorphism in homology, that is

$$H_n(X \times Y) \cong H_n(C_\bullet(X) \otimes C_\bullet(Y))$$

1.5.3 KÜNNETH THEOREM FOR TOPOLOGICAL SPACES

Theorem 1.5.7 (Künneth theorem)
In the category $\mathrm{R\text{-}Mod}$ where R is a PID, let $C_\bullet, D_\bullet$ be chain complexes of R-modules, and $C_\bullet$ is degree-wise free (each C_n is a free R-module). Then, there is a short exact sequence

$$0 \longrightarrow \bigoplus_{p+q=n} H_p(C_\bullet) \otimes H_q(D_\bullet) \xrightarrow{\times} H_n(C_\bullet \otimes D_\bullet) \longrightarrow \bigoplus_{p+q=n-1} \mathrm{Tor}_1(H_p(C_\bullet), H_q(D_\bullet)) \longrightarrow 0$$

and this sequence splits (but not naturally)

Theorem 1.5.8 (Künneth theorem)

Let X, Y be topological spaces and R be a PID, there is a natural short exact sequence

$$0 \longrightarrow \bigoplus_{p+q=n} H_p(X;R) \otimes H_q(Y;R) \xrightarrow{\times} H_n(X \times Y) \longrightarrow \bigoplus_{p+q=n-1} \mathrm{Tor}_1(H_p(X;R), H_q(Y;R)) \longrightarrow 0$$

and this sequence splits (but not naturally).

Corollary 1.5.9

If $H_\bullet(X;R)$ is torsion free over R (*of the form $R \oplus R \oplus$ ... without any R/nR term*), then

$$H_n(X \times Y) = \bigoplus_{p+q=n} H_p(X;R) \otimes H_q(Y;R)$$

Reserve for theory of categories

Chapter 2

RING AND IDEAL

2.1 RING HOMOMORPHISM, IDEALS, QUOTIENT RING

2.1.1 RING AND RING HOMOMORPHISM

Definition 2.1.1 (associative ring, commutative (unital) ring)
An associative ring R is an additive abelian group $(R, +)$ equipped with a multiplication $\times : R \times R \to R$ such that

1. the multiplication is associative, that is
$$(ab)c = a(bc)$$
for all $a, b, c \in R$
2. the distributive laws hold in R, that is
$$(a + b)c = ac + bc \text{ and } c(a + b) = ca + cb$$
for all $a, b, c \in R$

If the multiplication is commutative, that is, $ab = ba$ for all $a, b \in R$ and there is an element $1 \in R$ such that
$$1a = a1 = a$$
for all $a \in R$, then $(R, +, \times, 1)$ is called a commutative (unital) ring. The element 1 is called multiplicative identity or unity.

Remark 2.1.2
From now on, whenever we mention ring, that will mean *commutative (unital) ring*

Definition 2.1.3 (ring homomorphism)
A map $f : A \to B$ of a ring A into a ring B is called a ring homomorphism if

1. $f : A \to B$ is a group homomorphism of the additive groups
2. $f(xy) = f(x)f(y)$ for all $x, y \in A$
3. $f(1_A) = 1_B$

2.1.2 IDEAL AND QUOTIENT RING

Definition 2.1.4 (subring)
A subring S of a ring R is a subset if R that is also a ring

Definition 2.1.5 (ideal)
A ideal I of a ring R is an additive subgroup of R that is stable under multiplication by ring elements, that is for each $r \in R$, the multiplication map by r is

$$\begin{aligned} r : R \times I &\to I \\ (r, i) &\mapsto ri \end{aligned}$$

(*note that, ideal is not a subring*)

Definition 2.1.6 (quotient ring)
Given an ideal I of a ring R, the quotient group R/I inherits a naturally defined multiplication from R which makes it into a ring, namely, the quotient ring. The multiplication in R/I is as follows:

$$\begin{aligned} \times : R/I \times R/I &\to R/I \\ (x + I, y + I) &\mapsto xy + I \end{aligned}$$

for all $x, y \in R$. Moreover, the natural projection

$$\begin{aligned} \phi : R &\twoheadrightarrow R/I \\ x &\mapsto x + I \end{aligned}$$

is a surjective ring homomorphism. We also write $x + I = \bar{x} = [x] = \phi(x)$

Theorem 2.1.7 (the first isomorphism theorem for rings)
Let $f : A \to B$ be a ring homomorphism, then $\ker f$ is an ideal of A, $\operatorname{im} f$ is a subring of B, and $f : A \to B$ factors through $A/\ker f$ by the natural projection $\phi : A \twoheadrightarrow A/\ker f$ by a ring isomorphism $A/\ker f \xrightarrow{\sim} \operatorname{im} f$

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, two heads, "\phi"'] & \operatorname{im} f \subseteq B \\ A/\ker f \arrow[ur, "\sim"'] & \end{tikzcd}$$

Proof. TODO □

Theorem 2.1.8 (the forth isomorphism theorem for rings)
Let I be an ideal of R, there is a one-to-one correspondence between the set of ideals in A containing I and the set of ideals in A/I given by the map $\phi : A \twoheadrightarrow A/I$

$$\bar{J} = \phi(J)$$

Moreover, consider the partial order by inclusions of ideals, the correspondence is also order preserving, that is, given ideals J, K containing I in R, then $J \subseteq K \iff \bar{J} \subseteq \bar{K}$

$$\begin{tikzcd} I \arrow[r, hook] \arrow[d, dashed] & J \arrow[r, hook] \arrow[d, dashed] & K \arrow[r, hook] \arrow[d, dashed] & R \arrow[d, dashed] \\ \{0\} \arrow[r, hook] & \overline{J} \arrow[r, hook] & \overline{K} \arrow[r, hook] & R/I \end{tikzcd}$$

Proof. TODO □

Remark 2.1.9 (the second and third isomorphism theorems for rings)
Let R be a ring

1. (the second isomorphism theorem) Let S be a subring and I be an ideal of R, then

$$\frac{S+I}{I} \cong \frac{S}{S \cap I}$$

2. (the third isomorphism theorem) Let I, J be ideals of R with $I \subseteq J$, then

$$\frac{R/I}{J/I} = \frac{R}{J}$$

Remark 2.1.10 (existence of ideal)
Given any ring R, there always exist at least two ideals

1. the zero ideal: $(0) = \{0\}$
2. the whole ring $R = (1) = (u)$ for any unit u

2.2 PRIME IDEAL AND MAXIMAL IDEAL

Definition 2.2.1 (zero divisor, unit)
A zero divisor x in ring R is an element that divides 0, that is, there is $y \in R$ such that $xy = 0$. A unit x in ring R is an element that divides 1, that is, there is $y \in R$ such that $xy = 1$. The set of units forms the multiplicative group $R^\times$

2.2.1 PRIME IDEAL AND DOMAIN

Definition 2.2.2 (domain)

A ring R is a domain if $xy = 0$ implies $x = 0$ or $y = 0$ for all $x, y \in R$

Definition 2.2.3 (prime ideal)

A non-zero proper ideal $\mathfrak{p}$ of ring R is prime if $xy \in \mathfrak{p}$ implies $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$ for all $x, y \in R$

Proposition 2.2.4

An ideal $\mathfrak{p}$ of R is prime if and only if $R/\mathfrak{p}$ is a domain

Proof. An ideal $\mathfrak{p}$ of R is prime $\iff$ $xy \in \mathfrak{p}$ implies $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$ $\iff$ $\overline{xy} = \bar{x}\bar{y} \in \mathfrak{p}$ implies $\bar{x} \in \mathfrak{p}$ or $\bar{y} \in \mathfrak{p}$ $\iff$ $R/\mathfrak{p}$ is a domain $\square$

2.2.2 MAXIMAL IDEAL AND FIELD, LOCAL RING

Definition 2.2.5 (field)

Let R be a ring with $1 \neq 0$, then the following are equivalent

1. every non-zero element in R is a unit
2. the only ideals in R are (0) and R
3. every map $R \to S$ into a non-trivial ring S is injective.

The ring R satisfying one the those conditions is called field

Proof.

($1 \implies 2$) Let A be a nonzero ideal of R, then there exists a nonzero $x \in A$. Since R is a field, x is an unit. Then, $R = (x) \subseteq A$, hence $A = R$

($2 \implies 3$) If $\phi : R \to S$ is a ring homomorphism, then $\ker \phi$ is an ideal in R. Since S is non-trivial, $\ker \phi = (0) = \{0\}$, that is, ϕ is injective.

($3 \implies 1$) Let $x \in R$ that is not a unit, hence $(x) \neq R$. Then, $R/(x)$ is not trivial. The natural projection $\phi : R \to R/(x)$ is injective by the premise, hence $(x) = \ker \phi = \{0\}$. Then, $x = 0$ $\square$

Definition 2.2.6 (maximal ideal)

A proper ideal $\mathfrak{m}$ of R is maximal if there is no proper ideal $\mathfrak{a}$ such that

$$\mathfrak{m} \subsetneq \mathfrak{a} \subsetneq R$$

Proposition 2.2.7

An ideal $\mathfrak{m}$ of R is maximal if and only if $A/\mathfrak{m}$ is a field

Proof. prove by the characterization of field and order-preservation of fourth isomorphism theorem $\square$

Remark 2.2.8
every field is a domain implies every maximal ideal is prime.

Proposition 2.2.9
Every proper ideal is contained in a maximal ideal *(Zorn lemma)*

Definition 2.2.10 (local ring, residue field)
A ring A is local if it has exactly one maximal ideal $\mathfrak{m}$. The field $k = A/\mathfrak{m}$ is called residue field. We usually denote $(A, \mathfrak{m}, k)$

Proposition 2.2.11
Propositions on local rings

1. Let A be a ring and $\mathfrak{m}$ be a proper ideal of A such that every $x \in A - \mathfrak{m}$ is a unit. Then, $(A, \mathfrak{m})$ is a local ring.
2. Let A be a ring and $\mathfrak{m}$ be a maximal ideal of A such that every element of $1 + \mathfrak{m} = \{1 + x : x \in \mathfrak{m}\}$ is a unit in A. Then, A is a local

Proof.
(1) Any other maximal ideal contains a unit, hence it is the whole ring. Then, A is local
(2) Let $x \in A - \mathfrak{m}$, since $\mathfrak{m}$ is maximal, then the ideal $(x, \mathfrak{m}) = A$. Hence, $1 = rx + m$ for some $r \in R$, $m \in \mathfrak{m}$, then $xy = 1 - m \in 1 + \mathfrak{m}$, x is a unit. From 1, A is a local ring. ☐

2.3 RADICAL

2.3.1 RADICAL

Definition 2.3.1 (radical)
Given any ideal I of ring R, then the radical of I, denoted by $\sqrt{I}$, is defined by

$$\sqrt{I} = r(I) = \{x \in R : x^n \in I \text{ for some } n \geq 1\}$$

Proposition 2.3.2
Given any ideal I of ring R, the radical $\sqrt{I}$ of I is an ideal

Proof.
($\sqrt{I}$ is a group) $0 \in \sqrt{I}$. If $x \in \sqrt{I}$, then $x^n \in I$ for some $n > 0$, then $(-x)^n = (-1)^n x^n \in I$, hence $-x \in \sqrt{I}$. If $x, y \in \sqrt{I}$, then $x^n, y^m \in I$ for some $n, m > 0$, then $(x+y)^{n+m-1} = \sum_{k=0}^{n+m-1} \binom{n+m-1}{k} x^k y^{n+m-1-k} \in I$ since each $x^k y^{n+m-1-k} \in I$ for all $0 \leq k \leq n+m-1$, that is, $x + y \in \sqrt{I}$
($\sqrt{I}$ is stable under multiplication by ring elements) If $x \in \sqrt{I}$, then $x^n \in I$ for some $n > 0$. If $r \in R$, then $(rx)^n = r^n x^n \in I$, hence $rx \in \sqrt{I}$ ☐

Proposition 2.3.3
Given any ideal I of ring R and $\phi : R \twoheadrightarrow R/I$, then

$$\sqrt{I} = \phi^{-1}(\eta_{R/I})$$

where $\eta_{R/I}$ is the nilradical of R/I, that is, the radical of the zero ideal of R/I

Remark 2.3.4
Let I, J be ideals of R and $\mathfrak{p}$ be prime ideal of R, then

$$\begin{aligned}
&\sqrt{\sqrt{I}} = \sqrt{I} \\
&\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J} \\
&\sqrt{I} = R \iff I = R \\
&\sqrt{I + J} = \sqrt{\sqrt{I} + \sqrt{J}} \\
&\sqrt{\mathfrak{p}^n} = \mathfrak{p} && \text{(for every } n \geq 1\text{)}
\end{aligned}$$

Proposition 2.3.5
Given any ideal I of ring R, then

$$\sqrt{I} = \bigcap_{\mathfrak{p} \text{ prime and } I \subseteq \mathfrak{p}} \mathfrak{p}$$

Proof.
($\subseteq$) For any prime ideal $\mathfrak{p}$ such that $I \subseteq \mathfrak{p}$, if $x \in \sqrt{I}$, then $x^n \in I \subseteq \mathfrak{p}$ for some $n > 0$. Since $\mathfrak{p}$ is prime, $x \in \mathfrak{p}$
($\supseteq$) Let $x \in \sqrt{I}$, then $x^n \in I$ for some $n > 0$. Suppose there is a prime ideal $\mathfrak{p}$ such that $I \subseteq \mathfrak{p}$ and $x \notin \mathfrak{p}$. This is a contradiction since $x^n \in \mathfrak{p}$ implies $x \in \mathfrak{p}$. □

2.3.2 NILRADICAL

Definition 2.3.6 (nilpotent, nilradical)
A element x of a ring R is called nilpotent if $x^n = 0$ for some $n > 0$. The nilradical of a ring R is the collection of nilpotent elements, denoted by $\eta_R = \sqrt{(0)}$

Remark 2.3.7
Given a ring R, R/η_R has no nonzero nilpotent element.

Proof. Let $x \in R$ such that $\bar{x}^n = 0$, then $\overline{x^n} = \bar{x}^n = 0$, that is, $x^n \in \eta_R$, hence, $x^{nm} = (x^n)^m = 0$ for some $m > 0$, that is, x is nilpotent □

Corollary 2.3.8
The nilradical η_R of R is the intersection of all prime ideals of R

2.3.3 JACOBSON RADICAL

Definition 2.3.9 (Jacobson radical)
Given a ring R, the Jacobson radical is

$$J(R) = \bigcap_{\mathfrak{m} \text{ maximal}} \mathfrak{m}$$

Proposition 2.3.10
Given a ring R, $x \in J(R)$ if and only if $1 - xy$ is a unit in R for all $y \in R$

Proof.
($\Longrightarrow$) Let $x \in J(R)$, suppose $1 - xy$ is not a unit, then $1 - xy$ belongs to some maximal ideal $\mathfrak{m}$. Since $x \in \mathfrak{m}$ and $1 \notin \mathfrak{m}$, this is a contradiction
($\Longleftarrow$) Let $1 - xy$ be a unit in R for all $y \in R$ and there is a maximal ideal $\mathfrak{m}$ such that $x \notin \mathfrak{m}$. Since $\mathfrak{m}$ is maximal, $(\mathfrak{m}, x) = R$, then $1 = m + rx$ for some $m \in \mathfrak{m}$ and $r \in R$. Hence, $m = 1 - rx$ is a unit, this is a contradiction. $\square$

2.4 OPERATION ON IDEAL

2.4.1 IDEAL GENERATED BY SET

Definition 2.4.1 (principal ideal, ideal generated by a set)
Let A be a subset of ring R, then the ideal generated by A is the smallest ideal containing A, denoted by (A). This is well defined since the intersection of arbitrary number of ideals is an ideal. An explitcit construction of (A) is as follows:

$$(A) = RA = \{r_1 a_1 + ... + r_n a_n : r_1, ..., r_n \in R, a_1, ..., a_n \in A, n \geq 0\}$$

A principal ideal is an ideal generated by one element. In particular, the principal ideal generated by $x \in R$ is

$$(x) = \{rx : r \in R\}$$

2.4.2 OPERATION ON IDEAL

Definition 2.4.2 (sum, product, intersection, union)
Let I, J be ideals of ring R, define the following ideals

1. sum of ideals
$$I + J = \{i + j : i \in I, j \in J\}$$
arbitrary sum of ideals is defined by $\sum_{i \in I} \mathfrak{a}_i = \{a_{j_1} + ... + a_{j_n} : j_1, ..., j_n \in I, n \in \mathbb{Z}_{\geq 0}\}$

2. product of ideals
$$IJ = \{i_1 j_1 + i_2 j_2 + ... + i_n j_n : i_\bullet \in I, j_\bullet \in J\}$$

3. intersection of ideals
$$I \cap J$$

Remark 2.4.3
Let I, J, K be ideals, then we have the following

1. $I(J + K) = IJ + IK$
2. $IJ \subseteq I \cap J \subseteq I \subseteq I + J$
3. $(I + J)(I \cap J) \subseteq IJ$
4. the smallest ideal containing I and J is $I + J$

Definition 2.4.4 (coprime)
Two ideals I, J in R are called coprime (or comaximal) if $I + J = R$

Proposition 2.4.5 (chinese remainder theorem, CRT)
Let I and J be ideals of ring R, define the homomorphism

$$\begin{aligned} \phi : R &\to R/I \times R/J \\ r &\mapsto (r + I, r + J) \end{aligned}$$

Then

1. $\ker \phi = I \cap J$
2. $I + J = R$ implies $I \cap J = IJ$
3. $I + J = R$ if and only if ϕ is surjective. Hence, [a]
$$R/IJ \cong R/I \cap J \cong R/I \times R/J$$
4. $I \cap J = (0)$ if and only if ϕ is injective

[a] the statement is also true for the case of n ideals and ideals being pairwise coprime

Proof.
($\ker \phi = I \cap J$) the elements in R that are sent to $(0, 0)$ in $R/I \times R/J$ are exactly those in both I and J

($I+J=R$ implies $I\cap J=IJ$) If $I+J=R$, then $I\cap J=R(I\cap J)\subseteq IJ$. Since $IJ\subseteq I\cap J$, then $I\cap J=IJ$
($I+J=R$ if and only if ϕ is surjective) If $I+J=R$, then $1=i+j$ for some $i\in I$ and $j\in J$, we have

$$\phi(i)=\phi(1-j)=(0,1)$$
$$\phi(j)=\phi(1-i)=(1,0)$$

Hence, for any $(\bar{x},\bar{y})\in R/I\times R/J$ with $x,y\in R$, then $\phi(jx+iy)=(\bar{x},\bar{y})$. That is, the map ϕ is surjective. By the first isomorphism theorem, we have the isomorphism as required. In the contrary, if ϕ is surjective, there exists $x\in R$ such that $\phi(x)=(1,0)$, that is, $1-x\in I$ and $x\in J$. Therefore, $1\in I+J$, that is, $I+J=R$
($I\cap J=(0)$ if and only if ϕ is injective) this is true since $\ker\phi=I\cap J$ □

Remark 2.4.6
In general, union of ideals is not an ideal.

Proposition 2.4.7
Let A and B be ideals and I be an ideal contained in $A\cup B$, then $I\subseteq A$ or $I\subseteq B$. Let $\mathfrak{p}_1,\mathfrak{p}_2,...,\mathfrak{p}_n$ be prime ideals and I be an ideal contained in $\bigcup_{i=1}^n\mathfrak{p}_i$, then $I\subseteq\mathfrak{p}_i$ for some i

Proof.
(the case of two ideals) If $I\nsubseteq A$, then there exists $a\in I-A$. If $I\nsubseteq B$, then there exists $b\in I-B$. Consider the element $a+b\in I$, $a+b\notin A$ and $a+b\notin B$, contradiction
(the case of n prime ideals) We will prove by induction. The statement when $n=1$ is true. If $n>1$ and suppose the statement is true for all $1,2,...,n-1$. For each i, let $x_i\in I$ such that $x_i\in\mathfrak{p}_i-\bigcup_{j\neq i}\mathfrak{p}_j$. If this is not possible, then the statement falls back into one of the cases $1,2,...,n-1$. Consider the element $y\in I$

$$y=\sum_{i=1}^n x_1x_2...x_{i-1}x_{i+1}...x_n$$

For each i, the term $x_1x_2...x_{i-1}x_{i+1}...x_n\notin\mathfrak{p}_i$ since $\mathfrak{p}_i$ is prime and all other terms belong to $\mathfrak{p}_i$. Therefore, $y\notin\mathfrak{p}_i$. That is a contradiction. □

Proposition 2.4.8
Let $A_1,A_2,...,A_n$ be ideals and $\mathfrak{p}$ be a prime ideal containing $\bigcap_{i=1}^n A_i\neq\varnothing$, then $\mathfrak{p}\supseteq A_i$ for some i. Moreover, if $\mathfrak{p}=\bigcap_{i=1}^n A_i$, then $\mathfrak{p}=A_i$ for some i

Proof. Suppose $\mathfrak{p}\nsupseteq A_i$ for all i, then for each i there exists $x_i\in A_i-\mathfrak{p}$. Hence, $\prod x_i\in\bigcap A_i$ but $\prod x_i\notin\mathfrak{p}$ since $\mathfrak{p}$ is prime, contradiction. Moreover, if $\mathfrak{p}=\bigcap A_i$, then $\mathfrak{p}\subseteq A_i$ for all i. Hence, $\mathfrak{p}=A_i$ for some i □

Definition 2.4.9 (ideal quotient, annihilator)
If A,B are ideals in a ring R, their ideal quotient is

$$(A:B)=\{x\in R:xB\subseteq A\}$$

In particular, $(0,B)$ is called the annihilator of B, denoted by $\operatorname{ann}_R(B)$

$$\operatorname{ann}_R(B)=(0,B)=\{x\in R:xB=0\}$$

2.5 EXTENSION AND CONTRACTION

Let $f : A \to B$ be a ring homomorphism, if $\mathfrak{a}$ is an ideal of A, then the image $f(\mathfrak{a})$ is generally not an ideal in B. Let $f : \mathbb{Z} \to \mathbb{R}$ be the natural inclusion and $\mathfrak{a} = (2)$, then $\mathfrak{a}$ is an ideal in $\mathbb{Z}$ but not an ideal in $\mathbb{R}$. On the other hand, if $\mathfrak{b}$ is an ideal in B, then the preimage $f^{-1}(\mathfrak{b})$ is always an ideal in A

Definition 2.5.1 (extension, contraction)
Let $f : A \to B$ be a ring homomorphism.

1. Let $\mathfrak{a}$ be an ideal in A, the ideal generated by the image $f(\mathfrak{a})$ is called extension of $\mathfrak{a}$ under f denoted by

$$\mathfrak{a}^e = f(\mathfrak{a})B = \{ab : a \in f(\mathfrak{a}), b \in B\}$$

2. Let $\mathfrak{b}$ be an ideal in B, the preimage $f^{-1}(\mathfrak{b})$ is called contraction of $\mathfrak{b}$ under f, denoted by

$$\mathfrak{b}^c = f^{-1}(\mathfrak{b}) = \mathfrak{b} \cap A$$

Proposition 2.5.2
Let $f : A \to B$ be a ring homomorphism, contraction by f maps primes into primes

Proof. *TODO* □

Proposition 2.5.3
Let $f : A \to B$ be a ring homomorphism, $\mathfrak{a} \subseteq A$, $\mathfrak{b} \subseteq B$ be ideals

1. $\mathfrak{a} \subseteq \mathfrak{a}^{ec}$ and $\mathfrak{b}^{ce} \subseteq \mathfrak{b}$
2. $\mathfrak{a}^{ece} = \mathfrak{a}^e$ and $\mathfrak{b}^{cec} = \mathfrak{b}^e$
3. *TODO - proposition 1.17*

Proof.
TODO □

2.6 SPECTRUM OF RING

Definition 2.6.1 (spectrum of ring, Zariski topology)
Let R be a ring and the spectrum of R be defined by

$$\operatorname{Spec} R = \{\mathfrak{p} \text{ prime in } R\}$$

Moreover, $\operatorname{Spec} R$ admits a topology generated by the collection of closed sets

$$\{V(I) : I \text{ ideal in } R\}$$

where $V(I)$ is the set of prime ideals containing I. The topology is called Zariski topology. Under Zariski topology, given any ring homomorphism $f : A \to B$, contraction under f defines a continuous map

$$\begin{aligned} f^* : \operatorname{Spec} B &\to \operatorname{Spec} A \\ \mathfrak{p} &\mapsto f^{-1}(\mathfrak{p}) \end{aligned}$$

Remark 2.6.2
Using this language, the radical of an ideal I of ring R is

$$\sqrt{I} = \bigcap_{\mathfrak{p} \in V(I)} \mathfrak{p}$$

Chapter 3

MODULES

3.1 MODULE AND MODULE HOMOMORPHISM

Definition 3.1.1 (module)
An module M over a ring R is an abelian group in which R acts linearly on: that is, there is a multiplication map $\cdot : R \times M \to M$ such that

$$
\begin{aligned}
r(x+y) &= rx + ry \\
(r+s)x &= rx + sx \\
(rs)x &= r(sx) \\
1x &= x
\end{aligned}
$$

for all $r, s \in R$ and $x, y \in M$

Definition 3.1.2 (module homomorphism)
Let M and N be R-modules, a map $f : M \to N$ is an R-module homomorphism (or R-linear) if

$$
\begin{aligned}
f(x+y) &= f(x) + f(y) \\
f(ax) &= af(x)
\end{aligned}
$$

for all $a \in A$ and $x, y \in M$

Remark 3.1.3 ($\mathrm{Hom}_R(M, N)$ is an R-module)
Let M and N be R-modules, the set of R-module homomorphisms of M into N, denoted by $\mathrm{Hom}_R(M, N)$ is naturally an R-module by defining addition $+ : \mathrm{Hom}_R(M, N) \times \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M, N)$ and multiplication $\cdot : \mathrm{Hom}_R(M, N) \times \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M, N)$ as follows:

$$
\begin{aligned}
(f+g)(x) &= f(x) + g(x) \\
(rg)(x) &= rg(x)
\end{aligned}
$$

for all $x \in M$, $f, g \in \mathrm{Hom}_R(M, N)$, and $r \in R$

Remark 3.1.4
Let M be an R-module, then there is a natural isomorphism

$$\begin{aligned}\mathrm{Hom}_R(R, M) &\xrightarrow{\sim} M \\ f &\mapsto f(1)\end{aligned}$$

Let I be an ideal of R, then there is a natural isomorphism

$$\mathrm{Hom}_R(R/I, M) \xrightarrow{\sim} M[I]$$

where $M[I] = \{m \in M : im = 0 \text{ for all } i \in I\}$

Remark 3.1.5 (functor $\mathrm{Hom}_R(L, -)$ and $\mathrm{Hom}_R(-, L)$)
Let L be a R-module, $\mathrm{Hom}_R(L, -)$ is a covariant functor and $\mathrm{Hom}_R(-, L)$ is a contravariant functor. If $f : M \to N$ is an R-module morphism, then the induced morphism is defined by

$$\begin{aligned}f^* : \mathrm{Hom}_R(L, M) &\to \mathrm{Hom}_R(L, N) \\ g &\mapsto fg \\ f^* : \mathrm{Hom}_R(M, L) &\leftarrow \mathrm{Hom}_R(N, L) \\ gf &\mapsfrom g\end{aligned}$$

$$\begin{tikzcd} L \arrow[d, "g"'] \arrow[dr, dashed, "fg"] & \\ M \arrow[r, "f"] & N \end{tikzcd} \qquad \begin{tikzcd} M \arrow[r, "f"] \arrow[dr, dashed, "gf"'] & N \arrow[d, "g"] \\ & L \end{tikzcd}$$

3.2 SUBMODULE AND QUOTIENT MODULE

Definition 3.2.1 (submodule)
A submodule N of an R-module M is a subgroup of M and closed under multiplication by elements of R, that is,

$$RN \subseteq N$$

N is also an R-module.

Remark 3.2.2
Let A be a ring, then A is naturally an A-module. The submodules of A as an A-module is precisely the ideals of A

Definition 3.2.3 (quotient module)
Let N be a submodule of an R-module M, then the quotient group M/N is also an R-module and called quotient module with multiplication defined by

$$\bar{x}\bar{y} = \overline{xy}$$

for all $x, y \in M$. Moreover, the natural projection

$$\begin{aligned} \phi : M &\twoheadrightarrow M/N \\ x &\mapsto \bar{x} \end{aligned}$$

is a surjective R-module homomorphism.

Remark 3.2.4
Let $f : M \to N$ be an R-module homomorphism, let

$$\begin{aligned} \ker f &= \{x \in M : f(x) = 0\} \subseteq M \\ \operatorname{im} f &= \{f(x) : x \in M\} \subseteq N \end{aligned}$$

Then, $\ker f$ is a submodule of M, $\operatorname{im} f$ is a submodule of N

Theorem 3.2.5 (the first isomorphism theorem for modules)
Let $f : M \to N$ be an R-module homomorphism, then $f : A \to B$ factors through $M/\ker f$ by the natural projection and a module homomorphism

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[d, "\phi"'] & \operatorname{im} f \\ M/\ker f \arrow[ur, "\sim"'] & \end{tikzcd}$$

Theorem 3.2.6 (the fourth isomorphism theorem for modules)
Let N be a submodule of M. There is a one-to-one correspondence between the set of submodules of M containing N and the set of submodules of M/N given by the map $\phi : M \twoheadrightarrow M/N$

$$\bar{P} = \phi(P)$$

Moreover, consider the partial order by inclusions of submodules, the correspondence is also order preserving, that is, given submodule P, Q containing N in M, then $P \subseteq Q \iff \bar{P} \subseteq \bar{Q}$

$$\begin{tikzcd} N \arrow[r, hook] \arrow[d, dashed] & P \arrow[r, hook] \arrow[d, dashed] & Q \arrow[r, hook] \arrow[d, dashed] & M \arrow[d, dashed] \\ \{0\} \arrow[r, hook] & \bar{P} \arrow[r, hook] & \bar{Q} \arrow[r, hook] & M/N \end{tikzcd}$$

3.3 OPERATION ON SUBMODULE

Definition 3.3.1 (sum, intersection)
Let M be an R-module and P and Q be submodules of M, define the following modules

1. sum of submodules
$$P + Q = \{p + q : p \in P, q \in Q\}$$
$P + Q$ is the smallest submodule containing P and Q.

2. arbitrary sum of submodules
$$\sum_{i \in I} N_i = \{n_{j_1} + ... + n_{j_k} : j_1, ..., j_k \in I, k \in \mathbb{Z}_{\geq 0}\}$$

3. intersection of submodules
$$P \cap Q$$

Proposition 3.3.2 (the second and third isomorphism theorems for modules)
If $L \supseteq M \supseteq N$ are R-modules, then
$$\frac{L/N}{M/N} \cong \frac{L}{M}$$
If P and Q are submodules of M, then
$$\frac{P+Q}{P} \cong \frac{Q}{P \cap Q}$$

Remark 3.3.3
Let $f : M \to P$ be a R-module morphism such that $N \subseteq \ker f$ for some submodule N of M, then f factors uniquely through the natural projection $M \twoheadrightarrow M/N$ by a map $f' : M/N \to P$ defined by $f'(\bar{x}) = f(x)$. This is a consequence of the second isomorphism theorems for modules.

Remark 3.3.4 (IM-notation)
Let M be an R-module and I be a subset in R, then
$$IM = \{i_1 m_1 + i_2 m_2 + ... + i_n m_n : i_1, ..., i_n \in I, m_1, ..., m_n \in M\} \subseteq M$$
if I is an ideal in R, then IM is a submodule of M.
Let A be a subset of R, then $RA = (A)$ is the ideal generated by set A.
Let $f : A \to B$ be a ring map, and $\mathfrak{a} \subseteq A$ be an ideal in A, then $f(\mathfrak{a})B$ is the extension of $\mathfrak{a}$ in B

3.4 DIRECT SUM AND DIRECT PRODUCT

Definition 3.4.1 (direct sum, direct product)
Let $(M_i)_{i\in I}$ be R-modules, define the direct product $\prod_{i\in I} M_i$ and direct sum $\bigoplus_{i\in I} M_i$

$$\bigoplus_{i\in I} M_i = \left\{(m_i)_{i\in I} \in \prod_{i\in I} M_i : \ m_i \text{ are all zeros but a finite number}\right\}$$

In particular, if M and N are R-module, $M \oplus N = M \times N$. Direct product and direct sum are R-modules with addition and multiplication defined element-wise.

3.5 EXACT SEQUENCE

Definition 3.5.1 (complex, exact sequence)
Given a sequence R-module maps

$$\ldots \longrightarrow M_{i-1} \xrightarrow{f} M_i \xrightarrow{f} M_{i+1} \longrightarrow \ldots$$

for every $i \in \mathbb{Z}$. The sequence is called a complex if

$$\operatorname{im}(f : M_{i-1} \to M_i) \subseteq \ker(f : M_i \to M_{i+1})$$

for every $i \in \mathbb{Z}$. The sequence is called exact at M_i if

$$\operatorname{im}(f : M_{i-1} \to M_i) = \ker(f : M_i \to M_{i+1})$$

The sequence is called exact if it is exact at every $i \in \mathbb{Z}$

Remark 3.5.2
Some example of exact sequences

1. $0 \longrightarrow M \xhookrightarrow{f} N$ is exact if and only if f is injective
2. $N \xrightarrow{g} Q \longrightarrow 0$ is exact if and only if g is surjective
3. $0 \longrightarrow M \xrightarrow{id} M \longrightarrow 0$ is always exact
4. $0 \longrightarrow M \xhookrightarrow{f} N \xrightarrow{g} Q \longrightarrow 0$ is exact if and only if f is injective, g is surjective, and $\operatorname{im} f = \ker g$. A sequence of this form is called short exact sequence (SES).
5. given any $f : M \to N$, there are two short exact sequences

$$0 \longrightarrow \ker f \hookrightarrow M \xrightarrow{f} \operatorname{im} f \longrightarrow 0$$

$$0 \longrightarrow \operatorname{im} f \hookrightarrow N \twoheadrightarrow \operatorname{coker} f \longrightarrow 0$$

3.6 FINITELY GENERATED MODULE FINITELY PRESENTED MODULE

Definition 3.6.1 (free module)
A free R-module is a module M isomorphic to R^A for some set A

Definition 3.6.2 (finitely generated (f.g) module)
Let M be an R-module, if there exists a finite set $\{x_1, x_2, ..., x_n\} \subseteq M$ such that every element $x \in M$ can be expressed as

$$x = r_1 x_1 + r_2 x_2 + ... + r_n x_n$$

for some $r_1, r_2, ..., r_n \in R$. Then M is called finitely generated module.

Proposition 3.6.3
M is a finitely generated R-module if and only if there is an exact sequence

$$R^n \twoheadrightarrow M \longrightarrow 0$$

so that the map $R^n \to M$ maps the i-th basis vector of R^n into x_i

Corollary 3.6.4
A-module M generated by one element is the same as a quotient module of A, that is, there exists an ideal $\mathfrak{a}$ in A so that $M \cong A/\mathfrak{a}$

Definition 3.6.5 (finitely presented (f.p))
M is finitely presented R-module if and only there is an exact sequence

$$R^m \longrightarrow R^n \twoheadrightarrow M \longrightarrow 0$$

Remark 3.6.6 (finitely generated module but not finitely presented)
Let K be a field, $R = K[x_1, x_2, ...]$ be the polynomial ring of countably infinite number of variables over K, $\mathfrak{m} = (x_1, x_2, ...)$, and $M = R/\mathfrak{m} \cong K$. Then M is finitely genrated but not finitely presented as R-module.

$$R^m \overset{\nexists}{\dashrightarrow} R \twoheadrightarrow M = R/\mathfrak{m} \cong K \longrightarrow 0$$

TODO

Proposition 3.6.7

Given a short exact sequence

$$0 \longrightarrow M \hookrightarrow N \twoheadrightarrow Q \longrightarrow 0$$

Then,

1. If M and Q are finitely generated then N is finitely generated
2. If M and Q are finitely presented then N is finitely presented

Proof.

1. (If M and Q are finitely generated then N is finitely generated)

   homework 1 (chapter 2 - problem 9)

2. (If M and Q are finitely presented then N is finitely presented)

   TODO - use snake lemma

□

Lemma 3.6.8 (snake lemma)

Let R be a ring, given a commutative diagram of modules and module homomorphisms

$$\begin{tikzcd} 0 \arrow[r, dashed] & M_1 \arrow[r, "a"] \arrow[d, "f_1"] & M_2 \arrow[r, two heads, "b"] \arrow[d, "f_2"] & M_3 \arrow[r] \arrow[d, "f_3"] & 0 \\ 0 \arrow[r] & N_1 \arrow[r, hook, "c"] & N_2 \arrow[r, "d"] & N_3 \arrow[r, dashed] & 0 \end{tikzcd}$$

and rows are exact, then there exists a **natural** exact sequence

$$\begin{tikzcd} 0 \arrow[r, dashed] & \ker f_1 \arrow[r] & \ker f_2 \arrow[r] & \ker f_3 \arrow[dll, "\delta"] & \\ & \operatorname{coker} f_1 \arrow[r] & \operatorname{coker} f_2 \arrow[r] & \operatorname{coker} f_3 \arrow[r, dashed] & 0 \end{tikzcd}$$

Moreover, if there are maps $0 \to M_1$ and $N_3 \to 0$, then there are maps $0 \to \ker f_1$ and $\operatorname{coker} f_3 \to 0$. The connecting homomorphism $\delta : \ker f_3 \to \operatorname{coker} f_1$ is defined by

1. given $x \in \ker f_3 \subseteq M_3$
2. since b is surjective, pick $y \in M_2$ so that $by = x$, then $0 = f_3x = f_3by = df_2y$, thus, $f_2y \in \ker d = \operatorname{im} c$
3. since c is injective, there is a unique $z \in N_1$ so that $cz = f_2y$
4. define $\delta : \ker f_3 \to \operatorname{coker} f_1$ by $\delta(x) = [z]$

the construction is independent of the choice of y

Remark 3.6.9 (natural exact sequence)

By natural, we mean

$$
\begin{tikzcd}
0 \arrow[rr, dashed] & & M_1 \arrow[rr, "a"] \arrow[dr] \arrow[dd, "f_1"] & & M_2 \arrow[rr, "b"] \arrow[dr] \arrow[dd, "f_2"] & & M_3 \arrow[rr] \arrow[dr] \arrow[dd, "f_3"] & & 0 & \\
& 0 \arrow[rr, dashed] & & M_1' \arrow[rr, "a'"] \arrow[dd, "f_1'"] & & M_2' \arrow[rr, "b'"] \arrow[dd, "f_2'"] & & M_3' \arrow[rr] \arrow[dd, "f_3'"] & & 0 \\
0 \arrow[rr] & & N_1 \arrow[rr, "c"] \arrow[dr] & & N_2 \arrow[rr, "d"] \arrow[dr] & & N_3 \arrow[rr, dashed] \arrow[dr] & & 0 & \\
& 0 \arrow[rr] & & N_1' \arrow[rr, "c'"] & & N_2' \arrow[rr, "d'"] & & N_3' \arrow[rr, dashed] & & 0
\end{tikzcd}
$$

induces

$$
\begin{tikzcd}
0 \arrow[r, dashed] & \ker f_1 \arrow[r] \arrow[d] & \ker f_2 \arrow[r] \arrow[d] & \ker f_3 \arrow[r, "\delta"] \arrow[d] & \operatorname{coker} f_1 \arrow[r] \arrow[d] & \operatorname{coker} f_2 \arrow[r] \arrow[d] & \operatorname{coker} f_3 \arrow[r, dashed] \arrow[d] & 0 \\
0 \arrow[r, dashed] & \ker f_1' \arrow[r] & \ker f_2' \arrow[r] & \ker f_3' \arrow[r, "\delta"] & \operatorname{coker} f_1' \arrow[r] & \operatorname{coker} f_2' \arrow[r] & \operatorname{coker} f_3' \arrow[r, dashed] & 0
\end{tikzcd}
$$

Proof. TODO □

Lemma 3.6.10 (Nakayama lemma - useless version)

Let A be a ring and M be a finitely generated A-module. If $\phi \in \operatorname{Hom}_A(M, M)$ is an R-module endomorphism such that $\operatorname{im} \phi \subseteq IM$ for an ideal I of A. Then there is an equation in $\operatorname{Hom}_A(M, M)$

$$\phi^n + a_1\phi^{n-1} + ... + a_{n-1}\phi + a_n = 0$$

for some $a_1, a_2, ..., a_n \in I$

Proof. Let $\{x_1, x_2, ..., x_n\}$ generates M. Since $\operatorname{im} \phi \subseteq IM$, then for each $i = 1, ..., n$, $\phi(x_i) \in IM$, we can write

$$\phi(x_i) = \sum_{j=1}^{n} a_{ij} x_j$$

for some $a_{ij} \in I$. We can rewrite the equation for each $i = 1, ..., n$

$$\sum_{j=1}^{n} (\delta_{ij}\phi - a_{ij}) x_j = 0$$

where $\delta_{ij} = 1$ if and only if $i = j$, otherwise $\delta_{ij} = 0$ (Kronecker delta). We can rewrite the system of equations in matrix form

$$A\vec{x} = 0$$

where $\vec{x} = (x_1, x_2, ..., x_n) \in M^n$ is a vector of n-dimension and $A \in M_n[\operatorname{Hom}_A(M, M)]$ with $A_{ij} = \delta_{ij}\phi - a_{ij}$ is a $n \times n$ matrix. Consider the ring $\operatorname{Hom}_A(M, M)$ with multiplication defined by function composition, we have [1]

$$\det(A) I_n = \operatorname{adj}(A) A$$

[1] $\operatorname{adj}(A)$ is the adjugate matrix of A

Hence,

$$\begin{bmatrix} \det(A)x_1 \\ \det(A)x_2 \\ \dots \\ \det(A)x_n \end{bmatrix} = \det(A)I_n\vec{x} = \operatorname{adj}(A)A\vec{x} = 0$$

Thus, $\det(A)x_i = 0$ for each $i = 1, 2, ..., n$. Hence, $\det(A) = 0$ in $\operatorname{Hom}_A(M, M)$. Hence, there is a polynomial as required. □

Corollary 3.6.11

Let M be a finitely generated A-module and $M = IM$ for an ideal I of A, then there is $a \in A$ so that $a = 1 \mod I$ and $aM = 0$

Proof. Let $\phi = \mathrm{id}_M : M \to M$. Nakayama lemma implies that there exists $a_n \in I$ such that $\mathrm{id}_M + a_n = 0 \in \operatorname{Hom}_A(M, M)$. Let $a = 1 + a_n \in A$, then $aM = 0$ □

Lemma 3.6.12 (Nakayama lemma - version 1)

Let M be a finitely generated A-module. If $I \subseteq J(A)$ is an ideal of A and $IM = M$, then $M = 0$

Proof. Let $a \in A$ so that $a = 1 \mod I$ such that $aM = 0$. Since $I \subseteq J(A)$, then $a \in A^\times$ is a unit of A, hence $M = a^{-1}aM = 0$ □

Lemma 3.6.13 (Nakayama lemma - version 2)

Let M be a finitely generated A-module. If $I \subseteq J(A)$ is an ideal of A and N is a submodule of M such that $M = IM + N$, then $M = N$.

Proof. Let $Q = M/N$ be an A-module, observe that $I(M/N) = (IM + N)/N$

$$IQ = I(M/N) = (IM + N)/N = M/N = Q$$

By Nakayama lemma version 1, $Q = 0$, hence $M = N$ □

Remark 3.6.14

Given any R-module M and ideal I of R, M/IM is a R/I-module

Proof. IM is a submodule of M, then M/IM is a quotient group of M. We need to define the action of R/I on M/IM. Let $r \in R$, $m \in M$, define

$$\begin{aligned} \times : R/I \times M/IM &\to M/IM \\ (\bar{r}, \bar{m}) &\mapsto \overline{rm} \end{aligned}$$

The action is well defined. Let $r_1 - r \in I$ and $m_1 - m \in IM$, then

$$\bar{r}_1\bar{m}_1 - \bar{r}\bar{m} = \overline{r_1m_1 - rm} = \overline{r_1(m_1 - m) + (r_1 - r)m} = 0$$

□

Lemma 3.6.15 (Nakayama lemma - version 3)
Let $(A, \mathfrak{m}, k)$ be a local ring. If M is finitely generated A-module and $\{x_1, x_2, ..., x_n\} \in M/\mathfrak{m}M$ generates the k-vector space $M/\mathfrak{m}M$, then any choice of lifts $\{\tilde{x}_1, \tilde{x}_2, ..., \tilde{x}_n\}$ generates M

Proof. Let N be the submodule of M generated by $\{\tilde{x}_1, \tilde{x}_2, ..., \tilde{x}_n\}$, then $M = N + \mathfrak{m}M$. By Nakayama lemma version 2, $N = M$ □

Chapter 4

LOCALIZATION

4.1 LOCALIZATION OF RING

Definition 4.1.1 (multiplicatively closed set)
Let A be a ring and a subset S of A is a multiplicatively closed if $1 \in S$ and S is closed under multiplication, that is, $s_1, s_2 \in S$ implies $s_1 s_2 \in S$.

Remark 4.1.2
If $\mathfrak{p}$ is an ideal in a ring A, then $S = A - \mathfrak{p}$ is multiplicatively closed if and only if $\mathfrak{p}$ is prime.

Theorem 4.1.3 (localization of ring, ring of fractions)
Let A be a ring and a multiplicatively closed subset $S \subseteq A$. Then, there exists a naturally associated ring $S^{-1}A$, namely ring of fractions, and a ring map $\phi_S : A \to S^{-1}A$ such that for any ring map $f : A \to B$ such that $f(S) \subseteq B^\times$, then f factors through ϕ_S by a unique ring map $g : S^{-1}A \to B$.

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "\phi_S"'] & B \\ S^{-1}A \arrow[ur, dashed, "\exists!"'] & \end{tikzcd}$$

The process of passing from A into $S^{-1}A$ is called localization.

Construction. Construct the ring $S^{-1}A$ by

$$S^{-1}A = A \times S / \sim$$

where $(a, s) \sim (a_1, s_1)$ if and only if there exists $t \in S$ such that $t(s_1 a - s a_1) = 0$. The equivalence class of (a, s) is denoted by $\frac{a}{s}$. The addition and multiplication are defined by

$$\frac{a}{s} + \frac{a_1}{s_1} = \frac{s_1 a + s a_1}{s s_1}$$
$$\frac{a}{s}\frac{a_1}{s_1} = \frac{a a_1}{s s_1}$$

The additive identity and multiplicative identity of $S^{-1}A$ are

$$0 = \frac{0}{1} \text{ and } 1 = \frac{1}{1}$$

The map $\phi_S : A \to S^{-1}A$ is

$$\begin{aligned} \phi_S : A &\to S^{-1}A \\ a &\mapsto \frac{a}{1} \end{aligned}$$

□

Remark 4.1.4

From the universal property, any construction satisfying the universal property is unique up to isomorphism. Moreover, ϕ_S is not injective in general. Observe that

1. $a \in \ker \phi_S \iff (a, 1) \sim (0, 1) \iff \exists s \in S, sa = 0$
2. for each $s \in S$, $\phi_S(s)$ is a unit in $S^{-1}A$ since $(s/1)(1/s) = 1/1$
3. ϕ_S is the universal map sending S into units in domain ring

Proof.

($\Longleftarrow$) The ring map $f' : S^{-1}A \to B$ maps units into units, then the composition $f'\phi_S : A \to B$ maps S into units of B

($\Longrightarrow$)

Existence of $f' : S^{-1}A \to B$, define

$$\begin{aligned} f' : S^{-1}A &\to B \\ \frac{a}{s} &\mapsto f(a)f(s)^{-1} \end{aligned}$$

f' is well defined because if $a_1/s_1 = a/s$, then there exists $t \in S$ such that $t(s_1 a - s a_1) = 0$. Then

$$f(t)f(s_1)f(a) - f(t)f(s)f(a_1) = 0$$

Since $f(t), f(s), f(s_1)$ are units in B, then

$$f(a)f(s)^{-1} = f(a_1)f(s_1)^{-1}$$

Uniqueness of $f' : S^{-1}A \to B$, for any map $g : S^{-1}A \to B$ satisfies the same condition. We have

$$g\left(\frac{1}{s}\right) = g\left(\left(\frac{s}{1}\right)^{-1}\right) = g\left(\frac{s}{1}\right)^{-1} = f(s)^{-1}$$

Hence,

$$g\left(\frac{a}{s}\right) = g\left(\frac{a}{1}\frac{1}{s}\right) = g\left(\frac{a}{1}\right)g\left(\frac{1}{s}\right) = f(a)f(s)^{-1} = f'\left(\frac{a}{s}\right)$$

another proof for uniqueness using $\ker f \supseteq \ker \phi_S$, then f factors through ϕ_S - need elaboration □

Corollary 4.1.5

$\phi_S : A \to S^{-1}A$ is an isomorphism if and only if $S \subseteq A^\times$

Proof.
($\implies$) For each $s \in S$, $\phi_S(s)$ is a unit in $S^{-1}A$, since $\phi_S : A^\times \to (S^{-1}A)^\times$ is a morphism of multiplicative groups and it is injective, s is a unit in A. Hence, $S \subseteq A^\times$
($\impliedby$) If $S \subseteq A^\times$, let $1_A : A \to A$, then 1_A factors through $\phi_S : A \to S^{-1}A$ by a map $f : S^{-1}A \to A$

$$\begin{tikzcd} A \arrow[r, "1_A"] \arrow[d, hook, "\phi_S"'] & A \\ S^{-1}A \arrow[ur, dashed, "f"'] & \end{tikzcd} \qquad \begin{tikzcd} A \arrow[r, "\phi_S"] \arrow[d, "\phi_S"'] & S^{-1}A \\ S^{-1}A \arrow[ur, dashed, "1_{S^{-1}A}"'] & \end{tikzcd}$$

ϕ_S is injective since $f\phi_S = 1_A$. Moreover, let $\phi_S : A \to S^{-1}A$, then ϕ_S factors **uniquely** through $\phi_S : A \to S^{-1}A$ by the map $1_{S^{-1}A} : S^{-1}A \to S^{-1}A$. That is, any map $g : S^{-1}A \to S^{-1}A$ such that $g\phi_S = \phi_S$, then g must be $1_{S^{-1}A}$. We have

$$(\phi_S f)\phi_S = \phi_S$$

Hence, $\phi_S f = 1_{S^{-1}A}$, thus ϕ_S is surjective. □

Remark 4.1.6
If S contains no zero divisor, then ϕ_S is injective. In particular, if A is a domain, then ϕ_S is injective for all S. Moreover, $S^{-1}A$ is also a domain.

Proof. *TODO* □

Remark 4.1.7
Given a ring A, if S, T are multiplicatively closed subsets of A and $S \subseteq T$. Then localizing at S then localizing at T is equivalent to localizating at T, that is,

$$T^{-1}A \cong \phi_S(T)^{-1}(S^{-1}A)$$

Proof. Given any $f : S^{-1}A \to B$ such that $f\phi_S$ sends T into units of B, then f sends $\phi_S(T)$ into units of B. Both $S^{-1}A \to T^{-1}A$ and $S^{-1}A \to \phi_S(T)^{-1}(S^{-1}A)$ satisfy the same universal property.

$$\begin{tikzcd} A \arrow[r, "\phi_S"] \arrow[d, "\phi_T"'] \arrow[rr, bend left] & S^{-1}A \arrow[r, "f"] \arrow[d, "f_2"] \arrow[dl, dashed] & B \\ T^{-1}A \arrow[urr, dashed] & \phi_S(T)^{-1}(S^{-1}A) \arrow[ur, dashed, "f_1"'] & \end{tikzcd}$$

□

Remark 4.1.8
Let A be a ring, $f \in A$, and $S = \{1, f, f^2, \dots\}$ be a multiplicative closed set. Let $A_f = S^{-1}A$, then

$$A_f \cong A[x]/(1 - fx)$$

Given any $\psi : A \to C$ that sends f into units in C, extend ψ into $\psi' : A[x] \to C$ with $\psi'(x) = \psi(f)^{-1}$. Then, $\psi'(1 - fx) = 0$. Thus ψ' factors uniquely through the natural surjection $A[x] \to A[x]/(1 - fx)$ by a map $\psi'' : A[x]/(1 - fx) \to C$

4.2 EXTENSION AND CONTRACTION

Theorem 4.2.1

Let R be a ring and S be a multiplicatively closed subset of R, and a map $\phi_S : R \to S^{-1}R$, then there is a bijection

$$\{\mathfrak{p} \text{ prime in } R \text{ such that } \mathfrak{p} \subseteq R - S\} \cong \{\mathfrak{q} \text{ prime of } S^{-1}R\}$$
$$\alpha : \mathfrak{p} \mapsto \mathfrak{p}^e$$
$$\beta : \mathfrak{q}^c \leftarrow\!\shortmid \mathfrak{q}$$

Definition 4.2.2 (saturation)

If S is a multiplicatively closed subset of a ring R, let $\mathfrak{a}$ be a subset of R, define the saturation of $\mathfrak{a}$ with respect to S by

$$\mathfrak{a}^S = \{a \in R : as \in \mathfrak{a} \text{ for some } s \in S\}$$

Note that, $\mathfrak{a} \subseteq \mathfrak{a}^S$ and $\mathfrak{a}^S = \mathfrak{a}$, then $\mathfrak{a}$ is called saturated.

$\mathfrak{a}^S = \bigcup_{s \in S}(\mathfrak{a} : s)$ where each $(A : B)$ is the collection of elements x such that multiplication by x sends B into A

Proposition 4.2.3

If $\mathfrak{a}$ is an ideal in R then $\ker \phi_S = \{0\}^S$ and $\mathfrak{a}^S$ is an ideal

Proof.

$(\ker \phi_S = \{0\}^S)$

$$x \in \ker \phi_S \iff (x, 1) \sim (0, 1) \iff tx = 0 \text{ for some } t \in S \iff x \in \{0\}^S$$

($\mathfrak{a}^S$ is an ideal) if $a, b \in \mathfrak{a}^S$, then there exists $t, s \in S$ such that $ta, sb \in \mathfrak{a}$, then $ts(a + b) \in \mathfrak{a}$ and $t(ac) \in \mathfrak{a}$ for all $c \in R$. Thus, $a + b \in \mathfrak{a}^S$ and $ac \in \mathfrak{a}^S$ for all $c \in R$. Hence, $\mathfrak{a}^S$ is an ideal. ☐

$y \in \mathfrak{a}^S \iff \frac{y}{1} = \frac{x}{s}$ in $S^{-1}A$ for some $x \in \mathfrak{a}$ and $s \in S$

Lemma 4.2.4

Let S be a multiplicatively closed subset of a ring R and $\phi_S : R \to S^{-1}R$

1. If $\mathfrak{b}$ is an ideal in $S^{-1}R$, then $\mathfrak{b}^c$ is saturated and $\mathfrak{b} = \mathfrak{b}^{ce}$
2. If $\mathfrak{a}$ is an ideal in R, then $\mathfrak{a}^e = (\mathfrak{a}^S)^e$, $\mathfrak{a}^S = \mathfrak{a}^{ec}$, and $\mathfrak{a} \subseteq R - S \iff \mathfrak{a}^e \subsetneq S^{-1}R$
3. If $\mathfrak{p}$ is a prime ideal in R such that $\mathfrak{p} \subseteq R - S$, then $\mathfrak{p} = \mathfrak{p}^S$ and $\mathfrak{p}^e$ is a prime ideal of $S^{-1}R$

Proof of Lemma.

($\mathfrak{b}^c$ is saturated) Since $\mathfrak{b}^c \subseteq (\mathfrak{b}^c)^S$, we will show that $(\mathfrak{b}^c)^S \subseteq \mathfrak{b}^c$. Let $x \in (\mathfrak{b}^c)^S$, that is, there exists $s \in S$ such that $xs \in \mathfrak{b}^c$. Hence $\frac{xs}{1} \in \mathfrak{b}$. We have $\frac{x}{1} = \frac{xs}{1}\frac{1}{s} \in \mathfrak{b}$. Then, $x \in \mathfrak{b}^c$

($\mathfrak{b} = \mathfrak{b}^{ce}$) Since $\mathfrak{b} \supseteq \mathfrak{b}^{ce}$, we will show that $\mathfrak{b} \subseteq \mathfrak{b}^{ce}$. Let $\frac{x}{s} \in \mathfrak{b}$,

$$\frac{x}{1} = \frac{x}{s}\frac{s}{1} \in \mathfrak{b} \implies x \in \mathfrak{b}^c \implies \frac{x}{1} \in \mathfrak{b}^{ce} \implies \frac{x}{s} = \frac{x}{1}\frac{1}{s} \in \mathfrak{b}^{ce}$$

($\mathfrak{a}^e = (\mathfrak{a}^S)^e$) Since $\mathfrak{a} \subseteq \mathfrak{a}^S$, then $\mathfrak{a}^e \subseteq (\mathfrak{a}^S)^e$, we will show that $(\mathfrak{a}^S)^e \subseteq \mathfrak{a}^e$. Let $x \in \mathfrak{a}^S$, then there exists $s \in S$ such that $xs \in \mathfrak{a}$. Hence $\frac{xs}{1} \in \mathfrak{a}^e$. We have $\frac{x}{1} = \frac{xs}{1}\frac{1}{s} \in \mathfrak{a}^e$. Then, $\phi_S(\mathfrak{a}^S) \subseteq a^e$. As $\mathfrak{a}^e$ is an ideal, $(\mathfrak{a}^S)^e$ is the ideal generated by a subset of $\mathfrak{a}^e$. Therefore, $(\mathfrak{a}^S)^e \subseteq \mathfrak{a}^e$
($\mathfrak{a}^S \subseteq \mathfrak{a}^{ec}$) We have $\mathfrak{a}^S \subseteq (\mathfrak{a}^S)^{ec}$, because $(\mathfrak{a}^S)^e = \mathfrak{a}^e$, then $\mathfrak{a}^S \subseteq \mathfrak{a}^{ec}$
($\mathfrak{a}^S \supseteq \mathfrak{a}^{ec}$) Let $x \in \mathfrak{a}^{ec}$, then $\frac{x}{1} \in \mathfrak{a}^e = (\phi_S(\mathfrak{a}))$. Hence

$$\frac{x}{1} = \frac{r_1}{s_1}\frac{a_1}{1} + \frac{r_2}{s_2}\frac{a_2}{1} + ... + \frac{r_n}{s_n}\frac{a_n}{1}$$

for some $r_1, r_2, ..., r_n \in R$, $s_1, s_2, ..., s_n \in S$, and $a_1, a_2, ..., a_n \in \mathfrak{a}$. This simplifies into $\frac{x}{1} = \frac{a}{s}$ for some $a \in \mathfrak{a}$ and $s \in \mathfrak{s}$. Thus, there exists $t \in S$ such that $tsx = ta \in \mathfrak{a}$. Therefore, $x \in \mathfrak{a}^S$
($\mathfrak{a} \cap S = \varnothing \implies \mathfrak{a}^e \neq S^{-1}R$) $s \in \mathfrak{a} \cap S \implies \frac{s}{1} \in \mathfrak{a}^e \implies 1 = \frac{s}{1}\frac{1}{s} \in \mathfrak{a}^e \implies \mathfrak{a}^e = S^{-1}R$
($\mathfrak{a} \cap S = \varnothing \impliedby \mathfrak{a}^e \neq S^{-1}R$) $\mathfrak{a}^e = S^{-1}R \implies \mathfrak{a}^S = \mathfrak{a}^{ec} = (S^{-1}R)^c = R$. Hence, there exists $s \in S$ such that $s1 \in \mathfrak{a}$. Thus, $S \cap \mathfrak{a} \neq \varnothing$
($\mathfrak{p} = \mathfrak{p}^S$) Since $\mathfrak{p} \subseteq \mathfrak{p}^S$, we will show that $\mathfrak{p}^S \subseteq \mathfrak{p}$. Let $x \in \mathfrak{p}^S$, that is, there exists $s \in S$ such that $xs \in \mathfrak{p}$. Since $\mathfrak{p}$ is prime and $s \in S \subseteq R - \mathfrak{p}$, then $x \in \mathfrak{p}$
($\mathfrak{p}^e$ is prime in $S^{-1}R$) Note that, $\mathfrak{p}^e$ is proper since $\mathfrak{p} \cap S = \varnothing$. Now, suppose $\frac{a}{s}\frac{b}{t} \in \mathfrak{p}^e$, then $\frac{ab}{st} = \frac{c}{u}$ for some $c \in \mathfrak{p}$ and $u \in S$. Hence $u(ab) = c(st) \in \mathfrak{p}$. Since $\mathfrak{p}$ is prime and $u \in S \subseteq A - \mathfrak{p}$, then $ab \in \mathfrak{p}$. Hence, $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. Then $\frac{a}{s} = \frac{a}{1}\frac{1}{s} \in \mathfrak{p}^e$ or $\frac{b}{t} = \frac{b}{1}\frac{1}{t} \in \mathfrak{p}^e$. That is, $\mathfrak{p}^e$ is prime. ☐

Proof of Theorem.
(α is well-defined) The lemma implies that extension of a prime ideal that does not intersect S in R is prime in $S^{-1}R$. Therefore, α is well-defined.
(β is well-defined) $\mathfrak{q}$ prime implies $\mathfrak{q}^c$ is also prime. Moreover, $\mathfrak{q} = \mathfrak{q}^{ce}$ is proper in $S^{-1}R$, then $\mathfrak{q}^c \cap S \neq \varnothing$. Therefore, β is well-defined.
(α and β are isomorphisms) The lemma implies that
For any prime ideal $\mathfrak{p}$ in R such that $\mathfrak{p} \cap S = \varnothing$, we have

$$\beta\alpha(\mathfrak{p}) = \mathfrak{p}^{ec} = \mathfrak{p}^S = \mathfrak{p}$$

For any prime ideal $\mathfrak{q}$ in $S^{-1}R$, we have

$$\alpha\beta(\mathfrak{q}) = \mathfrak{q}^{ce} = \mathfrak{q}$$

Hence, $\beta\alpha = 1$ and $\alpha\beta = 1$ ☐

Remark 4.2.5 (An equivalent formulation of the previous theorem)
Let S be a multiplicatively closed subset of a ring R and the natural map $\phi_S : R \to S^{-1}R$. Then ϕ_S induces an injective map

$$\phi_S^* : \operatorname{Spec} S^{-1}R \to \operatorname{Spec} R$$
$$\mathfrak{q} \mapsto \mathfrak{q}^c$$
$$\mathfrak{p}^e \leftarrow\!\shortmid \mathfrak{p}$$

with the image

$$\{\mathfrak{p} \text{ prime ideal in } R \text{ such that } \mathfrak{p} \subseteq R - S\}$$

Remark 4.2.6 (localization on complement of prime ideal, local ring)
Let $\mathfrak{p}$ be an ideal in A, then $S = A - \mathfrak{p}$ is multiplicatively closed if and only if $\mathfrak{p}$ is prime. When $\mathfrak{p}$ is prime, we write $A_\mathfrak{p} = S^{-1}A$. The natural map $\phi_S : A \to A_\mathfrak{p}$ induces an injective map

$$\phi_S^* : \operatorname{Spec} A_\mathfrak{p} \to \operatorname{Spec} A$$

with image

$$\{\mathfrak{q} \text{ prime ideal in } A \text{ such that } \mathfrak{q} \subseteq \mathfrak{p}\}$$

In particular, $A_\mathfrak{p}$ is a local ring since it admits the unique maximal ideal $\mathfrak{p}^e = \mathfrak{p}A_\mathfrak{p}$.

$$\mathfrak{p}A_\mathfrak{p} = \left\{\frac{x}{s} : x \in \mathfrak{p}, s \in A - \mathfrak{p}\right\}$$

quotienting at a prime $\mathfrak{p}$ is like getting the primes outside of $\mathfrak{p}$, localizing at $\mathfrak{p}$ is like getting the primes inside of $\mathfrak{p}$

Proof. Let $\mathfrak{q}$ be a prime ideal in $A_\mathfrak{p}$. We have, $\mathfrak{q}^c = \phi_S^*(\mathfrak{q}) \subseteq \mathfrak{p}$. Then $\mathfrak{q}^{ce} \subseteq \mathfrak{p}^e$. From the previous lemma, $\mathfrak{q} = \mathfrak{q}^{ce}$. Hence, any prime ideal is contained in $\mathfrak{p}^e$ □

Remark 4.2.7
If $\mathfrak{p}_1 \subseteq \mathfrak{p}_2$ are prime ideals of a ring A. The extension $\mathfrak{p}_1 A_{\mathfrak{p}_2}$ of $\mathfrak{p}_1$ is a prime ideal in $A_{\mathfrak{p}_2}$ and the localization of $A_{\mathfrak{p}_2}$ with multiplicatively closed set $A_{\mathfrak{p}_2} - \mathfrak{p}_1 A_{\mathfrak{p}_2}$ equals $A_{\mathfrak{p}_1}$

$$(A_{\mathfrak{p}_2})_{\mathfrak{p}_1 A_{\mathfrak{p}_2}} = A_{\mathfrak{p}_1}$$

Proof. *TODO* □

Remark 4.2.8 (localization in Zariski topology)
If $S = \{1, f, f^2, ...\}$, then $\operatorname{Spec} R_f \to \operatorname{Spec} R$ is an injective map with image $X_f = \operatorname{Spec} R - V(f)$. That is the set of prime ideals that do not contain f. Thus, the localization on the ideal generated by f is analogous to restriction of the spectrum of R into a basic open set in Zariski topology. Similarly, image of the image $\phi_S^* : \operatorname{Spec} S^{-1}A \to \operatorname{Spec} A$ is an open set in Zariski topology for any multiplicatively closed set.

4.3 LOCALIZATION OF MODULE

Definition 4.3.1 (localization of module, module of fractions)
Let S be a multiplicatively closed subset of a ring A and M be an A-module. Construct the $S^{-1}A$-module $S^{-1}M$ as follows:

$$S^{-1}M = M \times S / \sim$$

where $(m_1, s_1) \sim (m_2, s_2)$ if and only if there exists $t \in S$ such that $t(s_2 m_1 - s_1 m_2) = 0$. The equivalence class of (m_1, s_1) is denoted by $\frac{m_1}{s_1}$. The addition and scalar multiplication on $S^{-1}M$ are defined by

$$\frac{m_1}{s_1} + \frac{m_2}{s_2} = \frac{s_2 m_1 + s_1 m_2}{s_1 s_2}$$
$$\frac{a}{s}\frac{m_1}{s_1} = \frac{a m_1}{s s_1}$$

The zero in $S^{-1}M$ is $0 = \frac{0}{1}$

Remark 4.3.2 (localizing modules as a functor)
Let S be a multiplicatively closed subset of a ring A and $f : M \to N$ be an A-module morphism. Then there is an induced $S^{-1}A$-module morphism

$$S^{-1}f : S^{-1}M \to S^{-1}N$$
$$\frac{m}{s} \mapsto \frac{f(m)}{s}$$

That is, S^{-1} is a functor from A-mod into $S^{-1}A$-mod

Proposition 4.3.3 (localization is exact)
Let S be a multiplicatively closed subset of a ring A, then S^{-1} is exact. That is, if $M \xrightarrow{f} N \xrightarrow{g} L$ is exact at N, then the induced sequence $S^{-1}M \xrightarrow{S^{-1}f} S^{-1}N \xrightarrow{S^{-1}g} S^{-1}L$ is also exact at $S^{-1}N$

Proof.
($\operatorname{im} S^{-1}f \subseteq \ker S^{-1}g$) Let $\frac{m}{s} \in S^{-1}M$, then

$$(S^{-1}g)(S^{-1}f)\frac{m}{s} = (S^{-1}g)\frac{f(m)}{s} = \frac{(gf)(m)}{s} = \frac{0}{s} = 0$$

($\operatorname{im} S^{-1}f \supseteq \ker S^{-1}g$) Let $n \in N$ and $s \in S$ so that $\frac{n}{s} \in \ker S^{-1}g \subseteq S^{-1}N$, that is $0 = (S^{-1}g)\frac{n}{s} = \frac{g(n)}{s}$ in $S^{-1}N$. Then, there exists $t \in S$ such that $tg(n) = 0$ in L, hence $g(tn) = 0$, thus $tn \in \ker g$ implies there exists $m \in M$ such that $f(m) = tn$. Hence

$$(S^{-1}f)\frac{m}{ts} = \frac{f(m)}{ts} = \frac{tn}{ts} = \frac{n}{s}$$

□

Proposition 4.3.4 (localzation commutes with sum, intersection, quotient of submodules)
TODO - cololary 3.4

4.4 LOCAL PROPERTIES

Proposition 4.4.1 (being zero module is a local property)
Let M be any A-module, the following are equivalent

1. $M = 0$
2. $M_\mathfrak{p} = 0$ for every prime ideal $\mathfrak{p}$ of A
3. $M_\mathfrak{m} = 0$ for every maximal ideal $\mathfrak{m}$ of A

Proof. It is clear that $1 \implies 2 \implies 3$, we will show that $3 \implies 1$. Suppose $M \neq 0$, let $x \in M$ so that $x \neq 0$. Let

$$\operatorname{ann}(x) = \{a \in A : ax = 0\}$$

$\operatorname{ann}(x)$ is a proper ideal of A because if otherwise, $1 \in \operatorname{ann}(x) \implies x = 1x = 0$. This, there exists a maximal ideal $\mathfrak{m}$ containing $\operatorname{ann}(x)$. Let $\frac{x}{1} \in M_\mathfrak{m}$, since $M_\mathfrak{m} = 0$, we must have $\frac{x}{1} = 0$ in $M_\mathfrak{m}$. That is, there exists $t \in A - \mathfrak{m}$ so that $tx = 0$, hence, $t \in \operatorname{ann}(x)$. However, by definition of $\mathfrak{m}$,

$$(A - \mathfrak{m}) \cap \operatorname{ann}(x) = \varnothing$$

That is a contradiction. □

Proposition 4.4.2 (being injective and being surjective are local properties)
Let $f : M \to N$ be any A-module morphism.

1. The following are equivalent:
   (a) f is injective
   (b) $f_\mathfrak{p} = S^{-1}f : M_\mathfrak{p} \to N_\mathfrak{p}$ is injective for every prime ideal $\mathfrak{p}$ of A
   (c) $f_\mathfrak{m} = S^{-1}f : M_\mathfrak{m} \to N_\mathfrak{m}$ is injective for every maximal ideal $\mathfrak{m}$ of A
2. The following are equivalent:
   (a) f is surjective
   (b) $f_\mathfrak{p} = S^{-1}f : M_\mathfrak{p} \to N_\mathfrak{p}$ is surjective for every prime ideal $\mathfrak{p}$ of A
   (c) $f_\mathfrak{m} = S^{-1}f : M_\mathfrak{m} \to N_\mathfrak{m}$ is surjective for every maximal ideal $\mathfrak{m}$ of A

Proof.
$1a \implies 1b$ because $0 \to M \to N$ being exact at M implies $0 \to M_\mathfrak{p} \to N_\mathfrak{p}$ being exact at $M_\mathfrak{p}$ since S^{-1} is an exact functor, $1b \implies 1c$ is clear. We will show that $1c \implies 1a$. Let $K = \ker f$, then the following two sequences are exact

$$0 \longrightarrow K \longrightarrow M \xrightarrow{f} N$$

$$0 \longrightarrow K_\mathfrak{m} \longrightarrow M_\mathfrak{m} \xrightarrow{f_\mathfrak{m}} N_\mathfrak{m}$$

$f_\mathfrak{m}$ being injective implies $K_\mathfrak{m} = 0$. By the previous proposition, $K = 0$, hence f is injective
$2a \implies 2b$ because $M \to N \to 0$ being exact at N implies $M_\mathfrak{p} \to N_\mathfrak{p} \to 0$ being exact at $N_\mathfrak{p}$ since S^{-1} is an exact functor. $2b \implies 2c$ is clear. We will show that $2c \implies 2a$. Let $L = \operatorname{coker} f$, then the following two sequences are exact

$$M \xrightarrow{f} N \longrightarrow L \longrightarrow 0$$

$$M_{\mathfrak{m}} \xrightarrow{f_{\mathfrak{p}}} N_{\mathfrak{m}} \longrightarrow L_{\mathfrak{m}} \longrightarrow 0$$

$f_{\mathfrak{m}}$ being surjective implies $L_{\mathfrak{m}} = 0$. By the previous proposition, $L = 0$, hence f is surjective.

$\square$

Chapter 5

TENSOR PRODUCT

5.1 TENSOR PRODUCT OF MODULES

Definition 5.1.1 (bilinear map, multilinear map)
Let M, N, L be A-modules. A map $b : M \times N \to L$ is A-bilinear if it is A-linear in each component, that is

$$\begin{aligned} b(m_1 + m_2, n) &= b(m_1, n) + b(m_2, n) \\ b(m, n_1 + n_2) &= b(m, n_1) + b(m, n_2) \\ ab(m, b) &= b(am, n) = b(m, an) \end{aligned}$$

for all $a \in A$, $m_1, m_2 \in M$, and $n_1, n_2 \in N$. The set of all A-bilinear maps $M \times N \to L$ is denoted by

$$\mathrm{Bil}_A(M \times N, L)$$

and it carries a A-module structure induced from L, that is

$$\begin{aligned} (f + g)(m, n) &= f(m, n) + g(m, n) \\ (af)(m, n) &= af(m, n) \end{aligned}$$

Similar definition for A-multilinear maps

Theorem 5.1.2 (tensor product)
Let M, N be A-modules, there exists an A-module denoted by $M \otimes_A N$ together with a bilinear map b_{univ} : $M \times N \to M \otimes N$ so that for every A-module L the map below is an A-module isomorphism

$$\begin{aligned} \mathrm{Hom}_A(M \otimes_A N, L) &\xrightarrow{\sim} \mathrm{Bil}_A(M \times N, L) \\ f &\mapsto fb_{univ} \end{aligned}$$

Construction. Let F be the free A-module generated by $M \times N$. Let $R \subseteq F$ be the submodule generated by the elements

$$
\begin{aligned}
&(m+m_1,n)-(m,n)-(m_1,n)\\
&(m,n+n_1)-(m,n)-(m,n_1)\\
&a(m,n)-(am,n)\\
&a(m,n)-(m,an)
\end{aligned}
$$

for all $a \in A$, $m, m_1 \in M$, and $n, n_1 \in N$. Set $M \otimes N = F/R$. Let the equivalence class of (m,n) denoted by $m \otimes n$. Define

$$
\begin{aligned}
b_{univ} : M \times N &\to M \otimes N\\
(m,n) &\mapsto m \otimes n
\end{aligned}
$$

□

Proof. It is clear that the composition fb_{univ} is bilinear. Conversely, consider the bilinear map $b : M \times N \to L$, define

$$
\begin{aligned}
\tilde{b} : F &\to L\\
\sum_i a_i(m_i,n_i) &\mapsto \sum_i a_i b(m_i,n_i)
\end{aligned}
$$

As $R \subseteq \tilde{b}$, by property of kernel, $\tilde{b}$ factors through $F/R = M \otimes N$ by a unique map $\beta : M \otimes N \to L$

$$
\begin{tikzcd}
M \times N \arrow[r, hook] \arrow[d, "b"'] & F \arrow[r, two heads] \arrow[dl, "\tilde{b}"'] & F/R = M \otimes N \arrow[dll, dashed, "\beta"] \\
L & &
\end{tikzcd}
$$

The construction makes a pair of isomorphisms $\mathrm{Hom}(M \otimes N, L) \to \mathrm{Bil}(M \times N, L)$ and $\mathrm{Bil}(M \times N, L) \to \mathrm{Hom}(M \otimes N, L)$. □

Proposition 5.1.3

Some properties of tensor product induced from the universal property

$$
\begin{aligned}
M \otimes A = A \otimes M &= A\\
M \otimes N &\cong N \otimes M && \text{(since } \mathrm{Bil}(M \times N, L) \cong \mathrm{Bil}(N \times M, L)\text{)}\\
(M_1 \oplus M_2) \otimes N &\cong (M_1 \otimes N) \oplus (M_2 \otimes N)\\
(M \otimes N) \otimes L &\cong M \otimes (N \otimes L)
\end{aligned}
$$

Remark 5.1.4 (associativity of tensor product for modules of non-commutative rings)
Let A and B be any ring (possibly non-commutative), M be a right A-module, N be a left B-module, and L be a (A,B)-bimodule. Then, $M \otimes_A L$ and $L \otimes_B N$ are (A,B)-bimodules and

$$
(M \otimes_A L) \otimes_B N \cong M \otimes_A (L \otimes_B N)
$$

Remark 5.1.5 (tensor product as a functor)
Let $f_1 : M_1 \to N_1$ and $g : M_2 \to N_2$ be A-module morphisms, there is an induced A-module morphism defined by

$$\begin{aligned} f \otimes g : M_1 \otimes M_2 &\to N_1 \otimes N_1 \\ m_1 \otimes m_2 &\mapsto f(m_1) \otimes f(m_1) \end{aligned}$$

Then $(- \otimes L)$ can be defined as a functor from A-module into A-module. For any A-module morphism $f : M \to N$, the induced morphism is defined by $f \otimes 1_L : M \otimes L \to N \otimes L$

Remark 5.1.6 (extension of scalars)
Let $\phi : A \to B$ is a ring map, B is naturally an A-algebra

$$\begin{aligned} A \times B &\to B \\ (a, b) &\mapsto ab = \phi(a)b \end{aligned}$$

If M is an A-module and, then $M \otimes_A B$ carries a B-module structure with scalar multiplication in B-module defined by

$$\begin{aligned} B \times (M \otimes_A B) &\to M \otimes_A B \\ (b, m_i \otimes b_i) &\mapsto m_i \otimes bb_i \end{aligned}$$

The scalar multiplication is compatible with A-module, that is,

$$\begin{aligned} \phi(a)(m \otimes b) &= m \otimes \phi(a)b \\ &= m \otimes ab \\ &= am \otimes b \\ &= a(m \otimes b) \end{aligned}$$

Any ring map $\phi : A \to B$ induces a functor from A-module into B-module defined by $(- \otimes_A B)$

Proof. *TODO* $\square$

Proposition 5.1.7 (localizing modules is tensor product)
Let S be a multiplicatively closed subset of a ring A and M be an A-module, then there exists a canonical isomorphism of $S^{-1}A$-module

$$(S^{-1}A) \otimes_A M \xrightarrow{\sim} S^{-1}M$$

Proof. Define the map

$$\begin{aligned} (S^{-1}A) \times M &\to S^{-1}M \\ \left(\frac{a}{s}, m\right) &\mapsto \frac{am}{s} \end{aligned}$$

is A-bilinear that induces a unique A-module morphism

$$f : (S^{-1}A) \otimes M \to S^{-1}M$$
$$\frac{a}{s} \otimes m \mapsto \frac{am}{s}$$

this map is surjective since every $\frac{m}{s} \in S^{-1}M$ is mapped from $\frac{1}{s} \otimes m \in S^{-1}A \otimes M$. We will show that it is injective. Let $\sum_i \frac{a_i}{s_i} \otimes m_i \in S^{-1}A \otimes M$, let $s = \prod_i s_i$ and $t_i = \prod_{j \neq i} s_j$, then

$$\begin{aligned}
\sum_i \frac{a_i}{s_i} \otimes m_i &= \sum_i \frac{t_i a_i}{s} \otimes m_i \\
&= \sum_i \frac{1}{s} \otimes t_i a_i m_i \\
&= \frac{1}{s} \otimes \sum_i t_i a_i m_i
\end{aligned}$$

That is, every element of $S^{-1}A \otimes M$ is of the form $\frac{1}{s} \otimes m$ for some $s \in S$ and $m \in M$. Now, if $\frac{1}{s} \otimes m \in \ker f$, then $\frac{m}{s} = 0$ in $S^{-1}M$, then there exists $t \in S$ such that $tm = 0$. So

$$\frac{1}{s} \otimes m = \frac{1}{ts} \otimes tm = 0$$

Hence, $\ker f = 0$ □

Proposition 5.1.8 (tensor-hom adjunction)

Let M, N, L be A-modules, then

$$\mathrm{Hom}(M \otimes N, L) \cong \mathrm{Hom}(M, \mathrm{Hom}(N, L))$$

Proof. $\mathrm{Hom}(M \otimes N, L) \cong \mathrm{Bil}(M \times N, L) \cong \mathrm{Hom}(M, \mathrm{Hom}(N, L))$ □

5.2 EXACTNESS OF TENSOR PRODUCT

Definition 5.2.1 (exact functor)

For any exact sequence $0 \to M \to N \to L \to 0$

Let F be a covariant functor from A-module into A-module

1. F is left exact if $0 \to F(M) \to F(N) \to F(L)$
2. F is right exact if $F(M) \to F(N) \to F(L) \to 0$

Let G be a contravariant functor from A-module into A-module

1. G is left exact if $0 \to F(L) \to F(N) \to F(M)$
2. G is right exact if $F(L) \to F(N) \to F(M) \to 0$

A functor is called exact if it is both left exact and right exact.

note, one can prove that we don't require the original sequence $0 \to M \to N \to L \to 0$ to be complete

Lemma 5.2.2 (Hom functors are left exact)
For any A-module P, the covariant functor $\mathrm{Hom}(P,-)$ and the contravariant functor $\mathrm{Hom}(-,P)$ are **left exact**. That is, if the first row is exact then the following two rows are exact

$$\begin{tikzcd}
0 \arrow[r, dashed] & M \arrow[r, "i"] & N \arrow[r, "p"] & L \arrow[r, dashed] & 0 \\
0 \arrow[r] & \mathrm{Hom}(P,M) \arrow[r, hook, "i_1"] & \mathrm{Hom}(P,N) \arrow[r, "p_1"] & \mathrm{Hom}(P,L) \\
0 \arrow[r] & \mathrm{Hom}(L,P) \arrow[r, hook, "p_2"] & \mathrm{Hom}(N,P) \arrow[r, "i_2"] & \mathrm{Hom}(M,P)
\end{tikzcd}$$

Moreover, the statement is if and only if. That is, if one of Hom sequences is exact for every A-module P, then the original sequence is exact

Proof. *Below is a sketch proof for the ($\Longrightarrow$) direction, the ($\Longleftarrow$) direction can be constructed*

(i is mono $\implies$ i_1 is mono) Let a and b be two maps in $\mathrm{Hom}(P,M)$, then $i_1(a)=ia, i_1(b)=ib$, since i is mono, $ia=ib \implies a=b$, that is i_1 is mono

$$\begin{tikzcd}
M \arrow[r, hook, "i"] & N \\
P \arrow[u, "a"'] \arrow[u, bend left, "b"] \arrow[ur, dashed, "ia"] \arrow[ur, dashed, bend right, "ib"']
\end{tikzcd}$$

($\operatorname{im} i \subseteq \ker p \implies \operatorname{im} i_1 \subseteq \ker p_1$) Let $a \in \mathrm{Hom}(P,M)$, then $p_1 i_1(a) = pib$. As $pi=0$, then $p_1 i_1 = 0$, that is $\operatorname{im} i_1 \subseteq \ker p_1$

$$\begin{tikzcd}
M \arrow[r, "i"] & N \arrow[r, "p"] & L \\
P \arrow[u, "a"] \arrow[ur, dashed, "ia"] \arrow[urr, dashed, "pib"']
\end{tikzcd}$$

(i is mono and $\operatorname{im} i = \ker p \implies \operatorname{im} i_1 \supseteq \ker p_1$) Let $a \in \ker p_1$, that is $p_1(a)=pa=0$. Since $i: M \to N$ is the kernel of $p: N \to L$, then a factors uniquely through i by a map $b: M \to P$. Hence, $a = i_1(b)$, that is $a \in \operatorname{im} i_1$

$$\begin{tikzcd}
M \arrow[r, hook, "i"] & N \arrow[r, "p"] & L \\
& P \arrow[ul, dashed, "b"] \arrow[u, "a"] \arrow[ur, dashed, "0"']
\end{tikzcd}$$

(p is epi $\implies$ p_2 is mono) Let a and b be two maps in $\mathrm{Hom}(L,P)$, then $p_2(a)=ap, p_2(b)=bp$, since p is epi, $ap=bp \implies a=b$, that is p_2 is mono.

$$\begin{tikzcd}
& P \\
N \arrow[r, two heads, "p"'] \arrow[ur, dashed, "ap"'] \arrow[ur, dashed, bend left, "bp"] & L \arrow[u, "a"] \arrow[u, bend right, "b"']
\end{tikzcd}$$

($\operatorname{im} i \subseteq \ker p \implies \operatorname{im} p_2 \subseteq \ker i_2$) Let $a \in \mathrm{Hom}(L,P)$, then $i_2 p_2(a) = api$. As $pi=0$, then $i_2 p_2 = 0$, that is $\operatorname{im} p_2 \subseteq \ker i_2$

$$\begin{tikzcd}
& & P \\
M \arrow[r, "i"'] \arrow[urr, dashed, "api"] & N \arrow[r, two heads, "p"'] \arrow[ur, dashed, "ap"] & L \arrow[u, "a"']
\end{tikzcd}$$

(p is epi and $\operatorname{im} i = \ker p \implies \operatorname{im} p_2 \subseteq \ker i_2$) Let $a \in \ker i_2$, that is $i_2(a) = ai = 0$. Since $p : N \to L$ is the cokernel of $i : M \to N$, then a factors uniquely through p by a map $b : L \to P$. Hence, $a = p_2(b)$, that is $a \in \operatorname{im} p_2$

$$\begin{tikzcd} & P & \\ M \arrow[r, "i"'] \arrow[ur, dashed, "0"] & N \arrow[u, "a"] \arrow[r, two heads, "p"'] & L \arrow[ul, dashed, "b"'] \end{tikzcd}$$

□

Proposition 5.2.3 (adjunction induces exact functors)
Let (F, G) be an adjunction of A-modules, that is, for any A-modules M, N, then

$$\operatorname{Hom}(F(M), N) \cong \operatorname{Hom}(M, G(N))$$

Then, F is right exact and G is left exact

Proof. For any A-module P
(F is right exact) the following rows are exact

$$\begin{tikzcd} M \arrow[r] & N \arrow[r] & L \arrow[r] & 0 \end{tikzcd}$$

$$\begin{tikzcd} 0 \arrow[r] & \operatorname{Hom}(L, G(P)) \arrow[r] \arrow[d, "\sim"'] & \operatorname{Hom}(N, G(P)) \arrow[r] \arrow[d, "\sim"'] & \operatorname{Hom}(M, G(P)) \arrow[d, "\sim"'] \\ 0 \arrow[r] & \operatorname{Hom}(F(L), P) \arrow[r] & \operatorname{Hom}(F(N), P) \arrow[r] & \operatorname{Hom}(F(M), P) \end{tikzcd}$$

$$\begin{tikzcd} F(M) \arrow[r] & F(N) \arrow[r] & F(L) \arrow[r] & 0 \end{tikzcd}$$

(G is left exact) the following rows are are exact

$$\begin{tikzcd} 0 \arrow[r] & M \arrow[r] & N \arrow[r] & L \end{tikzcd}$$

$$\begin{tikzcd} 0 \arrow[r] & \operatorname{Hom}(F(P), M) \arrow[r] \arrow[d, "\sim"'] & \operatorname{Hom}(F(P), N) \arrow[r] \arrow[d, "\sim"'] & \operatorname{Hom}(F(P), L) \arrow[d, "\sim"'] \\ 0 \arrow[r] & \operatorname{Hom}(P, G(M)) \arrow[r] & \operatorname{Hom}(P, G(N)) \arrow[r] & \operatorname{Hom}(P, G(L)) \end{tikzcd}$$

$$\begin{tikzcd} 0 \arrow[r] & G(M) \arrow[r] & G(N) \arrow[r] & G(L) \end{tikzcd}$$

□

Corollary 5.2.4 (tensor product is right exact)
Tensor-hom adjunction $\operatorname{Hom}(M \otimes N, L) \cong \operatorname{Hom}(M, \operatorname{Hom}(N, L))$ where $F = (- \otimes N)$ and $G = \operatorname{Hom}(-, L)$. Then, $(- \otimes N)$ a right exact covariant functor. That is, for any A-module P, the following rows are exact

$$\begin{tikzcd} M \arrow[r] & N \arrow[r] & L \arrow[r] & 0 \end{tikzcd}$$

$$\begin{tikzcd} M \otimes P \arrow[r] & N \otimes P \arrow[r] & L \otimes P \arrow[r] & 0 \end{tikzcd}$$

Definition 5.2.5 (flat module)
An A-module L is flat if the functor $(- \otimes L)$ is exact. Equivalently, for any injective map $M \hookrightarrow N$, the induced map $M \otimes L \hookrightarrow N \otimes L$ is also injective.

Proposition 5.2.6
Let S be a multiplicatively closed subset of a ring A, then $S^{-1}A$ is flat.

Proof. Since $(S^{-1}-)$ is an exact functor from A-module into A-module and $(S^{-1}-) = (S^{-1}A \otimes -)$. Then $S^{-1}A$ is flat. ☐

Proposition 5.2.7 (flatness is a local property)
Let M be any A-module, the following are equivalent

1. M is flat
2. $M_{\mathfrak{p}}$ is flat over $A_{\mathfrak{p}}$ for every prime ideal $\mathfrak{p}$ of A
3. $M_{\mathfrak{m}}$ is flat over $A_{\mathfrak{m}}$ for every maximal ideal $\mathfrak{m}$ of A

Lemma 5.2.8 (useful calculation technique)
Let $\phi : A \to B$ be a ring map, I be an ideal of B and M be an A-module, then by right exactness of tensor product, the sequences below are exact

$$0 \longrightarrow I \xhookrightarrow{\ i\ } B \xrightarrow{\ p\ } B/I \longrightarrow 0$$

$$I \otimes_A M \xrightarrow{i \otimes 1} B \otimes_A M \longrightarrow B/I \otimes_A M \longrightarrow 0$$

Then, $B/I \otimes_A M = \operatorname{coker}(i \otimes 1)$. In particular, when $B = A$, $\phi = 1_A$ and I is an ideal in A, then

$$A/I \otimes_A M \cong M/IM$$

when $B = A$, I is an ideal of A and $M = A/J$, then

$$A/I \otimes_A A/J \cong A/(I + J)$$

Proof.
$(A/I \otimes_A M \cong M/IM)$

$$I \otimes_A M \xrightarrow{i \otimes 1} A \otimes_A M \xrightarrow{\ \sim\ } M$$

$$a \otimes m \longmapsto a \otimes m \longmapsto am$$

Every element $a \otimes m \in I \otimes_A M$ is mapped into the element $am \in M$, hence the image of $(i \otimes 1)$ in M is IM. Hence, $\operatorname{coker}(i \otimes 1) \cong M/IM$
$(A/I \otimes_A A/J \cong A/(I + J))$

$$\begin{array}{ccccc} I \otimes_A A/J & \xrightarrow{i\otimes 1} & A \otimes_A A/J & \xrightarrow{\sim} & A/J \\ a \otimes \bar{b} & \longmapsto & a \otimes \bar{b} & \longmapsto & \overline{ab} \end{array}$$

Every element $a \otimes \bar{b} \in I \otimes_A A/J$ is mapped into the element $\overline{ab} \in A/J$ for $a \in I$ and $b \in A$. Hence, $\mathrm{im}(i \otimes 1)$ in A/J is $\{i + J : i \in I\} = I/J = (I + J)/J$, then

$$\mathrm{coker}(i \otimes 1) = \frac{A/J}{(I+J)/J} = \frac{A}{I+J}$$

□

5.3 TENSOR PRODUCT OF ALGEBRAS

Theorem 5.3.1 (tensor product of algebras)

Let B and C be A-algebra and two maps from the initial object A of the category A-algebras into B and C. Then the A-module $B \otimes_A C$ carries an A-algebra structure and is the pushout of the diagram $B \leftarrow A \to C$

$$\begin{tikzcd} & B \arrow[d] \arrow[dr] & \\ A \arrow[ur] \arrow[dr] & B \otimes_A C \arrow[r, dashed] & D \\ & C \arrow[u] \arrow[ur] & \end{tikzcd}$$

Construction. We will define multiplication on $B \otimes_A C$. Consider the multilinear map

$$B \times C \times B \times C \to B \otimes_A C$$
$$(b_1, c_1, b_2, c_2) \mapsto b_1 b_2 \otimes c_1 c_2$$

The map induces a bilinear map $\mu : (B \otimes C) \times (B \otimes C) \to B \otimes C$

$$\begin{tikzcd} B \times C \times B \times C \arrow[d] \arrow[dr] & \\ (B \otimes C) \otimes (B \otimes C) \arrow[r, dashed] & B \otimes C \\ (B \otimes C) \times (B \otimes C) \arrow[u] \arrow[ur, "\mu"'] & \end{tikzcd}$$

The multiplicative identity on $B \otimes C$ is $1 \otimes 1$ □

Proof. *TODO - proof the universality* □

Remark 5.3.2

Let B be an A-algebra (there is a natural map $\phi : A \to B$ defined by $\phi(a) = a1_B$)), then

$$B \otimes_A A[x] \xrightarrow{\sim} B[x]$$

Proof. The isomorphism as A-module can be proven by writing $A[x] = \bigoplus_{n=0}^{\infty} A$, then $B \otimes A[x] = B \otimes_A \left(\bigoplus_{n=0}^{\infty} A\right) = \bigoplus_{n=0}^{\infty} B \otimes_A A = \bigoplus_{n=0}^{\infty} B = B[x]$. The proof for A-algebra can be done by constructing isomorphisms $f : B \otimes_A A[x] \to B[x]$ and $g : B[x] \to B \otimes_A A[x]$ by

$$f\left(\sum_i \left(b_i \otimes \sum_{ij} a_j x^j\right)\right) = \sum_i \sum_j a_{ij} b_i x^j$$

$$g\left(\sum_j b_j x^j\right) = \sum_j b_j \otimes x^j$$

(alternative proof using universal property) The image of composition $A \to B \to B[x]$ is identical to the image of the composition $A \to A[x] \to B[x]$ which is the subring A of B in $B[x]$

$$\begin{tikzcd}
 & B \arrow[d, "\beta"'] \arrow[dr, "f"] & \\
A \arrow[ur] \arrow[dr] & B[x] \arrow[r, dashed, "h"] & D \\
 & A[x] \arrow[u, "\alpha"] \arrow[ur, "g"'] &
\end{tikzcd}$$

Let $f : B \to D$ and $g : A[x] \to D$ so that the diagram commutes. We will construct the map $h : B[x] \to D$ so that the diagram commutes. For any $b_n x^n \in B[x]$, define

$$h(b_n x^n) = f(b_n) g(x^n)$$

For any $b \in B$, $h\beta(b) = h(b) = f(b)$. For any $a_n x^n \in A[x]$, $h\alpha(a_n x^n) = h(a_n x^n) = f(a_n) g(x^n)$. Note that, $f(a_n) = g(a_n)$, then $h\alpha(a_n x^n) = g(a_n) g(x^n) = g(a_n x^n)$. Hence, the diagram with h commutes
Now, if $h_1 : B[x] \to D$ is another map that makes the diagram commutes, then we must have $h_1(b_n) = h_1\beta(b_n) = f(b_n)$ and $h_1(x^n) = h_1\alpha(x^n) = g(x^n)$, then

$$h_1(b_n x^n) = h_1(b_n) h_1(x^n) = f(b_n) g(x^n) = h(b_n x^n)$$

Hence, h is unique. $\square$

Remark 5.3.3
Calculate $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$

Proof. We have $\mathbb{C} = \mathbb{R}[x]/(x^2+1)$, and the exact sequence

$$(x^2+1) \otimes_{\mathbb{R}} \mathbb{C} \xrightarrow{i \otimes 1} \mathbb{R}[x] \otimes_{\mathbb{R}} \mathbb{C} \twoheadrightarrow \mathbb{R}[x]/(x^2+1) \otimes_{\mathbb{R}} \mathbb{C} \longrightarrow 0$$

Then

$$\begin{aligned} \mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} &= \mathbb{R}[x]/(x^2+1) \otimes_{\mathbb{R}} \mathbb{C} \\ &= (\mathbb{R}[x] \otimes_A \mathbb{C}) / \operatorname{im}(i \otimes 1) \end{aligned}$$

We have

$$(x^2+1)\otimes_{\mathbb{R}}\mathbb{C} \xrightarrow{i\otimes 1} \mathbb{R}[x]\otimes_{\mathbb{R}}\mathbb{C} \xrightarrow{\sim} \mathbb{C}[x]$$

$$f(x)(x^2+1)\otimes c \longmapsto f(x)(x^2+1)\otimes c \longmapsto cf(x)(x^2+1)$$

Hence, $\mathrm{im}(i\otimes 1)$ in $\mathbb{C}[x]$ is the ideal generated by (x^2+1), then

$$\mathbb{C}\otimes_{\mathbb{R}}\mathbb{C} = \mathbb{C}[x]/(x^2+1) = \mathbb{C}[x]/(x+i)(x-i)$$

By CRT for coprime ideals $(x+i)$ and $(x-i)$

$$\mathbb{C}\otimes_{\mathbb{R}}\mathbb{C} = \mathbb{C}[x]/(x+i)(x-i) = \mathbb{C}[x]/(x+i)\times\mathbb{C}[x]/(x-i) = \mathbb{C}\times\mathbb{C}$$

Note that, the map $\mathbb{C}\otimes_{\mathbb{R}}\mathbb{C}\to\mathbb{C}\times\mathbb{C}$ is defined by $a\otimes b\mapsto(\bar{a}b, ab)$ □

Remark 5.3.4

For any Galois extension of fields E/F

$$E\otimes_F E = E^{\deg(E/F)}$$

never studied any field theory - I absolutely have no idea what a Galois extension is

5.4 TEASER

Remark 5.4.1

Tor and Ext functors

Remark 5.4.2

If L is a flat module and the top sequence is exact, then the bottom sequence is also exact

$$0 \longrightarrow M \longrightarrow N \longrightarrow L \longrightarrow 0$$

$$0 \longrightarrow M\otimes P \longrightarrow N\otimes P \longrightarrow N\otimes P \longrightarrow 0$$

An A-module M is flat if and only if for any ideal $I\subseteq A$, the canonical map

$$I\otimes_A M\to IM$$

is an isomorphism

Chapter 6

NOETHERIAN RING

6.1 NOETHERIAN RING

Definition 6.1.1 (Noetherian ring)
Given a ring A, the following are equivalent

1. Ascending chain condition (ADC): every chain of ideals in A stablizes

$$I_1 \subseteq I_2 \subseteq I_3 ...$$

   That is, $I_n = I_{n+1}$ for large n

2. Every ideal I in A is finitely generated

3. For any A-modules N and M so that $N \subseteq M$, M is finitely generated implies N is finitely generated

A ring A satisfies one of those conditons is called Noetherian ring.

Proof.
($1 \implies 2$) Suppose an ideal I of A is not finitely generated, there exists a sequence $a_1, a_2, a_3, ... \in I$ that generate I, that is, $I = (a_1, a_2, a_3, ...)$, then there exists a chain

$$(a_1) \subseteq (a_1, a_2) \subseteq (a_1, a_2, a_3) \subseteq ... \subseteq I$$

so that infinitely many number of inclusions are strict.
($2 \implies 3$) Induction of minimal number of generators of M
If M is generated by 1 element, namely m, then any element in M can be written by am for some $a \in A$. The map

$$\begin{aligned} \phi : A &\to M \\ a &\mapsto am \end{aligned}$$

is a surjective A-module morphism, then $M \cong A/\ker\phi$. $\ker\phi$ is a submodule of A as A-module and also an ideal of A be cause if $r \in A$ and $a \in \ker\phi$, then

$$\phi(ra) = r\phi(a) = 0$$

Hence, $M \cong A/I$ for some ideal I of A. Now, any submodule N in M corresponds to an ideal in A/I and any ideal in

A/I corresponds to an ideal J in A containing I. Since J is finitely generated, then J/I in A/I is finitely generated, then N is also finitely generated.
Suppose $2 \implies 3$ for every number of generators $1, 2, ..., n-1$ of M. If M is generated by $\{x_1, x_2, ..., x_n\}$, let M_1 be the submodule generated by x_1, then M/M_1 is generated by $\{\bar{x}_2, ..., \bar{x}_n\}$. Let N be a submodule of M, then the following two sequences are exact

$$\begin{tikzcd} 0 \arrow[r] & N \cap M_1 \arrow[r] \arrow[d, hook] & N \arrow[r] \arrow[d, hook] & N/(N \cap M_1) \arrow[r] \arrow[d, hook] & 0 \\ 0 \arrow[r] & M_1 \arrow[r] & M \arrow[r] & M/M_1 \arrow[r] & 0 \end{tikzcd}$$

$N \cap M_1$ is finitely generated since it is a submodule of M_1 which is generated by 1 elements. $N/(N \cap M_1)$ is finitely generated since it is a submodule of M/M_1 which is generated by $n-1$ elements. Hence N is finitely generated due to exactness of the top sequence.
($3 \implies 1$) Given a chain of ideals

$$I_1 \subseteq I_2 \subseteq I_3 ...$$

Then $I = \bigcup_{n \in \mathbb{N}} I_n$ is also an ideal. Ideals in A are the submodules of A as an A-module. Therefore, A is finitely generated as an A-module implies I is finitely generated as an A-module which is also finitely generated as an ideal. Let

$$I = \langle x_1, x_2, ..., x_m \rangle$$

Each $x_i \in \{x_1, x_2, ..., x_m\}$ belong to some I_n in $I_1, I_2, I_3 ...$, let I_N be the the smallest ideal in the chain containing $\{x_1, x_2, ..., x_m\}$. Then

$$I = \langle x_1, x_2, ..., x_m \rangle \subseteq I_N \subseteq I$$

Hence, $I_n = I_{n+1}$ for all $n \geq N$ $\square$

Remark 6.1.2
Some examples of Noetherian rings

1. $\mathbb{Z}$ is Noetherian, all fields are Noetherian
2. If A is Noetherian and I is an an ideal of A, then A/I is Noetherian
3. If A is Noetherian and S is a multiplicatively closed subset of A, then $S^{-1}A$ is Noetherian

Proof.
(2) one to one correspondence between ideals of A/I and ideal of A containing I
(3) Any ideal I of $S^{-1}A$ is extended from ideal J of A which is finitely generated, if $J = (x_1, x_2, ..., x_n)$, then $I = \left(\frac{x_1}{1}, \frac{x_2}{s}, ..., \frac{x_n}{1}\right)$ $\square$

Theorem 6.1.3 (Hilbert basis theorem)
If A is a Noetherian ring, then $A[x]$ is also Noetherian

Proof. If a nonzero ideal I in $A[x]$ is not finitely generated, we inductively construct $f_0(x), f_1(x), f_2(x), ... \in A[x]$ and ideals $I_n = (f_0(x), f_1(x), ..., f_n(x))$ as follows:
Pick a nonzero polynomial $f_0(x) \in I$ of minimal degree, set

$$I_0 = (f_0(x))$$

If we already picked $f_0(x), f_1(x), ..., f_{n-1}(x)$, pick a nonzero polynomial $f_n(x) \in I - I_{n-1}$ of minimal degree, set

$$I_n = (f_0(x), f_1(x), ..., f_n(x))$$

By construction, the sequence of degrees of $f_0(x), f_1(x), f_2(x), ...$ is non-decreasing, that is

$$\deg f_0(x) \leq \deg f_1(x) \leq \deg f_2(x) \leq ...$$

Let $a_n \in A$ be the leading coefficient of $f_n(x)$ and $J \subseteq A$ be the ideal

$$J = (a_0, a_1, a_2, ...)$$

Since A is Noetherian, J is finitely generated, hence

$$J = (a_0, a_1, ..., a_{N-1})$$

for some $N \in \mathbb{N}$. Thus,

$$a_N = \sum_{i=0}^{N-1} y_i a_i$$

for some $y_1, y_2, ..., y_{N-1} \in A$. Consider the polynomial

$$g(x) = \sum_{i=1}^{N-1} y_i x^{\deg f_N(x) - \deg f_i(x)} f_i(x) = a_N x^{\deg f_N(x)} + h(x)$$

where $\deg h(x) < \deg f_N(x)$. Since $g(x)$ is a $A[x]$-linear combination of $f_i(x)$, $g(x) \in I_{N-1}$. $f(x) \notin I_{N-1}$, then $f_N(x) - g(x) \notin I_{N-1}$. This is a contradiction of minimality of degree of $f_N(x)$ because $f_N(x) - g(x) \notin I_{N-1}$ and $\deg(f_N(x) - g(x)) < \deg f_N(x)$ □

Corollary 6.1.4

If A is Noetherian, then $A[x_1, x_2, ..., x_n]$ is also Noetherian

Remark 6.1.5

If A is Noetherian, then the power series ring $A[[x]]$ is also Noetherian

Proof. *HW* □

Definition 6.1.6 (finitely generated algebra, finite presented algebra)

Let A be a ring and B be an A-algebra. B is called finite generated (or finite type) as an A-algebra if the inclusion $A \to A[x_1, x_2, ..., x_n]$ factors through B

$$\begin{tikzcd} & A[x_1, x_2, ..., x_n] \arrow[d, two heads] \\ A \arrow[ur, hook] \arrow[r] & B \end{tikzcd}$$

That is, there exists an isomorphism $B \cong \frac{A[x_1, x_2, ..., x_n]}{I}$ for some ideal I of $A[x_1, x_2, ..., x_n]$. If moreover, I is a finitely generated as an $A[x_1, x_2, ..., x_n]$-module, B is called finitely presented A-algbera.

Proposition 6.1.7
If A is Notherian, then any finitely generated A-algebra is Noetherian.

6.2 A PREVIEW OF DIMENSION THEORY

Definition 6.2.1 (height, Krull dimension)
Given a prime ideal $\mathfrak{p}$ of a ring A, define the height of $\mathfrak{p}$ by

$$\operatorname{ht}\mathfrak{p} = \sup\{n \geq 0 : \text{ there exists a chain of prime ideals } (0) = \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \mathfrak{p}_2 \subsetneq ... \subsetneq \mathfrak{p}_n = \mathfrak{p}\}$$

The dimension of A is defined by

$$\dim A = \sup_{\mathfrak{p} \text{ prime in } A} \operatorname{ht}\mathfrak{p}$$

Remark 6.2.2
Some examples of dimension

1. $\dim k = 0$ for any field k
2. $\dim \mathbb{Z} = 1$ ($\operatorname{ht}\mathfrak{p} = 1$ for any prime $\mathfrak{p}$ in $\mathbb{Z}$)
3. $\dim k[x_1, x_2, ..., x_n] \geq n$ for any field k ($(x_1) \subsetneq (x_1, x_2) \subsetneq ... \subsetneq (x_1, x_2, .., x_n)$)

Theorem 6.2.3
If A is Noetherian, then

$$\dim A[x] = \dim A + 1$$

will be proved in chapter dimension theory

Remark 6.2.4
If A is Noetherian, then $\operatorname{ht}\mathfrak{p}$ is finite for any prime ideal $\mathfrak{p}$ of A. However, $\dim A$ can be infinite (Nagata 50s)

Remark 6.2.5
If A is not Noetherian and $\dim A$ is finite, then

$$\dim A + 1 \leq \dim A[x] \leq 2 \dim A$$

There are examples exhibiting every possibility of this range

Chapter 7

INTEGRAL DEPENDENCE

7.1 INTEGRAL DEPENDENCE

Remark 7.1.1 (ring extension)
If ring map $A \to B$ is injective, we usually write $A \subset B$ or $A \hookrightarrow B$. The ring map $A \to B$ is called a ring extension.

Definition 7.1.2 (integral)
Given a ring extension $A \hookrightarrow B$, an element $x \in B$ is integral over A if it satisfies a monic polynomial with coefficients in A, that is

$$x^n + a_1 x^{n-1} + ... + a_n = 0$$

for some $a_1, a_2, ..., a_n \in A$

Remark 7.1.3
Some examples of integral: $\mathbb{Z} \hookrightarrow \mathbb{Q}$, the integral elements over $\mathbb{Z}$ is $\mathbb{Z}$

Proposition 7.1.4
Given a ring extension $A \hookrightarrow B$, let $x \in B$, the following are equivalent:

1. x is integral over A
2. the ring $A[x] \subseteq B$ is finitely generated A-module
3. $A[x]$ is contained in a subring C of B such that C is also a finitely generated A-module
4. there exists a faithful $A[x]$-module M which is finitely generated as an A-module An R-module M is faithful if and only if $\mathrm{ann}_R(M) = \{r \in R : rM = 0\} = 0$ if and only if $R \to \mathrm{Hom}_R(M, M)$ is injective.

Proof. $(1 \implies 2)$ If x is integral over A, then

$$x^n = -(a_1 x^{n-1} + ... + a_n)$$

for some $a_1, a_2, ..., a_n \in A$. That is x^n can be written as a polynomial of degree $\leq n-1$, hence $A[x]$ is generated by $1, x, x^2, ..., x^{n-1}$ as an A-module.

($2 \implies 3$) take $C = A[x]$

($3 \implies 4$) take $M = C$ which is a faithful $A[x]$-module since $yC = 0 \implies y1 = 0$

($4 \implies 3$) Consider the $A[x]$-module endomorphism

$$\phi : M \to M$$
$$m \mapsto xm$$

By Nakayama lemma useless version for ideal A in $A[x]$, then there is an equation in $\mathrm{Hom}_{A[x]}(M, M)$

$$\phi^n + a_1\phi_{n-1} + ... + a_n = 0$$

for some $a_1, a_2, ..., a_n \in A$. Since M is faithful, the map $A[x] \to \mathrm{Hom}_{A[x]}(M, M)$ is injective. Taking the preimage of $\phi^n + a_1\phi_{n-1} + ... + a_n$ under $A[x] \to \mathrm{Hom}_{A[x]}(M, M)$ is

$$x^n + a_1x^{n-1} + ... + a_n = 0$$

□

Corollary 7.1.5

Given a ring extension $A \hookrightarrow B$ and $x_1, x_2, ..., x_n \in B$ are integral over A, then $A[x_1, x_2, ..., x_n] \subseteq B$ is a finitely generated A-module

Proof. Prove by induction. Base case $n = 1$ is from the previous proposition. Suppose the statement is true for $n - 1$, since $x_2, ..., x_n$ are integral over A, they are also integral over $A[x_1]$. Moreover, $A[x_1] \hookrightarrow B$ is also a ring extension, hence $A[x_1][x_2, ..., x_n] \subseteq B$ is a finitely generated $A[x_1]$-module, that is also a finitely generated A-module. □

Definition 7.1.6 (integral closure, integrally closed, integral ring extension)

Given a ring extension $A \hookrightarrow B$, the subset $C \subseteq B$ of integral elements over A is a subring of B.

1. C is called the integral closure of A in B, denoted by $A^{icl \subset B}$
2. if $C = B$, $A \hookrightarrow B$ is called integral ring extension
3. if $C = A$, A is called integrally closed in B

Proof. If x, y are integral over A, then $C = A[x, y]$ is a finitely generated A-module and $x \pm y$ and xy are elements of C, hence $A[x \pm y], A[xy] \in C$. By ($3 \implies 1$), $x \pm y$ and xy are integral over A □

Remark 7.1.7

Some example of integral closure

1. $\mathbb{Z} \hookrightarrow \mathbb{Q}$, then $\mathbb{Z}^{icl \subset \mathbb{Q}} = \mathbb{Z}$
2. $\mathbb{Z} \hookrightarrow \mathbb{Q}[\sqrt{5}]$, then $\mathbb{Z}^{icl \subset \mathbb{Q}[\sqrt{5}]} = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$

Proposition 7.1.8 (transitivity of integral dependence)

If $A \hookrightarrow B$ and $B \hookrightarrow C$ are integral ring extensions, then $A \hookrightarrow C$ is an integral ring extension

Proof. Let $x \in C$, since $B \to C$ is integral ring extension, then

$$x^n + b_1 x^{n-1} + ... + b_n = 0$$

for some $b_1, ..., b_n \in B$. Since $A \to B$ is integral ring extension, then the subring $B' = A[b_1, ..., b_n]$ of B is a finitely generated A-module. Note that, x is integral with respect to the ring extension $B' \hookrightarrow B$, hence $B'[x]$ is a finitely generated B'-module. B' is a finitely generated A-module, hence $B'[x]$ is a finitely generated A-module. Thus

$$A[x] \subseteq B'[x] \subseteq C$$

Hence, x is integral with respect to the ring extension $A \to C$ □

Remark 7.1.9

Given ring extension $A \hookrightarrow B$, if x is integral over A in B, then $A[x]$ is a subring of the integral closure of A in B and $A \hookrightarrow A[x]$ is an integral ring extension. In other words, integral closure of A in B is the union of subrings $A[x]$

Proof. For any $y \in A[x]$, $A[y]$ is contained in $A[x]$ and $A[x]$ is a finitely generated A-module, by 3, y is integral over A in $A[x]$ □

Corollary 7.1.10 (integral closure is idempotent)

Let $A \hookrightarrow B$ be a ring extension and C be the integral closure of A in B, then C is integrally closed in B.

Proof. Let $x \in B$ integral over C, then $C \to C[x]$ is also a integral ring extension. Hence $A \to C[x]$ is an integral ring extension. Hence, $x \in C[x]$ is integral over A, so $x \in C$. □

Proposition 7.1.11 (integral dependence under quotient and localization)

Let $A \hookrightarrow B$ be an integral ring extension

1. Let $\mathfrak{b} \subseteq B$ be an ideal, let $\mathfrak{a} = \mathfrak{b}^c = \mathfrak{b} \cap A$ be the contraction of $\mathfrak{b}$

$$A/\mathfrak{a} \hookrightarrow B/\mathfrak{b}$$

   is also an integral ring extension.

2. Let $S \subseteq A$ be an multiplicatively closed subset, then

$$S^{-1}A \hookrightarrow S^{-1}B$$

   is also an integral ring extension.

Proof.
(1) Let $\bar{b} \in B/\mathfrak{b}$, lift $b \in B$ satisfies

$$b^n + a_1 b^{n-1} + ... + a_n = 0$$

for some $a_1, ..., a_n \in A$, mod $\mathfrak{b}$ gives

$$\bar{b}^n + \bar{a}_1 \bar{b}^{n-1} + ... + \bar{a}_n = 0$$

(2) Let $x/s \in S^{-1}B$, for $x \in B$ and $s \in S$, then

$$x^n + a_1 x^{n-1} + ... + a_n = 0$$

Then,
$$\frac{x^n}{s^n} + \frac{a_1}{s}\frac{x^{n-1}}{s^{n-1}} + \frac{a_2}{s^2}\frac{x^{n-2}}{s^{n-2}} + ... + \frac{a_n}{s^n} = 0$$
in $S^{-1}B$. Hence, x/s is integral in $S^{-1}A$ □

7.2 THE LYING-OVER THEOREM THE GOING-UP THEOREM

Proposition 7.2.1

Let $A \hookrightarrow B$ be integral ring extension of domains, then A is a field if and only if B is a field. In this case, $A \hookrightarrow B$ is an algebraic extension.

Proof.

($\Longrightarrow$) If A is a field, let $x \in B$ be nonzero, let

$$x^n + a_1x^{n-1} + ... + a_{n-1}x + a_n = 0$$

for some $a_1, ..., a_n \in A$ be the polynomial of smallest degree that x satisfies. Since B is a domain, if $a_n = 0$, then $(x^{n-1} + a_1x^{n-2} + ... + a_{n-1})x = 0$, hence $x^{n-1} + a_1x^{n-2} + ... + a_{n-1} = 0$ contradicts the minimality of degree. Hence, $a_n \neq 0$. Then
$$y = -a_n^{-1}(x^{n-1} + a_1x^{n-2} + ... + a_{n-1}) \in B$$
is the inverse of x

($\Longleftarrow$) If B is a field, let $x \in A$ be nonzero, $x^{-1} \in B$ is integral over A, then

$$x^{-n} + a_1x^{-n+1} + ... + a_n = 0$$

for some $a_1, ..., a_n \in A$. Hence
$$x^{-1} = -(a_1 + a_2x + ... + a_nx^{n-1}) \in A$$

□

Corollary 7.2.2

Let $A \hookrightarrow B$ be integral ring extension, $\mathfrak{q}$ be a prime ideal of B and $\mathfrak{p} = \mathfrak{q}^c = \mathfrak{q} \cap A$ be the contraction of $\mathfrak{q}$. Then, $\mathfrak{q}$ is maximal if and only if $\mathfrak{p}$ is maximal.

Proof. $A/\mathfrak{p} \hookrightarrow B/\mathfrak{q}$ is a integral ring extension of domains.

$$\mathfrak{q} \text{ is maximal} \iff B/\mathfrak{q} \text{ is a field} \iff A/\mathfrak{p} \text{ is a field} \iff \mathfrak{p} \text{ is maximal}$$

□

Proposition 7.2.3 (lying over theorem: part 1)

Let $A \hookrightarrow B$ be a integral ring extension, given $\mathfrak{q}_1 \subseteq \mathfrak{q}_2$ prime ideals of B such that $\mathfrak{q}_1 \cap A = \mathfrak{q}_2 \cap A = \mathfrak{p}$, then $\mathfrak{q}_1 = \mathfrak{q}_2$

Proof. The integral ring extension $A \hookrightarrow B$ induces another integral ring extension $A_\mathfrak{p} \hookrightarrow B_\mathfrak{p}$

$$\begin{tikzcd} A \arrow[r, hook] \arrow[d] & B \arrow[d] \\ A_\mathfrak{p} \arrow[r, hook] & B_\mathfrak{p} \end{tikzcd}$$

Let $\mathfrak{m} = \mathfrak{p}A_\mathfrak{p}$, $\mathfrak{n}_1 = \mathfrak{q}_1 B_\mathfrak{p}$, and $\mathfrak{n}_2 = \mathfrak{q}_2 B_\mathfrak{p}$ Then, $\mathfrak{n}_1 \cap A_\mathfrak{p} = \mathfrak{n}_2 \cap A_\mathfrak{p} = \mathfrak{m}$. Since $A_\mathfrak{p} \to B_\mathfrak{p}$ is an integral ring extension, $\mathfrak{n}_1, \mathfrak{n}_2$ are maximal ideals. Since $\mathfrak{n}_1 \subseteq \mathfrak{n}_2$, $\mathfrak{n}_1 = \mathfrak{n}_2$. Hence, $\mathfrak{q}_1 = \mathfrak{q}_2$ $\square$

Theorem 7.2.4 (lying over theorem: main statement)

Let $A \hookrightarrow B$ be an integral ring extension, $\mathfrak{p} \subseteq A$ be a prime ideal, then there exists prime ideal $\mathfrak{q} \subseteq B$ so that $\mathfrak{q} \cap A = \mathfrak{p}$. In other words, the induced function

$$\operatorname{Spec} B \to \operatorname{Spec} A$$

is surjective

Proof. Given any prime ideal $\mathfrak{p} \subseteq A$, the integral ring extension $A \hookrightarrow B$ induces another integral ring extension $A_\mathfrak{p} \hookrightarrow B_\mathfrak{p}$

$$\begin{tikzcd} A \arrow[r, hook] \arrow[d] & B \arrow[d] \\ A_\mathfrak{p} \arrow[r, hook] & B_\mathfrak{p} \end{tikzcd}$$

Let $\mathfrak{n}$ be a maximal ideal in $B_\mathfrak{p}$, then $\mathfrak{n} \cap A_\mathfrak{p}$ is the unique maximal ideal in the local ring $A_\mathfrak{p}$, hence $\mathfrak{n} \cap A_\mathfrak{p} = \mathfrak{p}A_\mathfrak{p}$. Let $\mathfrak{q} = \mathfrak{n} \cap B$, $\mathfrak{q}$ is prime since it is a contraction of prime ideal. Moreover, $\mathfrak{q} \cap A = \mathfrak{p}$ since $(\mathfrak{n} \cap B) \cap A = (\mathfrak{n} \cap A_\mathfrak{p}) \cap A$, then the map $\operatorname{Spec} B \to \operatorname{Spec} A$ is surjective. $\square$

Theorem 7.2.5 (going-up theorem)

Let $A \hookrightarrow B$ be an integral ring extension. Let $\mathfrak{p}_\bullet$ be a chain of prime ideals in A and $\mathfrak{q}_\bullet$ be a chain of prime ideals in B

$$\begin{tikzcd} \operatorname{Spec} B \arrow[d, two heads] & \mathfrak{q}_1 \arrow[r, hook] \arrow[d] & \mathfrak{p}_2 \arrow[r, hook] \arrow[d] & \dots \arrow[r, hook] & \mathfrak{p}_m \arrow[d] & & \\ \operatorname{Spec} A & \mathfrak{p}_1 \arrow[r, hook] & \mathfrak{p}_2 \arrow[r, hook] & \dots \arrow[r, hook] & \mathfrak{p}_m \arrow[r, hook] & \dots \arrow[r, hook] & \mathfrak{p}_n \end{tikzcd}$$

so that $\mathfrak{q}_i \cap A = \mathfrak{p}$ for all $i = 1, 2, ..., m$. Then $\mathfrak{q}_\bullet$ is extended the the chain

$$\begin{tikzcd} \operatorname{Spec} B \arrow[d, two heads] & \mathfrak{q}_1 \arrow[r, hook] \arrow[d] & \mathfrak{p}_2 \arrow[r, hook] \arrow[d] & \dots \arrow[r, hook] & \mathfrak{p}_m \arrow[r, hook] \arrow[d] & \dots \arrow[r, hook] & \mathfrak{q}_n \arrow[d] \\ \operatorname{Spec} A & \mathfrak{p}_1 \arrow[r, hook] & \mathfrak{p}_2 \arrow[r, hook] & \dots \arrow[r, hook] & \mathfrak{p}_m \arrow[r, hook] & \dots \arrow[r, hook] & \mathfrak{p}_n \end{tikzcd}$$

so that $q_i \cap A = \mathfrak{p}_i$ for all $i = 1, ..., n$

Proof. The proof of the general case can be reduced to the case when $m = 1$, $n = 2$.

$$\begin{tikzcd} A \arrow[r, hook] \arrow[d] & B \arrow[d] \\ A/\mathfrak{p}_1 \arrow[r, hook] & B/\mathfrak{q}_1 \end{tikzcd}$$

Let $\bar{A} = A/\mathfrak{p}_1$ and $\bar{B} = B/\mathfrak{q}_1$, because $\mathfrak{p}_1 = \mathfrak{q}_1 \cap A$, then $\bar{A} \hookrightarrow \bar{B}$ is an integral ring extension extension. Let $\bar{\mathfrak{p}_2} = \mathfrak{p}_2/\mathfrak{p}_1 \subseteq \bar{A}$, then $\bar{\mathfrak{p}_2}$ is a prime ideal in $\bar{A}$. $\operatorname{Spec}\bar{B} \twoheadrightarrow \operatorname{Spec}\bar{A}$ is surjective, there exists a prime ideal $\bar{\mathfrak{q}} \subseteq \bar{B}$ so that $\bar{\mathfrak{q}} \cap \bar{A} = \bar{\mathfrak{p}}_2$. Take $\mathfrak{q} = \bar{\mathfrak{q}} \cap B$ □

Corollary 7.2.6
If $A \hookrightarrow B$ is an integral ring extension, then $\dim A \leq \dim B$

Proof. omitted □

7.3 INTEGRALLY CLOSED DOMAIN THE GOING-DOWN THEOREM

Proposition 7.3.1
Let $A \hookrightarrow B$ be a ring extension, let C be the integral closure of A in B, let $S \subseteq A$ be a multiplicative subset of A, then $S^{-1}C$ is the integral closure of $S^{-1}A$ in $S^{-1}B$

Proof. $A \hookrightarrow C$ is integral ring extension, then $S^{-1}A \hookrightarrow S^{-1}C$ is also an integral ring extension. For any $b/s \in S^{-1}B$ being integral over $S^{-1}A$, that is

$$\frac{b^n}{s^n} + \frac{a_1}{s_1}\frac{b^{n-1}}{s^{n-1}} + ... + \frac{a_n}{s_n} = 0$$

for some $a_1, ..., a_n \in A$ and $s_1, ..., s_n \in S$. Let $t = s_1...s_n$, multiply both sides by $s^n t^n$, we have

$$(bt)^n + \frac{a_1 st}{s_1}(bt)^{n-1} + ... + \frac{a_n s^n t^n}{s_n} = 0$$

Hence, bt is integral over A, that is $bt \in C$. Hence, $b/s = (bt)/(st) \in S^{-1}C$ □

Definition 7.3.2 (total field of fractions)
Let A be a domain, then

$$\operatorname{Frac}(A) = (A - \{0\})^{-1}A$$

is a field and it is called the total field of fractions of A

Definition 7.3.3 (integrally closed domain)
A domain A is called integrally closed if it is integrally closed in $\operatorname{Frac}(A)$

Theorem 7.3.4 (being integrally closed is a local property)
Let A be an domain, the following are equivalent

1. A is integrally closed
2. $A_{\mathfrak{p}}$ is integrally closed for all prime ideal $\mathfrak{p}$ in A
3. $A_{\mathfrak{m}}$ is integrally closed for all maxmal ideal $\mathfrak{m}$ in A

Proof. Let $K = \mathrm{Frac}(A)$ and C is the integral closure of A in K with $f : A \hookrightarrow C$ is an integral ring extension. Then A is integrally closed in C if and only if f is surjective if and only if $f_\mathfrak{p}$ is surjective for all prime ideal $\mathfrak{p}$. $f_\mathfrak{p}$ is surjective for all prime ideal $\mathfrak{p}$ if and only if $A_\mathfrak{p}$ is integrally closed for all prime ideal $\mathfrak{p}$. $f_\mathfrak{p}$ is surjective for all prime ideal $\mathfrak{p}$ if and only if $f_\mathfrak{m}$ is surjective for all maximal ideal $\mathfrak{m}$ if and only if $A_\mathfrak{m}$ is integrally closed for all maxmal ideal $\mathfrak{m}$ □

Definition 7.3.5 (normal domain)
A domain A is normal if $A_\mathfrak{p}$ is a integrally closed for every prime ideal $\mathfrak{p}$

Lemma 7.3.6
Let C be the integral closure of A in B and $\mathfrak{a}$ be an ideal in A, then the integral closure of $\mathfrak{a}$ in B is $\sqrt{\mathfrak{a}C}$

Proposition 7.3.7
Let $A \subseteq B$ be domains, A be integrally closed and $x \in B$ be integral over an ideal $\mathfrak{a}$ in A, then x is algebraic over $K = \mathrm{Frac}(A)$ and if its minimal polynomial over K is

$$t^n + a_1 t^{n-1} + ... + a_n$$

then $a_1, ..., a_n$ lie in $\sqrt{\mathfrak{a}}$ *wtf is this?*

Theorem 7.3.8 (going-down theorem)
Let $A \hookrightarrow B$ be integral ring extension of domains, A is integrally closed in $K = \mathrm{Frac}(A)$, let $\mathfrak{p}_\bullet$ be a chain of prime ideals in A and $\mathfrak{q}_\bullet$ be a chain of prime ideals in B

$$\begin{tikzcd}
\mathrm{Spec}\, B \arrow[d, two heads] & \mathfrak{q}_1 \arrow[d] & \mathfrak{p}_2 \arrow[l, hook'] \arrow[d] & ... \arrow[l, hook'] & \mathfrak{p}_m \arrow[l, hook'] \arrow[d] & & \\
\mathrm{Spec}\, A & \mathfrak{p}_1 & \mathfrak{p}_2 \arrow[l, hook'] & ... \arrow[l, hook'] & \mathfrak{p}_m \arrow[l, hook'] & ... \arrow[l, hook'] & \mathfrak{p}_n \arrow[l, hook']
\end{tikzcd}$$

so that $q_i \cap A = \mathfrak{p}_i$ for all $i = 1, ..., m$. Then $\mathfrak{q}_\bullet$ is extended to the chain

$$\begin{tikzcd}
\mathrm{Spec}\, B \arrow[d, two heads] & \mathfrak{q}_1 \arrow[d] & \mathfrak{p}_2 \arrow[l, hook'] \arrow[d] & ... \arrow[l, hook'] & \mathfrak{p}_m \arrow[l, hook'] \arrow[d] & ... \arrow[l, hook'] & \mathfrak{q}_n \arrow[l, hook'] \arrow[d] \\
\mathrm{Spec}\, A & \mathfrak{p}_1 & \mathfrak{p}_2 \arrow[l, hook'] & ... \arrow[l, hook'] & \mathfrak{p}_m \arrow[l, hook'] & ... \arrow[l, hook'] & \mathfrak{p}_n \arrow[l, hook']
\end{tikzcd}$$

so that $q_i \cap A = \mathfrak{p}_i$ for all $i = 1, ..., n$

Chapter 8

COMPLETION

Reference book: *Matsumura - Commutative Ring Theory*

8.1 LINEAR TOPOLOGY AND COMPLETION

Definition 8.1.1 (topological abelian group, linear topology)
An abelian group M is a topological abelian group if M is endowed with a topology so that the addition $M \times M \to M$ and inverse $M \to M$ are continuous. The topology on M is called linear topology

Remark 8.1.2 (fundamental system of open neighbourhoods of 0)
For any element $a \in M$, addition by a is a homeomorphism $M \to M$. Hence, U is a neighbourhood of 0 if and only if $a + U$ is a neighbourhood of a, that is the collection of neighbours around 0 generates the whole topology. We will restrict ourselves to the special kind of topologies occuring in commutative algebra, namely, assume that $0 \in G$ has a fundamental system of open neighbourhoods consisting of subgroups of M.

Definition 8.1.3 (linear topology on module and ring)
Let M be an A-module, given a collection $\mathcal{M} = \{M_\lambda\}_{\lambda \in \Lambda}$ of submodules of M. $\mathcal{M}$ generates a linear topology on M with basis

$$\{x + M_\lambda : x \in M, \lambda \in \Lambda\}$$

Under this topology, addition and A-action by any element $a \in A$ are continuous

$$\begin{aligned} M \times M &\xrightarrow{+} M \\ (x, y) &\mapsto x + y \end{aligned} \qquad\qquad \begin{aligned} a : M &\xrightarrow{\times} M \\ x &\mapsto ax \end{aligned}$$

M is said to be linearly topologized by $\mathcal{M}$. When $M = A$, then ring multiplication is also continuous, M is said to be a topological ring.

Definition 8.1.4 (separated module)
The separated module associated with M is defined by

$$M^{sep} = M / \bigcap_{\mu \in \Lambda} M_\mu$$

The separated module M^{sep} inherits the quotient topology under the map $M \to M^{sep}$, then it is Hausdorff. If $M = M^{sep}$ or equivalently $\bigcap_{\mu \in \Lambda} M_\mu = 0$, then M is called separated (or Hausdorff)

Remark 8.1.5 (quotient space M/M_λ has discrete topology)
M_λ is both open and closed, the quotient space M/M_λ inherits the discrete topology.

Remark 8.1.6 (directed set)
In this chapter, we will assume that the collection $\mathcal{M} = \{M_\lambda\}_{\lambda \in \Lambda}$ is a directed set. That is, $\mathcal{M}$ is a partially ordered set by inclusion and given any two submodules $M_\lambda, M_\mu \in \mathcal{M}$, there exists a submodule $M_\nu \in \mathcal{M}$ that is contained with both M_λ and M_μ. With Λ being a directed set, one can define the inverse limit $\hat{M} = \varprojlim_{\lambda \in \Lambda} M/M_\lambda$.

Definition 8.1.7 (completion, complete)
Let $\hat{M} = \varprojlim_{\lambda \in \Lambda} M/M_\lambda$ be the completion of M. For any $\nu \geq \mu$ (that is, $M_\nu \subseteq M_\mu$), there is a canonical map

$$\begin{aligned} \phi_{\mu\nu} : M/M_\nu &\twoheadrightarrow M/M_\mu \\ x + M_\nu &\mapsto x + M_\mu \end{aligned}$$

with the property that $\phi_{\lambda\mu}\phi_{\mu\nu} = \phi_{\lambda\nu}$ for all $\lambda \leq \mu \leq \nu$. The limit exists and can be characterized as a submodule of $\prod_{\lambda \in \Lambda} M/M_\lambda$

$$\hat{M} = \left\{ (x_\lambda)_{\lambda \in \Lambda} \in \prod_{\lambda \in \Lambda} M/M_\lambda : \forall \mu \leq \nu, \phi_{\mu\nu}(x_\nu) = x_\mu \right\} \subseteq \prod_{\lambda \in \Lambda} M/M_\lambda$$

The completion $\hat{M}$ inherits the subspace topology from $\prod_{\lambda \in \Lambda} M/M_\lambda$. M is said to be complete if $\hat{M} = M$

Remark 8.1.8 (completion)
In category theory words, $\hat{M}$ together with $\left\{ p_\nu : \hat{M} \to M/M_\nu \text{ defined by } (x_\lambda)_{\lambda \in \Lambda} \mapsto x_\nu \right\}_{\nu \in \Lambda}$ is the limit of the diagram consists of maps $\{\phi_{\mu\nu}\}$

$$\begin{tikzcd}
& N \arrow[d, dashed] \arrow[ddl] \arrow[ddr] & \\
& \hat{M} \arrow[dl, "p_\nu"'] \arrow[dr, "p_\mu"] & \\
M/M_\nu \arrow[rr, two heads, "\phi_{\mu\nu}"'] & & M/M_\mu
\end{tikzcd}$$

In other words, any module N together with maps $\{N \to M/M_\nu\}_{\nu \in \Lambda}$ factor uniquely through $\hat{M}$.

Remark 8.1.9

The projection map $M \twoheadrightarrow M/M_\lambda$ factors through $\hat{M}$ by the map $\psi : M \to \hat{M}$. Each $M \to M/M_\lambda$ is surjective, then each p_λ is also surjective.

$$\begin{tikzcd} M \arrow[r, "\psi"] \arrow[dr, two heads] & \hat{M} \arrow[d, two heads, "p_\lambda"] \\ & M/M_\lambda \end{tikzcd}$$

We also have $\ker\psi = \bigcap_{\lambda\in\Lambda} M_\lambda = \ker(M \to M^{sep})$ and $\operatorname{im}\psi$ is dense in $\hat{M}$

Proof. TODO - if have time □

Proposition 8.1.10

Given M topologized by $\{M_\lambda\}_{\lambda\in\Lambda}$

1. $\hat{M}$ is linearly topologized by the collection of submodules $\{\ker p_\lambda\}_{\lambda\in\Lambda}$
2. $\ker p_\lambda$ is the closure of $\psi(M_\lambda)$ in $\hat{M}$
3. $\hat{M}$ is complete in the sense that $\hat{\hat{M}} \cong \hat{M}$ where $\hat{\hat{M}}$ is the completion of $\hat{M}$ over the collection of submodules $\{\ker p_\lambda\}_{\lambda\in\Lambda}$ (in Bourbaki terms, complete and separated)

Proof.

- ($\hat{M}$ is linearly topologized by the collection of submodules $\{\ker p_\lambda\}_{\lambda\in\Lambda}$)

  We will show that the linear topology generated by $\{\ker p_\lambda\}_{\lambda\in\Lambda}$ on $\hat{M}$ is precisely the (linear) subspace topology on $\hat{M}$ by $\hat{M} \hookrightarrow \prod_{\lambda\in\Lambda} M/M_\lambda$. Let $U_I \subseteq \hat{M}$ for some finite subset $I \subseteq \Lambda$ be any basic open set around 0, then U_I is of the form

  $$U_I = \hat{M} \cap \left(\prod_{\mu\in I} \{0\} \times \prod_{\lambda\in\Lambda - I} M/M_\lambda \right)$$

  Observe that if $\nu \geq \mu$ (that is $M_\nu \subseteq M_\mu$) for all $\mu \in I$, then $\ker p_\nu \subseteq U_I$ due to the commutativity of the diagram below

  $$\begin{tikzcd} & \hat{M} \arrow[d, hook] \arrow[ddl, "p_\nu"'] \arrow[ddr, "p_\mu"] & \\ & \prod_{\lambda\in\Lambda} M/M_\lambda \arrow[dl, two heads] \arrow[dr, two heads] & \\ M/M_\nu \arrow[rr, "\phi_{\mu\nu}"'] & & M/M_\mu \end{tikzcd}$$

  Hence, the topology generated by $\{\ker p_\lambda\}_{\lambda\in\Lambda}$ is finer than the subspace topology on $\hat{M}$. On the other hand, $U_I \subseteq \ker p_\mu$ for any $\mu \in I$. Hence, $\hat{M}$ is linearly topologized by $\{\ker p_\lambda\}_{\lambda\in\Lambda}$

- ($\ker p_\lambda \subseteq \overline{\psi(M_\lambda)}$)

  For any $x = (x_\tau)_{\tau\in\Lambda} \in \ker p_\lambda$, $x_\lambda = 0$. Since $\hat{M}$ is linearly topologized by $\{\ker p_\nu\}_{\nu\in\Lambda}$, then we need to show that $x + \ker p_\nu$ intersects $\psi(M_\lambda)$ for all $\nu \in \Lambda$. Since Λ is directed, let $\mu \geq \nu$ and $\mu \geq \lambda$, then

$$
\begin{tikzcd}
M \arrow[rr, "\psi"] \arrow[drr, two heads] & & \hat{M} \arrow[dl, "p_\nu"'] \arrow[d, "p_\mu"] \arrow[dr, "p_\lambda"] & \\
& M/M_\nu & M/M_\mu \arrow[l, "\phi_{\nu\lambda}"] \arrow[r, "\phi_{\lambda\mu}"'] & M/M_\lambda
\end{tikzcd}
$$

p_μ sends $x + \ker p_\mu$ into $\{x_\mu\}$, let $y_\mu \in M$ be the lift of x_μ under the quotient map $M \twoheadrightarrow M/M_\mu$. Then $\psi(y_\mu) - x \in \ker p_\mu$. Hence, $\psi(y_\mu) \in x + \ker p_\mu$. Because $\ker p_\mu \subseteq \ker p_\lambda$ and $x \in \ker p_\lambda$, then $\psi(y_\mu) \in \ker p_\lambda$, that is, y_μ is sent to $0 \in M/M_\lambda$, hence $y_\mu \in M_\lambda$. So, $y_\mu \in (x + \ker p_\mu) \cap \psi(M_\lambda)$. Because $\ker p_\mu \subseteq \ker p_\nu$, so $y_\mu \in (x + \ker p_\nu) \cap \psi(M_\lambda)$

- ($\ker p_\lambda = \overline{\psi(M_\lambda)}$)

  $\ker p_\lambda$ is the preimage of the closed set $\{0\} \subseteq M/M_\lambda$, hence $\ker p_\lambda$ is closed. $\psi(M_\lambda) \subseteq \ker p_\lambda \subseteq \overline{\psi(M_\lambda)}$ implies $\ker p_\lambda = \overline{\psi(M_\lambda)}$

- (completeness of completion)

  Note that, the surjectivity of p_λ gives that

$$
\frac{\hat{M}}{\ker p_\lambda} \cong M/M_\lambda
$$

  Thus, the completion $\hat{\hat{M}}$ of $\hat{M}$ linearly topologized by $\{\ker p_\lambda\}_{\lambda \in \Lambda}$ is

$$
\hat{\hat{M}} = \lim \frac{\hat{M}}{\ker p_\lambda} = \lim \frac{M}{M_\lambda} = \hat{M}
$$

□

Remark 8.1.11 (cofinal directed sets)
Different set of submodules can generate the same topology on M. In fact, $\{M_\lambda\}_{\lambda \in \Lambda}$ and $\{M_\xi\}_{\xi \in \Xi}$ generate the same topology if and only if for all $\lambda \in \Lambda$, there exists $\xi \in \Xi$ so that $M_\lambda \supseteq M_\xi$ and for all $\xi \in \Xi$, there exists $\lambda \in \Lambda$ so that $M_\xi \supseteq M_\lambda$ (Λ and Ξ are said to be cofinal)

Proposition 8.1.12
Given M topologized by $\{M_\lambda\}_{\lambda \in \Lambda}$, let N be a submodule of M, observe that the closure of N in M is

$$
\bar{N} = \bigcap_{\lambda \in \Lambda} N + M_\lambda
$$

Proof.

$$
x \in \bar{N} \iff (x + M_\lambda) \cap N \neq \varnothing \text{ for every } \lambda \in \Lambda \iff x \in \bigcap_{\lambda \in \Lambda} N + M_\lambda
$$

□

Proposition 8.1.13
Given M topologized by $\{M_\lambda\}_{\lambda \in \Lambda}$, let N be a submodule of M, let

$$
M'_\lambda = \operatorname{im}(M_\lambda \hookrightarrow M \twoheadrightarrow M/N) = M_\lambda/N
$$

then the quotient topology on M/N is the linear topology induced by $\{M'_\lambda\}_{\lambda \in \Lambda}$

Proof. For any subset $U \subseteq M$

1. $U \subseteq M/N$ is open in M/N with the quotient topology
2. U is open in M
3. for every $x \in U$, there exists $\lambda \in \Lambda$, $x + M_\lambda \subseteq U$
4. for every $y \in U \subseteq M/N$, there exists $\lambda \in \Lambda$, $y + M'_\lambda \subseteq U \subseteq M/N$
5. U is open in M/N with the linear topology

$1 \iff 2 \iff 3 \iff 4 \iff 5$ □

Remark 8.1.14
Some remarks

1. M/N is separated $\iff$ $N \subseteq M$ is a closed set
2. subspace topology on N is the linear topology generated by $\{N \cap M_\lambda\}_{\lambda \in \Lambda}$
3. the sequence
$$0 \to \frac{N}{N \cap M_\lambda} \to \frac{M}{M_\lambda} \to \frac{M/N}{\ker p_\lambda} = \frac{M}{N + M_\lambda} \to 0$$
is exact and compatible with λ
4. the sequence
$$0 \to \hat{N} \to \hat{M} \to \widehat{M/N} \to 0$$
is exact

8.2 I-ADIC COMPLETION

the ring of 10-adic integers is defined as a set of formal sums

$$\mathbb{Z}_{10} = \left\{ \pm \sum_{i=0}^{\infty} a_i 10^i : a_i \in \{0,1,2,3,4,5,6,7,8,9\} \right\}$$

where there is a natural inclusion $\mathbb{Z} \hookrightarrow \mathbb{Z}_{10}$ by writing a natural number in base 10. One also write an element of $\mathbb{Z}_{10}$ by $...a_3a_2a_1a_0$. I-adic completition is a generalization of 10-adic integers

Definition 8.2.1 (I-adic topology, I-adic completion, I-adically complete)
Let M be an A-module and I be an ideal of A, then the direct set $\{M, IM, I^2M, ...\}$ linearly topologizes M. The linear topology on M is called I-adic topology. The completion $\hat{M} = \varprojlim_n M/I^nM$ is called I-adic completion. If $\hat{M} = M$ then M is called I-adically complete.

Remark 8.2.2 (I-adic completion functor)
Let an A-module M be equipped with the I-adic toplogy, then $\hat{M}$ is naturally a $\hat{A}$-module. More generally, I-adic completion is a functor from A-module into $\hat{A}$-module.

Remark 8.2.3 (Cauchy sequence)
A sequence $x_1, x_2, ... \in M$ is called Cauchy if for any $r \geq 0$, there exists $N \geq 0$ so that for every $m, n \geq N$

$$x_m - x_n \in I^r M$$

Informally, elements of the sequence become arbitrary "close" to each other as the sequence progresses where the notion of closeness is defined by the I-adic topology. Endow $\mathbb{Z}$ with the 10-adic topology, then the sequence

$$1, 11, 111, 1111, ...$$

does not converge in $\mathbb{Z}$ but converges into $\sum_{i=0}^{\infty} 10^i \in \mathbb{Z}_{10}$

Remark 8.2.4 (p-adic integers)
Why completion? get more units and ring becomes simpler. Let $A = \mathbb{Z}$, $I = (p)$ for some integer p (p is often prime), then

$$\mathbb{Z}_p = \hat{A} = \left\{ (a_n)_{n\geq 1} \in \prod_{n\geq 1} \mathbb{Z}/(p^n) : a_n \mod p^m = a_m \text{ for all } m \leq n \right\}$$

$1 + p$ is not a unit in $\mathbb{Z}$ but a unit in $\mathbb{Z}_p$. Let $a = (a_n)_{n\geq 1} \in \mathbb{Z}_p$ so that

$$a_n = 1 - p + p^2 - ... \pm p^{n-1}$$

then $(1+p)a = 1$ in $\mathbb{Z}_p$. $\mathbb{Z}_p$ is called p-adic integers

Proposition 8.2.5
If $\Lambda = \mathbb{Z}_{\geq 1}$, then the map $\hat{M} \to \widehat{M/N}$ is surjective, that is

$$\hat{M}/\hat{N} \cong \widehat{M/N}$$

Proof. *TODO - approximation argument* □

8.3 MORE I-ADIC COMPLETION

Proposition 8.3.1
Let I be an ideal in a ring A and M be an A-module

1. If A is I-adically complete, then $I \subseteq J(A)$ is in the Jacobson radical
2. If M is I-adically complete, then multiplication by $1 + a$ is an isomorphism on M

Proof.
(1) for $a \in I$, $(1+a)(1 - a + a^2 - a^3 + ...) = 1$. Note that $1, 1-a, 1-a+a^2, ...$ is a Cauchy sequence
(2) $M = \hat{M}$ is an $\hat{A}$-module, for $a \in I$, $1 + a \in \hat{A}$ is a unit in $\hat{A}$. Hence, multiplication by $1 + a$ in M is an automorphism □

Definition 8.3.2 (complete local ring)
If $(A, \mathfrak{m})$ is a local ring such that A is $\mathfrak{m}$-adically complete, then A is called complete local ring

Remark 8.3.3
Some examples of complete local ring

$$\mathbb{Z}_p, k[[x]], k[[x_1, ..., x_n]]$$

for some field k

Remark 8.3.4
For any local ring $(A, \mathfrak{m})$, then $(\hat{A}, \mathfrak{m}\hat{A})$ is a complete local ring

Theorem 8.3.5 (Hensel lemma)
Suppose $(A, \mathfrak{m}, k)$ is a complete local ring. Let $F \in A[X]$ be a monic polynomial. Suppose that there is a factorization $\bar{F} = gh$ in $k[X]$ for some coprime monic polynomials $g, h \in k[X]$. Then there exist lifts $\tilde{g}, \tilde{h} \in A[X]$ so that $F = \tilde{g}\tilde{h}$

Proof. *TODO - approximation argument* □

Remark 8.3.6
Let $A = \mathbb{Z}_5$, $f = x^2 + 1$, then $k = \mathbb{F}_5$ and $\bar{f} = x^2 + 1 = x^2 - 4 = (x+2)(x-2) \in \mathbb{F}_5[x]$, by Hensel lemma, $f = l_1 l_2$ in $\mathbb{Z}_5[x]$, that is $\sqrt{-1} \in \mathbb{Z}_5$

Theorem 8.3.7
Let M be an A-module and I be an ideal of A, assume A is I-adically complete and M is I-adically separated, that is $\bigcap_{n \geq 1} I^n M = \{0\}$. If $\bar{w}_1, \bar{w}_2, ..., \bar{w}_n \in M/IM$ generate M/IM as an A/I-module, then any lifts $w_1, w_2, ..., w_n \in M$ generate M as an A-module.

Proof. Pick $w_1, ..., w_n$, since $\{\bar{w}_1, ..., \bar{w}_n\}$ generates M/IM as an A/I-module, then

$$M = \sum Aw_i + IM$$

Then,

$$IM = I\left(\sum Aw_i + IM\right) = \sum IAw_i + I^2 M$$

Keep iterating, for any $r \geq 1$, we have

$$I^r M = \sum_{i=1}^{n} I^r Aw_i + I^{r+1} M$$

Now, fix any $\xi \in M$, we can write

$$\begin{aligned}
\xi &= \sum a_i w_i + \xi_1 && \text{(for some } \xi_1 \in IM \text{ and for some } a_i \in A) \\
\xi_1 &= \sum a_{i1} w_i + \xi_2 && \text{(for some } \xi_2 \in I^2M \text{ and for some } a_{i1} \in IA) \\
\xi_2 &= \sum a_{i2} w_i + \xi_3 && \text{(for some } \xi_3 \in I^3M \text{ and for some } a_{i2} \in I^2A) \\
&\dots
\end{aligned}$$

Then, for any $n \geq 1$,

$$\xi = \sum (a_i + a_{i1} + \dots + a_{in}) w_i + \xi_{n+1}$$

Since A is I-adically complete, let $b_i = a_i + a_{i1} + a_{i2} + \dots \in A$. Then,

$$\xi - \sum b_i w_i \in \bigcap_{n \geq 1} I^n M = \{0\}$$

□

Remark 8.3.8

Let M be equipped with a linear topology by $\{M_\lambda\}_{\lambda \in \Lambda}$, if $N \subseteq M$ is a submodule, the subspace topology on N is not the linear topology by $\{M_\lambda \cap N\}_{\lambda \in \Lambda}$

Even in I-adic topology. Given ideal $I \subseteq A$ and an submodule $N \subseteq M$, the I-adic topology on N might not be the subspace topology on N relative to the I-adic topology on M

Let $A = \mathbb{Z}$, $I = (p)$ for some prime p. $N = \mathbb{Z}$, $M = \mathbb{Q}$, then

$$I^n M = \mathbb{Q}, I^n N = p^n \mathbb{Z}$$

Theorem 8.3.9 (Artin-Rees lemma)

Let A be a Noetherian ring and ideal I in A, let M be a finitely generated A-module and N be a submodule of M, then there exists $c > 0$ such that for all $n \geq c$

$$I^n M \cap N = I^{n-c}(I^c M \cap N)$$

Proof.

($\supseteq$) obvious

($\subseteq$) A is Notherian, let $I = (a_1, \dots, a_r)$ and $M = \sum A w_i$. Any element in $I^n M$ can be written as

$$\sum_{1 \leq i \leq s} f_i(\vec{a}) w_i$$

where $\vec{a} = (a_1, \dots, a_r) \in A^r$, $f_i \in B = A[X_1, \dots, X_r]$ is a homogeneous polynomial (all terms have the same degree) of degree n. For each $n \geq 1$, let J_n be the set of s-tuple of homogeneous polynomials of degree n in B so that $\sum_{1 \leq i \leq s} f_i(\vec{a}) w_i \in N$

$$J_n = \left\{ (f_1, \dots, f_s) \in B^s : f_i \text{ is homogeneous of degree } n \text{ and } \sum_{1 \leq i \leq s} f_i(\vec{a}) w_i \in N \right\} \subseteq B^s$$

Then, B^s is an A-module and J_n is a submodule of B^s. Let ring C be the B-module generated by $\bigcup_{n \geq 1} J_n \subseteq B^s$. A

being Noetherian implies B being Noetherian implies C being Noetherian. Write

$$C = \sum_{1\leq j\leq t} Bv_j$$

where $v_j \in B^s$ is a B-linear combination of elements in $\{J_n\}_{n\geq 1}$. Without loss of generality, assume each v_j lies in one of $\{J_n\}_{n\geq 1}$, then

$$v_j = (v_{j1}, ..., v_{js}) \in J_{d_j}$$

for some $d_j \geq 1$. Note that, each $v_{ji} \in B$ is a homogeneous polynomial of degree d_j . Let $c = \max\{d_j\}_{1\leq j\leq t}$. Now, for any $\eta = \sum_{1\leq i\leq s} f_i(\vec{a})w_i \in I^n M \cap N$ with $(f_1, ..., f_s) \in J_n \subseteq C$. Since $C = \sum_{1\leq j\leq t} Bv_j$, then

$$(f_1, ..., f_s) = \sum_{1\leq j\leq t} p_j(x)v_j$$

for some $p_j(x) \in B = A[x_1, ..., x_r]$. Since $v_j = (v_{j1}, ..., v_{js}) \in J_{d_j}$, each $v_{ji} \in B = A[x_1, ..., x_r]$ is a homogeneous polynomial of degree d_j. Each $f_i \in B = A[x_1, ..., x_r]$ is a homogeneous polynomial of degree n. Hence, we can choose $p_j(x)$ so that each $p_j(x)$ is a homogeneous polynomial of degree $n - d_j$, then

$$\begin{aligned}\eta &= \sum_{1\leq i\leq s} f_i(\vec{a})w_i \\ &= \sum_{1\leq i\leq s} w_i \sum_{1\leq j\leq t} p_j(\vec{a})v_{ji}(\vec{a}) \\ &= \sum_{1\leq j\leq t} p_j(\vec{a}) \sum_{1\leq i\leq s} v_{ji}(\vec{a})w_i \in I^n M \cap N\end{aligned}$$

Note that, $\sum_{1\leq i\leq s} v_{ji}(\vec{a})w_i \in N$ by definition of J_{d_j} and $\sum_{1\leq i\leq s} v_{ji}(\vec{a})w_i \in I^{d_j}M$, moreover, $p_j(\vec{a}) \in I^{n-d_j} = I^{n-c}I^{c-d_j}$. Hence,

$$p_j(\vec{a}) \sum_{1\leq i\leq s} v_{ji}(\vec{a})w_i \in I^{n-c}I^{c-d_j}(I^{d_j}M \cap N) \subseteq I^{n-c}(I^c M \cap N)$$

so $\eta \in I^{n-c}(I^c M \cap N)$ *this proof is disgustingly genius >_<* □

Corollary 8.3.10

Let A be a Noetherian ring and ideal I in A, let M be a A-module

1. If M is finitely generated, then for any short exact sequence $0 \to N \to M \to Q \to 0$, the induced sequence $0 \to \hat{N} \to \hat{M} \to \hat{Q} \to 0$ is exact
2. If M is finitely presented, then the natural map $M \otimes_A \hat{A} \to \hat{M}$ is an isomorphism

Proposition 8.3.11

An A-module M is flat if and only if for every ideal $I \subseteq A$, the natural map $I \otimes_A M \to M$ is injective

Proof. *TODO - black box - will be proved after homological algebra* □

Theorem 8.3.12

Let A be a Noetherian ring and ideal I in A, then I-adic completion $\hat{A}$ is a flat A-module

Proof. the composition is injective for any ideal $I \subseteq A$

$$\hat{I} \xrightarrow{\sim} I \otimes_A A \to \hat{A}$$

□

Theorem 8.3.13

Let A be a Noetherian ring and ideal I in A, let M be a finitely generated A-module and N be a submodule of M. If M is equipped with I-adic topology, the I-adic topology on N coincides with the subspace topology of $N \hookrightarrow M$ where

Proof. TODO □

Theorem 8.3.14

Let A be a Noetherian ring, I be an ideal of A, and M be a finitely generated A-module, then

$$M \otimes_A \hat{A} \cong \hat{M}$$

Hence, if A is I-adically complete, so is M

Theorem 8.3.15 (Krull)

Let A be a Noetherian ring, I be an ideal of A, and M be a finitely generated A-module, let $N = \bigcap_{n \geq 1} I^n M$. Then, there exists $a \in A$ so that $a = 1 \mod I$ and $aN = 0$

Proof. By Nakayama, it is enough to show that $N = IN$. By Artin-Rees, $N = I^n M \cap N \subseteq IN$ for sufficiently large n. Hence, $N = IN$ □

Theorem 8.3.16 (Krull intersection theorem)

The theorem consists of two parts

1. Let A be a Noetherian ring and I be an ideal of A with $I \subseteq J(A)$, then for any finitely generated A-module M, the I-adic topology is separated and any submodule is a closed set.
2. If A is a Noetherian domain and $I \subsetneq A$ is a proper ideal, then

$$\bigcap_{n \geq 1} I^n = 0$$

Proof.

(1) using the notation in Krull theorem, there exists $a \in A$ so that $a = 1 + x$ for some $x \in J(A)$, so a is a unit in A. Since, $aN = 0$, then $N = 0$, hence M is separated. If $L \subseteq M$ is a submodule, M/L is also I-adically separated, hence L is closed in M

(2) using the notation in Krull theorem, let $M = A$. $1 \notin I$, so $a \neq 0$, so a is not a zero-divisor, hence $aN = 0$ implies $N = 0$ □

Remark 8.3.17

In particular, if $(A, \mathfrak{m}, k)$ is a Noetherian local ring, then $\mathfrak{m}$-adic topology on A is separated, that is, $\bigcap_{n\geq 1} \mathfrak{m}^n = (0)$

Remark 8.3.18 (Matsumura CRT p63 - some results from local Noetherian ring)

Let $(A, \mathfrak{m})$ be a local Noetherian ring, then

1. $\bigcap_{n\geq 1} \mathfrak{m}^n = \ker(\psi : A \to \hat{A}) = 0$
2. For M a finitely generated A-module and $N \subseteq M$ a submodule
$$\bigcap_{n\geq 1} (N + \mathfrak{m}^n M) = N$$
3. The completion $\hat{A}$ of A is faithfully flat over A; hence $A \subseteq \hat{A}$ and $I\hat{A} \cap A = I$ for any ideal I of A
4. $\hat{A}$ is again a Noetherian local ring, with maximal ideal $\mathfrak{m}A$ and it has the same residue class field as A; moreover, $\hat{A}/\mathfrak{m}^n\hat{A} = A/\mathfrak{m}^n$ for all $n \geq 1$
5. If A is a complete local ring, the for any ideal $I \neq A$, A/I is afgain a complete local ring.

Theorem 8.3.19 (Cohen structure theorem)

Let $(A, \mathfrak{m})$ be any complete local ring, then

$$A \cong \frac{R[[x_1, x_2, ..., x_n]]}{I}$$

where n can be given explicitly and R is either a field (dimension 0) or discrete valuation ring (dimension 1)

Chapter 9

SOME OTHER CLASSES OF RINGS

9.1 ARTINIAN RING

Definition 9.1.1 (Artinian ring)
A ring is Artinian if it satisfies the decending chain condition (DDC): any decending chain of ideals

$$I_1 \supseteq I_2 \supseteq \dots$$

must stablize, that is, $I_n = I_{n+1}$ for large n

Remark 9.1.2
Some examples and non-examples

1. Let k be a field, $k[x,y]/(x^3, xy, y^3)$ is Artinian because it is of finite dimension
2. For any nonzero integer n, $\mathbb{Z}/n\mathbb{Z}$ is Artinian
3. $\mathbb{Z}$ is not Artinian
4. If A is Artinian and I is an ideal of A, then A/I is Artinian

Proposition 9.1.3
If A is a domain and Artinian, then A is a field

Proof. We will construct the inverse of any nonzero element $x \in A$. We have the decending chain

$$(x) \supseteq (x^2) \supseteq \dots$$

Hence, by DCC, $(x^n) = (x^{n+1})$ for some $n > 0$. $x^n \in (x^{n+1})$ implies $x^n = x^{n+1}y$ for some $y \in A$. Since A is a domain, left cancellation works, $1 = xy$ □

Corollary 9.1.4
Every prime ideal in an Artinian ring is maximal

Proof. Let $\mathfrak{p}$ be a prime ideal in Artinian ring A, then $A/\mathfrak{p}$ is also Artinian. Since $A/\mathfrak{p}$ is a domain, then it is also a field. Hence $\mathfrak{p}$ is maximal. $\square$

Proposition 9.1.5

Aritinian ring has only finitely many maximal ideals

Proof. Let $\mathfrak{m}_1, \mathfrak{m}_2, ...$ be maximal ideals of an Artinian ring A, then

$$\mathfrak{m}_1 \supseteq \mathfrak{m}_1\mathfrak{m}_2 \supseteq ...$$

is a decending chain. Since each pair of maximal ideals are coprime (or comaximal), by CRT,

$$\frac{A}{\mathfrak{m}_1...\mathfrak{m}_n} \cong \frac{A}{\mathfrak{m}_1} \times ... \times \frac{A}{\mathfrak{m}_n}$$

Note that, the RHS admits precisely n prime ideals of the form

$$\frac{A}{\mathfrak{m}_1} \times ... \times \frac{A}{\mathfrak{m}_{i-1}} \times \{0\} \times \frac{A}{\mathfrak{m}_{i+1}} \times ... \times \frac{A}{\mathfrak{m}_n}$$

Hence, $\frac{A}{\mathfrak{m}_1...\mathfrak{m}_n} \neq \frac{A}{\mathfrak{m}_1...\mathfrak{m}_{n+1}}$. That is, the decending chain consists of all strict inclusions. By DDC, the chain stablizes. Hence, A has finitely many maximal ideals. $\square$

Corollary 9.1.6

The nilradical and Jacobson radical of an Artinian ring is of the form

$$\eta_A = J(A) = \bigcap_{1 \leq i \leq n} \mathfrak{m}_i = \mathfrak{m}_1...\mathfrak{m}_n$$

where the last inequality is due to maximal ideals being comaximal

Proposition 9.1.7

If A is Artinian, then $\eta_A^k = 0$ for some large k. In other words, let $\mathfrak{m}_1, ..., \mathfrak{m}_n$ be the maximal ideals of an Artinian ring A, then $\mathfrak{m}_1^k...\mathfrak{m}_n^k = 0$ for large k

Proof. By DDC,

$$\eta_A \supseteq \eta_A^2 \supseteq ...$$

must stablize to some ideal $\mathfrak{a}$. We will show that $\mathfrak{a} = (0)$. Suppse $\mathfrak{a} \neq 0$, observe that $\mathfrak{a}^2 = (\eta_A^k)^2 = \eta_A^{2k} = \eta_A^k = \mathfrak{a}$. Let

$$\Sigma = \{\mathfrak{b} \subseteq A : \mathfrak{b} \text{ is ideal and } \mathfrak{b}\mathfrak{a} \neq 0\}$$

then $\Sigma \neq 0$ since $A \in \Sigma$. Due to Zorn lemma and DCC, let $\mathfrak{c}$ be a minimal element in Σ, pick $x \in \mathfrak{c}$ so that $x\mathfrak{a} \neq 0$. Since

$$(x\mathfrak{a})\mathfrak{a} = x(\mathfrak{a}\mathfrak{a}) = x\mathfrak{a} \neq 0$$

then $(x) \in \Sigma$, but $(x) \subseteq \mathfrak{c}$. By minimality of $\mathfrak{c} = (x)$. Moreover, $x\mathfrak{a} \in \Sigma$, then $\mathfrak{c} = (x) = x\mathfrak{a}$. Now, $x \in (x) = x\mathfrak{a}$, then $x = xy$ for some $y \in \mathfrak{a} \subseteq \eta_A$. Replace x by xy, we have $x = xy = xy^2 = xy^3 = ...$ Since $y \in \eta_A$, we have $x = xy^n = 0$ for some n. This contradicts with $x\mathfrak{a} \neq 0$ $\square$

Corollary 9.1.8
Let A be an Aritinian ring, then

$$A \cong A_1 \times \ldots \times A_l$$

where each A_i is Artinian and local

Proof.

$$A = \frac{A}{(0)} = \frac{A}{\mathfrak{m}_1^k, \ldots, \mathfrak{m}_l^k}$$

since $\mathfrak{m}_i^k$ and $\mathfrak{m}_j^k$ are comaximal for $i \neq j$ (*TODO - exercise*), then by CRT

$$A = \frac{A}{\mathfrak{m}_1^k} \times \ldots \times \frac{A}{\mathfrak{m}_l^k}$$

If $\mathfrak{n}$ is a maximal ideal in $A/\mathfrak{m}_i^k$, then it is maximal in A and $\mathfrak{n} \supseteq \mathfrak{m}_i^k$, then $\mathfrak{n} \supseteq \mathfrak{m}_i$, hence $\mathfrak{n} = \mathfrak{m}_i$. That is, each $A/\mathfrak{m}_i^k$ is local. Moreover, quotient of Artinian ring is Artinian. $\square$

9.2 LENGTH AND ARTINIAN RING

Definition 9.2.1 (length)
Define the length of an A-module M by

$$l_A(M) = \sup\{n \in \mathbb{N} : \text{ there exists a chain of submodules } M = M_n \supsetneq M_{n-1} \supsetneq \ldots \supsetneq M_0 = \{0\}\}$$

Remark 9.2.2
A ring A is Artinian if and only if $l_A(A) < \infty$

Remark 9.2.3
Some examples

1. $l_{\mathbb{Z}}(\mathbb{Z}) = \infty$
2. $l_{\mathbb{Z}}(\mathbb{Z}/6) = 2$ since the only chains in $\mathbb{Z}/6$ are $\mathbb{Z}/6 \supsetneq 3\mathbb{Z}/6 \supsetneq 0$ and $\mathbb{Z}/6 \supsetneq 2\mathbb{Z}/6 \supsetneq 0$

Remark 9.2.4
Some facts about length

1. l_A is uniquely characterized by two properties
   (a) $l_A(A/\mathfrak{m}) = 1$ for any maximal ideal $\mathfrak{m} \subseteq A$
   (b) If $0 \to K \to M \to Q \to 0$ is a short exact sequence of A-module, then $l_A(M) = l_A(K) + l_A(Q)$
2. $l_A(M) = n$ if and only if there exists a chain

$$0 = M_0 \subsetneq M_1 \subsetneq \ldots \subsetneq M_n = M$$

such that each M_i/M_{i-1} is A-simple, that is $M_i/M_{i-1} = A/\mathfrak{m}$ for some maximal ideal $\mathfrak{m}$ of A

Theorem 9.2.5

The following are equivalent

1. A is Noetherian and $(0) = \mathfrak{n}_1...\mathfrak{n}_l$ with each $\mathfrak{n}_i$ is a maximal ideal (there are possibly duplicates)

2. A is Noetherian and $\dim A = 0$

3. A is Artinian

Proof.
$(1 \implies 2)$ Let $\mathfrak{p}$ be any prime ideal, then

$$(0) = \mathfrak{n}_1...\mathfrak{n}_l \subseteq \mathfrak{p}$$

Then at least one $\mathfrak{n}_i \subseteq \mathfrak{p}$, then $\mathfrak{p} = \mathfrak{n}_i$ maximal
$(2 \implies 3)$ Let

$$\Delta = \{I \subseteq A : l_A(A/I) = \infty\}$$

Suppose $l_A(A) = \infty$, then $\Delta \neq \varnothing$ since $(0) \in \Delta$. Due A being Notherian and Zorn lemma, Let J be a maximal element of Δ. We will show that J is prime, or equivalently $S = A/J$ is a domain. Suppse $ab = 0$ for $a, b \in S$ being nonzero , then

$$l_S(S/a), l_S(S/b) < \infty$$

Because if $l_S(S/a) = \infty$, then $\infty = l_S(S/a) = l_A(A/(J,a))$, then $(J,a) \in \Delta$ which contradicts the maximality of J. *($S/a = S/(a) = S/aS$ is the quotient group of S over the ideal generated by a in S)*. Note that the natural map $S \to aS$ defined by $x \mapsto ax$ factors through S/b, so the map $S/b \to aS$ is surjective. The second row in the diagram below is exact

$$\begin{tikzcd}
 & & S \arrow[d] \arrow[dr, two heads] & & \\
0 \arrow[r] & ... \arrow[r, hook] & S/b \arrow[r, two heads] & aS \arrow[r] & 0
\end{tikzcd}$$

Hence, $l_S(aS) \leq l_S(S/b) < \infty$. But, the sequence below is exact

$$0 \longrightarrow aS \hookrightarrow S \twoheadrightarrow S/a \longrightarrow 0$$

Hence, $l_S(S) = l_S(aS) + l_S(S/a) < \infty$. Due to the correspondence of ideals, $l_A(A/J) = l_S(S)$, this is a contradiction. So, J is prime. So, J is a maximal ideal, hence $l_A(A/J) = 1$ which is a contradiction. Hence, $l_A(A) < \infty$
$(3 \implies 1)$ proved earlier. $(0) = \eta_A^k = \mathfrak{m}_1^k...\mathfrak{m}_n^k$

$\square$

Remark 9.2.6

Let $A \supseteq \mathfrak{n}_1 \supseteq \mathfrak{n}_1\mathfrak{n}_2 \supseteq \mathfrak{n}_1\mathfrak{n}_2\mathfrak{n}_3 \supseteq ... \supseteq 0$ and

$$\frac{A}{\mathfrak{n}_{i+1}} = \frac{\mathfrak{n}_1...\mathfrak{n}_i}{\mathfrak{n}_1...\mathfrak{n}_i\mathfrak{n}_{i+1}}$$

is a field, that is a dimension 1 vector space. Hence

$$l_A(A) = \sum_{1 \leq i \leq l} \dim\left(\frac{\mathfrak{n}_1...\mathfrak{n}_i}{\mathfrak{n}_1...\mathfrak{n}_i\mathfrak{n}_{i+1}}\right)$$

which is finite. (*from characterization of length*)

Remark 9.2.7
Given a chain of ideals $0 \subseteq ... \subseteq I_{n-1} \subseteq I_n \subseteq ... \subseteq A$. Then

$$0 \leq ... \leq l_A(I_{n-1}) \subseteq l_A(I_n) \subseteq ... \subseteq l_A(A)$$

9.3 EUCLIDEAN DOMAIN PRINCIPAL IDEAL DOMAIN UNIQUE FACTORIZATION DOMAIN

Definition 9.3.1 (Euclidean domain (ED))
A ring A is an Euclidean domain if there exists a norm function $f : A - \{0\} \to \mathbb{N}$ so that for every $a, b \in A$, there exist $q, r \in A$ so that

$$a = qb + r$$

with $r = 0$ or $f(r) < f(b)$.

Definition 9.3.2 (principal ideal domain (PID))
A ring A is a principal ideal domain if every ideal of A is principal

Definition 9.3.3 (irreducible, associate)
$a \in A$ is called irreducible if $a = bc$ implies b or c is unit. $a, b \in A$ are called associate if $a = ub$ for some unit u

Definition 9.3.4 (unique factorization domain (UFD))
A ring A is a unique factorization domain if every $a \in A$ can be written as

$$a = a_1 a_2 ... a_n$$

where each a_i is irreducible and the decomposition is unique up to associate.

Proposition 9.3.5

$$\{ED\} \subsetneq \{PID\} \subsetneq \{UFD\}$$

Remark 9.3.6
Some examples, non-examples

1. $k[x, y] \in \{UFD\} - \{PID\}$ for a field k
2. $\mathbb{Z}[\sqrt{-19}] \in \{PID\} - \{ED\}$
3. $\mathbb{Z}[i], k[x] \in \{ED\}$ for a field k

Proof. *proof idea for $PID \subseteq UFD$* Let A be a PID, observe that a nonzero prime ideal $\mathfrak{p}$, then $\mathfrak{p}$ is maximal. This is because if $\mathfrak{p} = (x) \subseteq (y)$, then there exists $a \in A$ so that $x = ay$. Thus, y divides 0 in $A/\mathfrak{p}$. $A/\mathfrak{p}$ is a domain, then $y = 0$ in $A/\mathfrak{p}$. Hence $(y) = (x)$. Now, for any nonzero $x \in A$, $A/(x)$ is Noetherian and every prime ideal is maximal, so $A/(x)$ is Artinian. Hence, $A/(x)$ is a product of Artinian local rings

$$A/(x) = \prod_{1 \leq i \leq l} (A_i, \mathfrak{m}_i)$$

Let $I_i = (A \twoheadrightarrow A_i)^{-1}\mathfrak{m}_i = (a_i)$ be the lift of $\mathfrak{m}_1$ in A. If e_i is the smallest integer so that $\mathfrak{m}_i^{e_i} = 0$, then

$$x = a_1^{e_1} ... a_l^{e_l}$$

□

9.4 PRIMARY IDEAL

A non-example for UFD is $\mathbb{Z}[\sqrt{-5}]$

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

and $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ are irreducible in $\mathbb{Z}[\sqrt{-5}]$. It can be seen by defining the norm function on $\mathbb{Z}[\sqrt{-5}]$ as follows

$$\begin{aligned} N : \mathbb{Z}[\sqrt{-5}] &\to \mathbb{Z} \\ a + b\sqrt{-5} &\mapsto a^2 + 5b^2 \end{aligned}$$

norm is multiplicative, that is $N(xy) = N(x)N(y)$, and $N(x) = 1 \iff x$ is a unit. Suppose 2 can be factored into xy, then $4 = N(2) = N(x)N(y)$, if $x = a + b\sqrt{-5}$ then $N(x) = 2$, then $a^2 + 5b^2 = 2$, the equation does not have solution in $\mathbb{Z}$, so $N(x) = 1$ or $N(y) = 1$, that is, either x or y is a unit. Moreover, 2 is not associate with $1 + \sqrt{-5}$ or $1 - \sqrt{-5}$ since $4 = N(2) \neq N(1 \pm \sqrt{-5}) = 6$. Hence, 6 admits two different decompositions into irreducibles, $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.
Another non-example for UFD is $\mathbb{Z}[\xi_n]$ where $\xi_n = e^{(2\pi i)/n}$ is the n-th root of unity. In $\mathbb{Z}[\xi_n]$, $x^n + y^n$ can be factorized into

$$x^n + y^n = (x + y)(x + \xi_n y)(x + \xi_n^2 y)...(x + \xi_n^{n-1} y)$$

If $\mathbb{Z}[\xi_n]$ is an UFD, then Fermat last theorem ($z^n = x^n + y^n$) holds for n. However, this is not the case for all n, $\mathbb{Z}[\xi_n]$ is an UFD for many $n \leq 90$ and no $n > 90$. This section is motivated by a solution for Fermat last theorem for many n by defining a weaker notion of irreducible decomposition. The answer will be revealed at the end of Dedekind domain.

Definition 9.4.1 (primary ideal)
Given a ring A, an ideal I is primary if $xy \in I$ implies $x \in I$ or $y^n \in I$ for some $n \geq 1$

Proposition 9.4.2
An ideal I is primary if and only if every zero divisor in A/I is nilpotent

Remark 9.4.3

Some examples and non-examples

1. if $\mathfrak{p}$ is a prime, then $\mathfrak{p}$ is primary and also $\mathfrak{p}$ is radical, that is $\mathfrak{p} = \sqrt{\mathfrak{p}}$
2. $(x^2, xy) \subseteq k[x,y]$ is primary for a field k
3. let $A = \{p(T) \in \mathbb{Z}[T] : 3 \text{ divides } p'(0)\}$, then $\mathfrak{p} = (3T, T^2, T^3)$ is prime but $\mathfrak{p}^2$ is not primary

Definition 9.4.4 ($\mathfrak{p}$-primary)

If I is a primary ideal, then $\mathfrak{p} = \sqrt{I}$ is prime, we call I a $\mathfrak{p}$-primary ideal.

Proposition 9.4.5

Given any ideal I, if $\sqrt{I}$ is a maximal then I is a primary ideal.

Proof. Let $\mathfrak{m} = \sqrt{I}$, we have $\mathfrak{m}/I \subseteq A/I$ is the unique prime ideal (every prime ideal containing I must contain $\mathfrak{m}$) if and only if all non-unit elements of A/I are in $\mathfrak{m}/I$. Then, any zero divisor of A/I is in $\mathfrak{m}/I$. But all elements of $\mathfrak{m}/I$ are nilpotent, hence I is primary. ☐

Lemma 9.4.6

Given a Notherian ring A

1. I is $\mathfrak{p}$-primary then $\mathfrak{p}^N \subseteq I$ for large N
2. I is $\mathfrak{m}$-primary for some maximal ideal $\mathfrak{m}$ if and only if A/I is Artinian local
3. I is $\mathfrak{m}$-primary for some maximal ideal $\mathfrak{m}$ and $IA_\mathfrak{m} = \mathfrak{m}^n A_\mathfrak{m}$ for some n, then $I = \mathfrak{m}^n$

Proof.

(1) A is Noetherian, then $\mathfrak{p} = (a_1, ..., a_n)$. I is $\mathfrak{p}$-primary, then for every i, there exists $e_i \geq 1$ so that $a_i^{e_i} \in I$. Let $N = e_1 + ... + e_n$, then $\mathfrak{p}^N \subseteq I$

(2 $\Longleftarrow$) Let $\mathfrak{n} \subseteq A/I$ be the unique maximal ideal, so

$$\mathfrak{m} = (A \twoheadrightarrow A/I)^{-1}\mathfrak{n} = \mathfrak{n} \cap A$$

is the lift of $\mathfrak{n}$ in A. Since A/I is Artinian local, then $\mathfrak{n}^k = 0$ for some k, then $\mathfrak{m}^k \subseteq I$, that is $\mathfrak{m} \subseteq \sqrt{I}$. Since $\mathfrak{m}$ is maximal, $\mathfrak{m} = \sqrt{I}$

(2 $\Longrightarrow$) Construct N so that $\mathfrak{m}^N \subseteq I$, then

$$A/\mathfrak{m}^N \twoheadrightarrow A/I$$

is surjective. Since $A/\mathfrak{m}^N$ is Artinian local, then A/I is also Artinian local.

(3) Let $\phi : A \to A_\mathfrak{m}$, then

$$I \subseteq \phi^{-1}(IA_\mathfrak{m}) = \phi^{-1}(\mathfrak{m}^n A_\mathfrak{m}) = \ker(A \to A_\mathfrak{m} \twoheadrightarrow A_\mathfrak{m}/(\mathfrak{m}^n A_\mathfrak{m}))$$

Since $\mathfrak{m}$ is maximal, there is an isomorphism $A_\mathfrak{m}/(\mathfrak{m}^n A_\mathfrak{m}) \xrightarrow{\sim} A/\mathfrak{m}^n$ and the composition $A \to A_\mathfrak{m} \twoheadrightarrow A_\mathfrak{m}/(\mathfrak{m}^n A_\mathfrak{m}) \xrightarrow{\sim} A/\mathfrak{m}^n$ is precisely the projection $A \twoheadrightarrow A/\mathfrak{m}^n$. Hence, $I \subseteq \mathfrak{m}^n$ (*TODO - check*)

Let $Q = \mathfrak{m}^n/I$ be a quotient module, will show that $Q = 0$. It suffices to show that $Q_\mathfrak{n} = 0$ for all maximal ideal $\mathfrak{n}$. Indeed, if $\mathfrak{n} = \mathfrak{m}$, then $Q_\mathfrak{m} = 0$ because $IA_\mathfrak{m} = \mathfrak{m}^n A_\mathfrak{m}$, if $\mathfrak{n} \neq \mathfrak{m}$, then $Q_\mathfrak{n} = A_\mathfrak{n}/A_\mathfrak{n} = 0$ (*TODO - check*). ☐

Theorem 9.4.7

Let A be a dimension 1 Noetherian domain, then every nonzero ideal $I \subseteq A$ admits unique factorization

$$I = \prod_{1 \leq i \leq l} I_i$$

for I_i be a primary ideal and $\sqrt{I_i} \neq \sqrt{I_j}$ for $i \neq j$

Proof. Note that, in A, every nonzero prime ideal is maximal. Then, A/I is Noetherian and dimension 0, hence A/I is Artinian, hence

$$A/I = \prod_{1 \leq j \leq l} A_j$$

for some Artinian local ring $(A_j, \mathfrak{m}_j)$. Let $I_j = \ker(A \twoheadrightarrow A/I \twoheadrightarrow A_j)$, then $A/I_j \cong A_j$. By the previous lemma, I_j is $\mathfrak{m}_j$-primary for some maximal ideal $\mathfrak{m}_j \subseteq A$. Then

$$I = \ker(A \twoheadrightarrow A/I) = I_1 ... I_l$$

□

Remark 9.4.8

$\mathbb{Z}[\xi_n]$ is a dimension 1 Notherian domain.

9.5 DISCRETE VALUATION RING

Definition 9.5.1 (valuation ring)

A domain B is called a valuation ring of $K = \mathrm{Frac}(B)$ if for each nonzero $x \in K$, either $x \in B$ or $x^{-1} \in B$

Definition 9.5.2 (discrete valuation, discrete valuation ring)

A discrete valuation on a field k is a map $V : k^{\times} \to \mathbb{Z}$ so that

1. $V(xy) = V(x) + V(y)$
2. $V(x + y) \geq \min\{V(x), V(y)\}$ and the equality holds if $V(x) \neq V(y)$

For convention, define $V(0) = \infty$. Let

$$\mathcal{O}_V = \{x \in k : V(x) \geq 0\}$$

be a subring of k. A ring of the form $\mathcal{O}_V$ is called discrete valuation ring (DVR).

Remark 9.5.3
Some examples

1. On field $\mathbb{Q}$, let p be a prime

$$V_p : \mathbb{Q}^\times \to \mathbb{Z}$$
$$p^n \frac{a}{m} \mapsto n$$

   Then, $\mathcal{O}_V = \mathbb{Z}/(p)$

2. On field $k[t]$

$$V : k[t]^\times \to \mathbb{Z}$$
$$t^n \frac{f(t)}{g(t)} \mapsto n$$

   Then, $\mathcal{O}_V = k[t]_{(t)}$

Remark 9.5.4 (structure of ideals of DVR, uniformizer)
Let (A, v) be a discrete valuation ring

1. for $x \in k^\times$, $0 = v(1) = v(x^{-1}x) = v(x^{-1}) + v(x)$
2. $u \in A^\times \iff v(u) = 0$
3. for $x, y \in A$, $(x) = (y) \iff x = uy \iff v(x) = v(y)$ for some unit $u \in A$
4. let $I \subseteq A$ be a nonzero ideal, let $x \in I$ with minimal valuation, then $x \in k^\times$, let $y \in I$, then $x^{-1}y \in k$ has valuation

$$v(x^{-1}y) = v(y) - v(x) \geq 0$$

   So, $x^{-1}y \in A$, hence $y = (x^{-1}y)x$ in A, so $y \in (x)$. That is, every ideal of A is principal.

Hence, every ideal in A is of the form

$$I_i = \{x \in A : v(x) \geq i\}_{i \geq 0}$$

Moreover, there exists an element $x \in A$ so that $v(x) = 1$ and $I_i = (x^i)$ and x is called a uniformizer.

Lemma 9.5.5
Let $(A, \mathfrak{m}, k)$ be Artinian local ring, then the following are equivalent

1. every ideal is principal
2. $\mathfrak{m}$ is principal
3. $\dim_k \mathfrak{m}/\mathfrak{m}^2 \leq 1$

Proof.
$(2 \implies 3)$ Let $\mathfrak{m} = (x)$, there exists a surjective map

$$k = \frac{A}{\mathfrak{m}} \twoheadrightarrow \frac{\mathfrak{m}}{\mathfrak{m}^2} = \frac{(x)}{(x^2)}$$
$$\bar{a} \mapsto ax + x^2$$

hence, $\dim_k \mathfrak{m}/\mathfrak{m}^2 \leq \dim k = 1$
$(3 \implies 1)$
If $\dim_k \mathfrak{m}/\mathfrak{m}^2$, then $\mathfrak{m}/\mathfrak{m}^2 = 0$, then $\mathfrak{m} = 0$ by Nakayama lemma. Hence, A is a field.
If $\dim_k \mathfrak{m}/\mathfrak{m}^2 = 1$, then there exists $x \in \mathfrak{m}$ whose image under the map $\mathfrak{m} \twoheadrightarrow \mathfrak{m}/\mathfrak{m}^2$ generates $\mathfrak{m}/\mathfrak{m}^2$. By Nakayama lemma, $\mathfrak{m} = (x)$. Now, suppose a nonzero ideal $I \subseteq A$ that is not principal, there exists $n \geq 1$ so that $I \subseteq \mathfrak{m}^n$ but $I \nsubseteq \mathfrak{m}^{n+1}$. Hence, there exists $y \in I$ so that $y = x^n t$ for some $t \notin (x)$, but $(x) = \mathfrak{m}$ is maximal, so t is a unit, hence $I = (x^n)$. *A is a DVR* □

Proposition 9.5.6 (characterization of discrete valuation ring)
Let $(A, \mathfrak{m}, k)$ be a dimension 1 Noetherian local ring, then the following are equivalent

1. A is discrete valuation ring
2. A is normal domain ($A_\mathfrak{p}$ is integrally closed for every prime $\mathfrak{p} \subseteq A$)
3. $\mathfrak{m}$ is principal
4. $\dim_k \mathfrak{m}/\mathfrak{m}^2 = 1$
5. every ideal in A is of the form (x^l) for some $l \geq 1$

Proof. TODO □

9.6 DEDEKIND DOMAIN

Proposition 9.6.1
Let A be a dimension 1 Notherian domain then the following are equivalent

1. A is a normal domain
2. $A_\mathfrak{m}$ is a normal domain for every maximal ideal $\mathfrak{m}$
3. $A_\mathfrak{m}$ is a discrete valuation ring for every maximal ideal $\mathfrak{m}$

Definition 9.6.2 (Dedekind domain)
A ring A is a Dedekind domain (DD) if it is a dimension 1 Notherian normal domain

Remark 9.6.3 (equivalent formulation for Dedekind domain)
A ring A is a Dedekind domain if and only if it is a dimension 1 Noeatherian integrally closed domain

Remark 9.6.4

$\mathbb{Z}[\xi_n]$ is a Dedekind domain for every n

Proposition 9.6.5

Let A be a Dedekind domain then any nonzero primary ideal is a power of primes

Proof. Let I be a nonzero primary ideal, then I is $\mathfrak{m}$-primary for some maximal ideal $\mathfrak{m}$. But $A_\mathfrak{m}$ is DVR, then $IA_\mathfrak{m} = \mathfrak{m}^n A_\mathfrak{m}$ for some n. Hence, $I = \mathfrak{m}^n$ (*TODO - check*) ☐

Theorem 9.6.6

Let A be a Dedekind domain and I be a nonzero ideal then I admits a unique decomposition

$$I = \prod_{1 \le i \le l} \mathfrak{p}_i^{e_i}$$

for some prime ideals $\mathfrak{p}_i$ and $e_i \in \mathbb{N}$.

we proved this in section of primary ideal

Relation to Fermat last theorem: By Kummer, for "regular" prime $p \in [0, 100]$, the structure of $\mathbb{Z}[\xi_p]$ implies Fermat last theorem for $n = p$. Back to $\mathbb{Z}[\sqrt{-5}]$, it is not a UFD but a DD, 6 can be decomposed into irreducibles in at least two ways

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

We have a decomposition of ideals

$$(6) = (2)(3) = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

However, $(2), (3), (1 + \sqrt{-5}), (1 - \sqrt{-5})$ are not prime ideals. They can be decomposed further into product of prime ideals as follows:

$$\begin{aligned}(2) &= (2, 1 + \sqrt{-5})^2 \\ (3) &= (3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5}) \\ (1 + \sqrt{-5}) &= (3, 1 + \sqrt{-5})(2, 1 + \sqrt{-5}) \\ (1 - \sqrt{-5}) &= (3, 1 - \sqrt{-5})(2, 1 + \sqrt{-5})\end{aligned}$$

We have a decomposition of prime ideals

$$(6) = (2, 1 + \sqrt{-5})^2 (3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5})$$

Remark 9.6.7

Alexander Youcis - This is really a remarkable thing!

9.7 FRACTIONAL IDEAL, INVERTIBLE IDEAL

Since PID is both UFD and DD, next, we quantify the difference between DD and PID.

Definition 9.7.1 (fractional ideal)
Let A be a domain and $K = \mathrm{Frac}(A)$, let M be an A-submodule of K (or any finite field extension of K) such that there exists $x \in A - \{0\}$ so that $xM \subseteq A$. M is called a fractional ideal of A. We write

$$(A : M) = \{x \in A : xM \subseteq A\}$$

then $(A : M)$ is an ideal of A and $(A : M) \neq 0$ if and only if M is fractional

Remark 9.7.2
xM is a A-submodule of A which is an ideal of A. $M \subseteq x^{-1}A$ is a A-submodule of K generated by x^{-1}, hence $M = x^{-1}J$ for some ideal J of A
Some examples

1. Any ideal I of A is a fractional ideal
2. Any $y \in K$ generates a fractional ideal $M = yA$

Every finitely generated A-submodule of K is a fractional ideal of A because if $M = A\left\{\frac{a_1}{b_1}, ..., \frac{a_n}{b_n}\right\}$ is a finitely generated submodule of K, then $x = b_1...b_n$ verifies M being a fractional ideal.
Conversely, if A is Noetherian, every fractional ideal of A is finitely generated because xM is an ideal of A

Definition 9.7.3 (invertible ideal)
Let A be a domain and $K = \mathrm{Frac}(A)$, let M be an A-submodule of K such that there exists a A-submodule N of K so that

$$MN = A$$

then, M is called an invertible ideal of A

Remark 9.7.4
Invertible ideals of A form a group and the principal invertible ideals form a subgroup of invertible ideals. An the quotient is called class group $\mathrm{Cl}(A)$

Proposition 9.7.5
Let A be a domain and $K = \mathrm{Frac}(A)$, if M is a invertible ideal and $MN = A$ for some A-submodule N of K, then N is unique and equal $(A : M)$

Proof. Since $(A : M)M \subseteq A$ for any submodule M, then

$$N \subseteq (A : M) = (A : M)MN \subseteq AN \subseteq N$$

$\square$

Proposition 9.7.6
Any invertible ideal is finitely generated A-module, so it is fractional

Proof. If M is invertible, then $A = M(A : M)$, then

$$1 = \sum x_i y_i$$

for some $x_i \in M, y_i \in (A : M)$. If $x \in M$, then

$$x = 1x = \sum x_i(y_i x)$$

That is, $\{x_i\}$ generates M as an A-module ☐

Proposition 9.7.7

Let $M \subseteq K$ be a fractional ideal, the following are equivalent

1. M is invertible
2. M is finitely generated and $M_\mathfrak{p}$ is invertible in $A_\mathfrak{p}$ for every prime ideal $\mathfrak{p}$
3. M is finitely generated and $M_\mathfrak{m}$ is invertible in $A_\mathfrak{m}$ for every maximal ideal $\mathfrak{m}$

($3 \implies 1$ without M being finitely generated)

Proof.
($1 \implies 2$) $A = M(A : M)$ implies $A_\mathfrak{p} = M_\mathfrak{p}(A : M)_\mathfrak{p} = M_\mathfrak{p}(A_\mathfrak{p} : M_\mathfrak{p})$, then $M_\mathfrak{p}$ is invertible (*TODO - check*)
($3 \implies 1$) Consider $I = M(A : M) \subseteq A$. It is equivalent to show that $I = A$ for every maximal ideal $\mathfrak{m}$. Indeed, $I_\mathfrak{m} = M_\mathfrak{m}(A_\mathfrak{m} : M_\mathfrak{m}) = A_\mathfrak{m}$, hence $I = A$ (recall that $M = 0 \iff M_\mathfrak{m} = 0$ for all maximal ideal $\mathfrak{m}$) ☐

Lemma 9.7.8

If A is a local domain and every nonzero fractional ideal is invertible then A is a principal ideal domain

Proof. *TODO* ☐

Proposition 9.7.9

If A is a local domain, then A is a discrete valuation ring if and only if every nonzero fractional ideal is invertible

Proof.
($\implies$) Let $\mathfrak{m} = (x)$, then every ideal of a local DVR is of the form (x^n). Let M be a nonzero fractional ideal, then $x^n M \subseteq A$ for some large n. As $x^n M$ is another ideal, then $x^n M = (x^t)$ for some t, hence $M = x^{t-n}A$. M is invertible with

$$(A : M) = x^{n-t}A$$

($\impliedby$)
Any fractional ideal of A is invertible, hence any ideal of A is invertible, hence any ideal of A is finitely generated, hence A is Noetherian. Suppose A is not DVR, let

$$\Sigma = \{\text{nonzero proper ideal } I \subsetneq A : I \neq \mathfrak{m}^r \text{for every } r\}$$

Since A is Noetherian, pick a maximal element $\Omega \in \Sigma$. Then $\Omega \subsetneq \mathfrak{m}$, hence $\mathfrak{m}^{-1}\Omega \subsetneq A$ is a proper ideal of A. If $\Omega = \mathfrak{m}^{-1}\Omega$, then $\mathfrak{m}\Omega = \Omega$, then $\Omega = 0$ by Nakayama lemma. So $\Omega \subseteq \mathfrak{m}^{-1}\Omega$, hence by maximality of Ω, $\mathfrak{m}^{-1}\Omega = \mathfrak{m}^r$, so $\Omega = \mathfrak{m}^{r+1}$ ☐

Theorem 9.7.10

Let A be a domain, then A is a Dedekind domain if and only if all nonzero fractional ideals are invertible.

Proof.
($\Longrightarrow$) If a nonzero A-module M is fractional, then M is finitely generated. For every prime ideal $\mathfrak{p}$, $M_\mathfrak{p}$ is a fractional ideal of $A_\mathfrak{p}$. Hence, for every prime ideal $\mathfrak{p}$, $M_\mathfrak{p}$ is invertible, hence M is invertible
($\Longleftarrow$) Every nonzero ideal I of A is invertible, hence I is finitely generated, then A is Noetherian. It is equivalent to show that for every nonzero prime ideal $\mathfrak{p}$, $A_\mathfrak{p}$ is DVR, that is every ideal $I \cap A_\mathfrak{p}$ is invertible. Let $J = I \cap A$, then J is invertible, then $I = JA_\mathfrak{p} = J_\mathfrak{p}$ is invertible. □

Corollary 9.7.11

If A is a Dedekind domain, then nonzero fractional ideals form an abelian group I_A under multiplication. If $I \subseteq K = \mathrm{Frac}(A)$ is a fractional ideal, then for every nonzero prime ideal $\mathfrak{p}$ of A, $IA_\mathfrak{p}$ is fractional ideal of $A_\mathfrak{p}$, hence

TODO

9.8 PROJECTIVE MODULE

Definition 9.8.1 (projective module)

An A-module P is projective if one of the following

1. P is a summand of a free A-module
2. $\mathrm{Hom}(P, -)$ is exact
3. for every diagram, there exists a unique map $P \to M$ making it commutes

$$\begin{tikzcd} & P \arrow[dl, dashed] \arrow[d] \\ M \arrow[r, two heads] & N \end{tikzcd}$$

Proof.
TODO □

Proposition 9.8.2

If A is a Noetherian local ring and M is a finitely generated and projective A-module, then M is free

Proof. *TODO* □

Proposition 9.8.3 (projective is locally free, rank of projective module)

Let A be a Noetherian ring and M is a finitely generated A-module, then M is projective if and only if $M_\mathfrak{p}$ is free for every prime ideal $\mathfrak{p}$ of A
The rank of M is defined as the rank of free module $M_\mathfrak{p}$

Proof. *TODO - looks like M is locally free - OMG, it is locally free sheaf - see notes* □

Definition 9.8.4 (rank of a module - https://mathoverflow.net/a/30024/146879)
Let A be a domain and $K = \mathrm{Frac}(A)$, the rank of an M-module is defined by

$$\operatorname{rank} M = \operatorname{rank}_K K \otimes_A M$$

when $M = A^I$ is a free module, then $\operatorname{rank} M = |I|$, when M is projective, then $\operatorname{rank} M = \operatorname{rank} A_{\mathfrak{p}}$. For projective module M, $\operatorname{rank} M$ is also the size of maximal linearly independent set.
*Consider a projective module P of finite type over a commutative ring A. It corresponds to a locally free sheaf $\mathcal{F}$ over $X = Spec(A)$. The rank of $\mathcal{F}$ at the prime ideal $\mathfrak{p}$ is that of the *free* $A_{\mathfrak{p}}$-module $\mathcal{F}_{\mathfrak{p}}$.*

Remark 9.8.5
If A is a normal domain, any fractional ideal is a projective module of rank 1, for Dedekind domain, it is easy to see that

$$I_{\mathfrak{p}} = \mathfrak{p}^n A_{\mathfrak{p}} \cong A_{\mathfrak{p}}$$

Proposition 9.8.6
If P_1, P_2, and $P_1 \otimes_A P_2$ are projective over a domain A and P_1 and P_2 are finitely generated of rank n_1 and n_2, then $\operatorname{rank}(P_1 \otimes P_2) = n_1 n_2$

Remark 9.8.7
Rank 1 projective modules form a monoid under tensor product, moreover, it is a group with inverse of P defined by $P^* = \mathrm{Hom}_A(P, A)$. For a domain A, define the Picard group $\mathrm{Pic}(A)$ by the set of rank 1 projective modules up to isomorphism.

Theorem 9.8.8
If A is a Dedekind domain, then

$$\mathrm{Cl}(A) \xrightarrow{\sim} \mathrm{Pic}(A)$$
$$I \mapsto [I]$$

9.9 GEOMETRY

Some applications/connections of commutative algebra in/to geometry

Definition 9.9.1 (finite-type algebra over field)
Let k be a field, A is a k-algebra of finite-type if there exists a surjection

$$k[x_1, ..., x_n] \twoheadrightarrow A$$

Proposition 9.9.2

If K is a field and a finite-type k-algebra, then K is a finite field extension of k, that is, K can be realized at a finite dimension k-vector space

Proof. TODO □

Theorem 9.9.3 (weak nullstellensatz)

Suppose k is an algebraically closed field, then

1. every maximal ideal of $k[x_1, ..., x_n]$ is of the form

$$(x_1 - a_1, ..., x_n - a_n)$$

for some point $(a_1, ..., a_n) \in k^n$

2. If $f_1, ..., f_m \in k[x_1, ..., x_n]$ are polynomials such that

$$V(f_1, ..., f_m) = \{x \in \mathbb{A}_k^n : f_i(x) = 0 \text{ for every } f_i\} = \varnothing$$

then $(f_1, ..., f_m) = 1$

Proof. TODO □

Remark 9.9.4

Some remarks on nullstellensatz

1. $\mathbb{A}_k^n = k^n$ is called affine n-space over k

2. let $f_1, ..., f_m \in k[x_1, ..., x_n]$, then the set of common zeros (zero locus) of $f_1, ..., f_m$

$$V(f_1, ..., f_m) = \{x \in \mathbb{A}_k^n : f_i(x) = 0 \text{ for every } f_i\}$$

is called an affine variety.

3. nullstellensatz connects classical geometry in an elegant way. every maximal ideal in $k[x_1, ..., x_n]$ corresponding to a single point in $\mathbb{A}_k^n$, when the affine variety $V(f_1, ..., f_m)$ is empty, then there is no corresponding maximal ideal

Theorem 9.9.5 (strong nullstellensatz)

Suppose k is an algebraically closed field. Let $f, f_1, ..., f_m \in k[x_1, ..., x_n]$, and

$$V(f_1, ..., f_m) \subseteq V(f)$$

then $f^d \in (f_1, ..., f_m)$ for some $d \in \mathbb{N}$

Proof. TODO □

Remark 9.9.6 (geometric version of strong nullstellensatz)
Let k be an algebraically closed field, $\mathfrak{a} \subseteq k[x_1, ..., x_n]$ be an ideal. The variety $V(\mathfrak{a})$ is the set of common zeros of polynomials in $\mathfrak{a}$

$$V(\mathfrak{a}) = \{x \in \mathbb{A}_k^n : f(x) = 0 \text{ for every } f \in \mathfrak{a}\} \subseteq \mathbb{A}_k^n$$

The ideal $I(V(\mathfrak{a})) \subseteq k[x_1, ..., x_n]$ of a variety $V(\mathfrak{a}) \subseteq \mathbb{A}_k^n$ is the set of polynomials that vanish on $V(\mathfrak{a}) \subseteq \mathbb{A}_k^n$

$$I(V(\mathfrak{a})) = \{f \in k[x_1, ..., x_n] : f(x) = 0 \text{ for every } x \in V(\mathfrak{a})\} \subseteq k[x_1, ..., x_n]$$

strong nullstellensatz states that I is an isomorphism

$$I : \{\text{algebraic sets in } \mathbb{A}_k^n\} \xrightarrow{\sim} \{\text{radical ideals of } k[x_1, ..., x_n]\}$$
$$V(\mathfrak{a}) \mapsto \sqrt{\mathfrak{a}}$$

Theorem 9.9.7 (Noether normalization theorem)
Let k be a field and A be a finite-type k-algebra, then there exists $x_1, ..., x_n \in A$ so that

$$\phi : k[X_1, ..., X_n] \hookrightarrow A$$
$$X_i \mapsto x_i$$

and A is finitely generated as a module over the image or equivalently A is integral over $k[x_1, ..., x_n]$. Moreover, $x_1, ..., x_n$ are algebraically independent over k, that is, x_i does not satisfy any nontrivial polynomial equation with coefficients in k

Proof. *TODO - I have to skip many proofs since proof-reading requires a lot of time - while understanding the statement is more important.* □

Chapter 10

HOMOLOGICAL ALGEBRA

10.1 BASIC HOMOLOGICAL ALGEBRA

Concrete version of Homological Algebra

Definition 10.1.1 ((co)chain complex)
TODO
Note that, the category of (co)chain complexes is also abelian

Definition 10.1.2 ((co)homology)
For any $n \in \mathbb{Z}$, homology $H_n(-)$ is a functor in the category of chain complexes defined by

$$H_n(C_\bullet) = \frac{\ker(d : C_n \to C_{n-1})}{\operatorname{im}(d : C_{n+1} \to C_n)}$$

Similar definition for cohomology

Definition 10.1.3 (category of (co)chain complexes, short exact sequence)
TODO

Lemma 10.1.4 (fundamental lemma of homological algebra)
A short exact sequence of (co)chain complexes $0 \to L_\bullet \to M_\bullet \to N_\bullet \to 0$ induces a natural long exact sequence in (co)homology

$$\begin{tikzcd}
 & \dots \arrow[r] & H_{n+1}(N_\bullet) \arrow[dll] \\
H_n(L_\bullet) \arrow[r] & H_n(M_\bullet) \arrow[r] & H_n(N_\bullet) \arrow[dll] \\
H_{n-1}(L_\bullet) \arrow[r] & \dots &
\end{tikzcd}$$

Definition 10.1.5 ((co)chain homotopy)
TODO

Proposition 10.1.6
homotopic (co)chain maps induce the same map in (co)homology

Definition 10.1.7 (projective module and projective resolution)
An A-module P is projective if one of the following

1. P is a summand of a free A-module
2. $\mathrm{Hom}(P, -)$ is exact
3. for every diagram, there exists a unique map $P \to M$ making it commutes

$$\begin{tikzcd} & P \arrow[dl, dashed] \arrow[d] \\ M \arrow[r, two heads] & N \end{tikzcd}$$

Given any A-module M, there exists an exact sequence

$$\ldots \to P_2 \to P_1 \to P_0 \to M \to 0$$

where $P_0, P_1, \ldots$ are projective. Then the sequence

$$\ldots \to P_2 \to P_1 \to P_0 \to 0$$

is called a projective resolution for M

Remark 10.1.8
We can break the projective resolution into short exact sequences

$$0 \to K_1 \to P_0 \to M \to 0$$
$$0 \to K_2 \to P_1 \to K_1 \to 0$$
$$0 \to K_3 \to P_2 \to K_2 \to 0$$
$$\ldots$$

where $K_1 = \ker(P_0 \to M)$ and $K_i = \ker(P_{i+1} \to P_i)$ for $i \geq 1$

Proof. *TODO - fill up* □

Remark 10.1.9
If A is Noetherian and M is finitely generated then there exists a free resolution $P_\bullet$ so that each P_n is finitely generated.
pseudo-coherent A-module

Definition 10.1.10 (Tor)
Define $\mathrm{Tor}_n^A(-,N)$ by the left derived functor of $(- \otimes_A N)$

Proposition 10.1.11 (properties of Tor)
Some other properties for Tor

1. $\mathrm{Tor}_n^A(M,N) = \mathrm{Tor}_n^A(N,M)$
2. $\mathrm{Tor}_n^A(M,-) = 0$ for every $n \geq 1 \iff \mathrm{Tor}_1^A(M,-) = 0 \iff M$ is flat
3. $\mathrm{Tor}_0^A(M,N) = M \otimes_A N$
4. M is projective $\implies M$ is flat
5. (left derived functor) given a short exact sequence $0 \to A \to B \to C \to 0$, then there exists a long exact sequence

$$\begin{tikzcd}
 & \dots \arrow[r] & \mathrm{Tor}_2(C,N) \arrow[dll] & \\
\mathrm{Tor}_1(A,N) \arrow[r] & \mathrm{Tor}_1(B,N) \arrow[r] & \mathrm{Tor}_1(C,N) \arrow[dll] & \\
A \otimes N \arrow[r] & B \otimes N \arrow[r] & C \otimes N \arrow[r] & 0
\end{tikzcd}$$

Why Tor? (read why left derived functor)
Let $x \in A$ be a nonzero divisor and any A-module M, then the SES $0 \to A \xrightarrow{x} A \to A/x \to 0$ induces a LES

$$\mathrm{Tor}_1^A(A/x, M) \to A \otimes M \xrightarrow{x \otimes 1} A \otimes M \to A/x \otimes M \to 0$$

Hence, $\mathrm{Tor}_1(A/x, M) = \ker(x \otimes 1) = \{m \in M : xm = 0\}$ which is the torsion-submodule of M

Theorem 10.1.12
Let M be an A-module, the following are equivalent

1. M is flat
2. for every injective map $0 \to N \to N_1$ such that N_1/N is finitely generated, then $0 \to N \otimes M \to N_1 \otimes M$ is exact
3. for every ideal I in A, $\mathrm{Tor}_1(A/I, M) = 0$
4. for every ideal I in A, the map $I \otimes M \to A \otimes M \cong M$ induced from $I \hookrightarrow A$ is injective

Proof. TODO $\square$

Definition 10.1.13 (injective module and injective resolution)
An A-module I is injective if one of the following

1. $\mathrm{Hom}(-, I)$ is exact
2. for every diagram, there exists a unique map $N \to I$ making it commutes

$$\begin{tikzcd} P & \\ M \arrow[u] \arrow[r, hook] & N \arrow[ul, dashed] \end{tikzcd}$$

Given any A-module N, there exists an exact sequence

$$0 \to N \to I_0 \to I_1 \to I_2 \to ...$$

where $I_0, I_1, ...$ are projective. Then the sequence

$$0 \to I_0 \to I_1 \to I_2 \to ...$$

is called an injective resolution for N

Remark 10.1.14
$\mathbb{Q}/\mathbb{Z}$ is an injective $\mathbb{Z}$-module

Definition 10.1.15 (Ext)
Define $\mathrm{Ext}^n_A(-, N)$ by the left derived functor of $\mathrm{Hom}(-, N)$.
Define $\mathrm{Ext}^n_A(M, -)$ by the right derived functor of $\mathrm{Hom}(M, -)$

Proposition 10.1.16 (properties of Ext)

Some other properties for Ext

1. M is projective $\implies \mathrm{Ext}^n_A(M,-)=0$ for every $n\geq 1$
2. (right derived functor) given a short exact sequence $0\to A\to B\to C\to 0$, then there exists a long exact sequence

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Hom}(M,A) \arrow[r] & \mathrm{Hom}(M,B) \arrow[r] & \mathrm{Hom}(M,C) \arrow[dll] \\
 & \mathrm{Ext}^1(M,A) \arrow[r] & \mathrm{Ext}^1(M,B) \arrow[r] & \mathrm{Ext}^1(M,C) \arrow[dll] \\
 & \mathrm{Ext}^2(M,A) \arrow[r] & \ldots &
\end{tikzcd}$$

3. (left derived functor) there exists a long exact sequence

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Hom}(C,N) \arrow[r] & \mathrm{Hom}(B,N) \arrow[r] & \mathrm{Hom}(A,N) \arrow[dll] \\
 & \mathrm{Ext}^1(C,N) \arrow[r] & \mathrm{Ext}^1(B,N) \arrow[r] & \mathrm{Ext}^1(A,N) \arrow[dll] \\
 & \mathrm{Ext}^2(C,N) \arrow[r] & \ldots &
\end{tikzcd}$$

4. (Baer criterion) An A-module M is injective if and only every map $I\to M$ from an ideal I can be extended into a map $M\to A$. In particular, if A is a PID, M is injective if and only if it is divisible, that is, for every nonzero $a\in A$ and every $m\in M$, there exists $n\in M$ so that $an=m$

10.2 COMOLOGICAL INVARIANT OF MODULES

Definition 10.2.1 (projective dimension)

Given an A-module M, define

$$\operatorname{projdim}_A M=\min\{d\in\mathbb{Z}_{\geq 0}: \text{ there exists a projective resolution } 0\to P_d\to\ldots\to P_0\to M\to 0\}$$

if there is no finite length projective resolution for M, define $\operatorname{projdim}_A M=+\infty$

Remark 10.2.2

Some remarks

1. M is projective $\iff \operatorname{projdim}_A M = 0$
2. let $A = k[x]$ for some field k and $M = A/(x)$, then $\operatorname{projdim}_A M = 1$ with the projective resolution
$$0 \to k[x] \xrightarrow{x} k[x] \to M \to 0$$
3. let $A = k[x]/(x^2)$ for some field k and $M = A/(x)$, then $\operatorname{projdim}_A M = +\infty$
4. let $A = \mathbb{C}[x, y, z]$ and $M = \operatorname{Frac}(A)$, then
$$\operatorname{projdim}_A M = \begin{cases} 2 & \text{if CH is true} \\ 3 & \text{if CH is false} \end{cases}$$

Proposition 10.2.3

Let M be an A-module, then the following are equivalent

1. $\operatorname{projdim}_A M \leq d$
2. $\operatorname{Ext}_A^i(M, -) = 0$ for all $i \geq d + 1$
3. $\operatorname{Ext}_A^{d+1}(M, -) = 0$

Remark 10.2.4

there is a similar notion for injective dimension injdim and similar proposition with $\operatorname{Ext}(-, N)$

Corollary 10.2.5

Given a short exact sequence $0 \to M \to P \to N \to 0$, and P is projective

1. if N is projective then $\operatorname{projdim}_A M = 0$
2. if N is not projective, then
$$\operatorname{projdim}_A M = \operatorname{projdim}_A N - 1$$

Given a Noetherian local ring $(A, \mathfrak{m}, k)$, and a map $\phi : M \to N$ of finitely generated A-modules, then $\bar{\phi} : M \otimes k \to N \otimes k$ is a map of k-vector spaces, then by Nakayama lemma

1. ϕ is surjective if and only if $\bar{\phi}$ is surjective
2. ϕ is an isomorphism if and only if $\bar{\phi}$ is surjective and $\ker \phi \subseteq \mathfrak{m}M$

If M and N are free (if and only if projective in Noetherian local ring), then

1. if $\bar{\phi}$ is an isomorphism then M and N has the same rank as A-modules
2. if ϕ is surjective, then ϕ is an isomorphism

Definition 10.2.6 (minimal free resolution)
Given a Noetherian local ring $(A, \mathfrak{m}, k)$ and an A-module M, a minimal free resolution of M is an exact sequence

$$... \to L_2 \xrightarrow{d_2} L_1 \xrightarrow{d_1} L_0 \xrightarrow{\epsilon} M \to 0$$

so that

1. each L_i is a finitely generated free A-module
2. each $\bar{d}_i : L_{i+1} \otimes k \to L_i \otimes k$ is zero, or equivalently $\operatorname{im} d_i \subseteq \mathfrak{m}L_{i-1}$
3. $\bar{\epsilon} : L_0 \otimes k \to M \otimes k$ is an isomorphism

Remark 10.2.7
We can break the free resolution into short exact sequences

$$\begin{aligned} 0 \to K_1 \to & L_0 \to M \to 0 \\ 0 \to K_2 \to & L_1 \to K_1 \to 0 \\ 0 \to K_3 \to & L_2 \to K_2 \to 0 \\ & ... \end{aligned}$$

where $K_1 = \ker(L_0 \to M)$ and $K_i = \ker(L_{i+1} \to L_i)$ for $i \geq 1$, then 2 and 3 are equivalent to

$$\begin{aligned} L_0 \otimes k &\cong M \otimes k \\ L_1 \otimes k &\cong K_1 \otimes k \\ L_2 \otimes k &\cong K_2 \otimes k \end{aligned}$$

Remark 10.2.8
Minimal free resolution exists for every A-module M and moreover, any two minimal free resolutions are term-wise isomorphic and compatible with differential maps

Proposition 10.2.9
Let M be a finitely generated A-module and $L_\bullet$ be a minimal free resolution of M, then

1. $\operatorname{rank}_A L_i = \dim_k \operatorname{Tor}_i^A(M, k)$ for every $i \geq 0$
2. projective dimension can be characterized by the length of minimal free resolution, that is, minimal free resolution is the length of the shortest projective resolution

$$\operatorname{projdim}_A M = \sup\{i \in \mathbb{Z}_{\geq 0} : \operatorname{Tor}_i^A(M, k) \neq 0\} \leq \operatorname{projdim}_A k$$

10.3 ANOTHER PREVIEW OF DIMENSION THEORY

Remark 10.3.1 (Serre-Auslander-Buchsbaum - turning point for homological algebra)
Let A be a Noetherian local ring

1. $\dim A \leq \dim_k \mathfrak{m}/\mathfrak{m}^2 \leq \infty$
2. the following are equivalent
   (a) $\dim A = \dim_k \mathfrak{m}/\mathfrak{m}^2$
   (b) $\operatorname{projdim}_A k < +\infty$
   (c) $\operatorname{projdim}_A M < +\infty$ for every finitely generated module M
3. if A is regular then $A_\mathfrak{p}$ is also regular.

to the best of Prof Hansen's knowledge, (3) can only be proved using homological algebra techniques

Definition 10.3.2 (regular sequence)
Let M be an A-module, elements $f_1, ..., f_r \in A$ form a M-regular sequence if (1) $M/(f_1, ..., f_r)M \neq 0$ and (2) the following functions are injective

$$\begin{aligned}
&f_1 : M \to M \\
&f_2 : M/f_1M \to M/f_1M \\
&\quad ... \\
&f_i : M/(f_1, ..., f_{i-1})M \to M/(f_1, ..., f_{i-1})M
\end{aligned}$$

(1) implies $f_1, ..., f_r$ are not unit (2) implies f_1 is not zero or zero divisor on A, f_2 is not zero or zero divisor on A/f_1A, ..., f_i is not a zero divisor on $A/(f_1, ..., f_{i-1})A$

Remark 10.3.3
Some remarks on M-regular sequence

1. If $A = k[x_1, ..., x_n]$ for some field k and $M = A$, then $x_1, ..., x_n$ is a regular sequence
2. If $f_1, ..., f_r$ form a M-regular sequence then so is
$$f_1^{\alpha_1}, ..., f_r^{\alpha_r}$$
for every $\alpha_i \in \mathbb{Z}_{\geq 1}$
3. If A is Noetherian local, M is finitely generated, and $f_1, ..., f_r$ is a M-regular sequence, so is
$$f_{\sigma(1)}, ..., f_{\sigma(r)}$$
for every $\sigma \in S_r$ element of symmetric group of r elements

Definition 10.3.4 (depth)
Let M be an A-module and I be an ideal of a ring A, then

$$I \text{ contains a } M\text{-regular sequence of length } r \iff \operatorname{Ext}_A^i(A/I, M) = 0 \ \forall i < r$$

In particular, $\inf\{i \geq 0 : \operatorname{Ext}_A^i(A/I, M) \neq 0\}$ is the maximal length of every M-regular sequence in I. Let $(A, \mathfrak{m}, k)$ be a Notherian local ring, define $\operatorname{depth}_A M$

$$\operatorname{depth}_A M = \inf\{i \geq 0 : \operatorname{Ext}_A^i(k, M) \neq 0\}$$

Remark 10.3.5
Some remarks on depth

1. $\operatorname{depth}_A k = 0$ because there is no k-regular sequence
2. $A = k[[x_1, ..., x_n]]$ for some field k, then $\operatorname{depth}_A A = n = \dim A$
3. $\operatorname{depth}_A A \leq \dim A$

Theorem 10.3.6 (Auslander–Buchsbaum formula)
If A is a Noetherian local ring and M is a finitely generated module with $\operatorname{projdim}_A M < +\infty$, then

$$\operatorname{projdim}_A M + \operatorname{depth}_A M = \operatorname{depth}_A A$$

After *André Weil* published his famous Fermat's last theorem proof, homological algebra is the tool to strim down his proof.

Chapter 11

DIMENSION THEORY

Remark 11.0.1 (dimension, projective dimension, embedding dimension)
dimension of a variety is like manifold dimension. embedding dimension is like the dimension of the tangent space.

11.1 NOETHERIAN RING

Definition 11.1.1 (minimal prime)
Let $\mathfrak{p}$ be a prime in A, then

$$\operatorname{ht}\mathfrak{p} = \sup\{n \in \mathbb{N} : \text{ there exists a chain of primes } \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \mathfrak{p}_2 \subsetneq \dots \subsetneq \mathfrak{p}_n = \mathfrak{p}\}$$

which is also $\operatorname{codim} V(\mathfrak{p})$ in $\operatorname{Spec} A$ (in manifold sense) and

$$\dim A = \sup_{\mathfrak{p} \subseteq A} \operatorname{ht}\mathfrak{p}$$

If I is an ideal in A, then a minimal prime $\mathfrak{p}$ over I is the minimal element of the poset set of primes containing I ordered by inclusion. Minimal prime over I is also the minimal prime in A/I

Theorem 11.1.2 (Krull principal ideal theorem)
Let A be a Noetherian ring and any $x \in A$, then any minimal prime over the principal ideal (x) has height $\operatorname{ht}\mathfrak{p} \leq 1$

Theorem 11.1.3 (Krull height theorem (KHT))
Let A be a Noetherian ring

1. given $x_1, \dots, x_n \in A$, any minimal prime $\mathfrak{p}$ over finitely generated ideal $(x_1, \dots, x_n)$ has height $\operatorname{ht}\mathfrak{p} \leq n$
2. if $\mathfrak{q}$ is a prime of height n then there exists $x_1, \dots, x_n$ such that $\mathfrak{q}$ is minimal over the finitely generated ideal $(x_1, \dots, x_n)$

Proof. *TODO* □

11.1.1 CONSEQUENCES OF KRULL HEIGHT THEOREM FOR LOCAL RING

Corollary 11.1.4
Some corollaries of KHT

1. If $(A, \mathfrak{m})$ is a Noetherian local ring, then $\dim A = \operatorname{ht} \mathfrak{m} < \infty$
2. If A is a Noetherian ring, and $\mathfrak{p} \subseteq A$ is a prime, then $\operatorname{ht} \mathfrak{p} < +\infty$

Lemma 11.1.5 (prime avoidance lemma)
Let I be an ideal in a ring A, let $J_1, ..., J_n$ be ideals in A such that for all but ≤ 2 of them are not prime. If $I \nsubseteq J_i$ for every $i = 1, ..., n$, then

$$I \nsubseteq \bigcup_{i=1}^{n} J_i$$

Corollary 11.1.6
If k is an algebraically closed field, then $\dim k[x_1, ..., x_n] = n$

Proposition 11.1.7
Let I be an ideal in a Noetherian local ring $(A, \mathfrak{m})$, the following are equivalent

1. $\mathfrak{m}$ is a minimal prime over I
2. $\sqrt{I} = \mathfrak{m}$
3. I is $\mathfrak{m}$-primary
4. $\mathfrak{m}^n \subseteq I$ for large n

Definition 11.1.8 (system of parameters (SoP))
By KHT, given a Noetherian local ring $(A, \mathfrak{m})$ with $\dim A = \operatorname{ht} \mathfrak{m} = n < \infty$, we can choose exactly n elements $x_1, ..., x_n \in A$ so that $\mathfrak{m}$ is minimal over $(x_1, ..., x_n)$, that is $(x_1, ..., x_n)$ is $\mathfrak{m}$-primary. Such a list is called a system of parameters of A

Proposition 11.1.9
Let $(A, \mathfrak{m})$ be a Noetherian local ring and $x_1, ..., x_m$ be some elements in $\mathfrak{m}$ with $m \leq \dim A$, then the following are equivalent

1. $x_1, ..., x_m$ can be extended into a system of parameters
2. $\dim A/(x_1, ..., x_m) \leq \dim A - m$
3. $\dim A/(x_1, ..., x_m) = \dim A - m$

Proof.
($2 \implies 1$) Pick a system of parameters $y_1, ..., y_d$ of the local ring $A/(x_1, ..., x_m)$ of dimension d, then $(y_1, ..., y_d)$ is $\mathfrak{m}$-primary in $A/(x_1, ..., x_m)$, that is every element $z+a_1x_1+...+a_mx_m \in \mathfrak{m}+(x_1, ..., x_m)$ satisfies $(z+a_1x_1+...+a_mx_m)^k = z^k + b_1x_1 + ... + b_mx_m \in (y_1, ..., y_d)$ for some k, so $z^k \in (x_1, ..., x_m, \tilde{y}_1, ..., \tilde{y}_d)$ where $\tilde{y}_i \in A$ is a lift for y_i. Hence, $(x_1, ..., x_n, \tilde{y}_1, ..., \tilde{y}_d)$ is $\mathfrak{m}$-primary. So, $\mathfrak{m}$ is minimal prime over $(x_1, ..., x_n, \tilde{y}_1, ..., \tilde{y}_d)$, by KHT,

$$\dim A = \operatorname{ht} \mathfrak{m} \leq \dim A/(x_1, ..., x_m) + m \leq \dim A$$

So $\dim A = d + m$. Hence, $(x_1, ..., x_n, \tilde{y}_1, ..., \tilde{y}_d)$ is a system of parameters for A
($1 \implies 3$) Choose y_i so that $(x_1, ..., x_m, y_1, ..., y_d)$ is a system of parameters for A, then any element $z + a_1x_1 + ... + a_mx_m \in \mathfrak{m} + (x_1, ..., x_m)$ satisfies $z^k + a_1x_1 + ... + a_mx_m = (z + a_1x_1 + ... + a_mx_m)^k + b_1x_1 + ... + b_mx_m \in (x_1, ..., x_m, y_1, ..., y_d)$ for some k. Hence, $(\bar{y}_1, ..., \bar{y}_d)$ is $\mathfrak{m}$-primary in $A/(x_1, ..., x_m)$ where $\bar{y}_i \in A/(x_1, ..., x_m)$ is the projection of y_i, so $d = \dim A/(x_1, ..., x_m)$. Hence

$$\dim A/(x_1, ..., x_m) = d = \dim A - m$$

$\square$

11.1.2 CONSEQUENCES OF KRULL HEIGHT THEOREM FOR NON-LOCAL RING

Lemma 11.1.10
Let A be Noetherian and $\mathfrak{p} \subseteq A$ be a minimal prime, then any element $x \in \mathfrak{p}$ is a zero divisor.

Proof. If $\mathfrak{p}$ is minimal, then $\dim A_\mathfrak{p} = \operatorname{ht} \mathfrak{p} = 0$, $A_\mathfrak{p}$ is local Noetherian of dimension 0, so it is local Artinian. So, the maximal ideal $\mathfrak{p}A_\mathfrak{p}$ is nilpotent. That is, for any nonzero element $x \in \mathfrak{p}$, let n be the smallest integer so that $x^n = 0$ in $A_\mathfrak{p}$. Hence, $x^n y = 0$ in A for some $y \in A - \mathfrak{p}$. Since $y \neq 0$ and $x^{n-1} \neq 0$ in A, $x(x^{n-1}y) = 0$ implies x is a zero divisor. $\square$

Theorem 11.1.11
Let A be a Noetherian ring and x is a non zero-divisor, then

$$\dim A/(x) \leq \dim A - 1$$

Proof. (Assuming $0 < \dim A$ and $\dim A < +\infty$) Given any maximal chain of primes in $A/(x)$ of strict inclusions

$$\mathfrak{p}_0 \subsetneq ... \subsetneq \mathfrak{p}_n$$

the chain is lifted into a chain of primes in A of strict inclusions

$$\tilde{\mathfrak{p}}_0 \subsetneq ... \subsetneq \tilde{\mathfrak{p}}_n$$

Since $x \in \tilde{\mathfrak{p}}_0$ is a non zero-divisor, hence $\tilde{\mathfrak{p}}_0$ is not a minimal prime, we can extend the lifted chain by the minimal prime contained in $\tilde{\mathfrak{p}}_0$. Hence

$$\dim A/(x) \leq \dim A - 1$$

$\square$

Remark 11.1.12
x being a non zero-divisor is necessary, if not let $A = k[x,y]/(x,y)$ for some field k, then $\dim A = 1$, and $\dim A/(x) = \dim k[y] = 1$

Theorem 11.1.13
Let A be Noetherian, then

$$\dim A[x] = \dim A + 1$$

and

$$\dim A[[x]] = \dim A + 1$$

Proof. *TODO* □

Theorem 11.1.14
Let $A \to B$ be a map of Noetherian rings. Let $\mathfrak{q} \subseteq B$ be a prime ideal and $\mathfrak{p} = \mathfrak{q} \cap A$, then

$$\operatorname{ht} \mathfrak{q} \leq \operatorname{ht} \mathfrak{p} + \dim B_{\mathfrak{q}}/\mathfrak{p}B_{\mathfrak{q}}$$

if going-down theorem holds for $A \to B$, then $\operatorname{ht} \mathfrak{q} = \operatorname{ht} \mathfrak{p} + \dim B_{\mathfrak{q}}/\mathfrak{p}B_{\mathfrak{q}}$

Remark 11.1.15
A local homomorphism of Notherian rings $(A, \mathfrak{m})$ and $(B, \mathfrak{n})$ is a ring map $\phi : A \to B$ so that $\mathfrak{m} = \mathfrak{n} \cap A$, then

$$\dim B \leq \dim A + \dim B/\mathfrak{p}B$$

if the map is flat, then the equality holds.

11.2 REGULAR NOETHERIAN LOCAL RING

11.2.1 AUSLANDER-BUCHSBAUM-SERRE THEOREM

Theorem 11.2.1 (Auslander-Buchsbaum-Serre)
Let $(A, \mathfrak{m}, k)$ be a Noetherian local ring, then the following are equivalent

1. A is regular, that is $\operatorname{embdim} A = \dim A$
2. $\operatorname{projdim}_A k < \infty$
3. $\operatorname{projdim}_A M < \infty$ for every finitely generated A-module M

Moreover, A is regular implies every localization $A_{\mathfrak{p}}$ is regular.

The proof of Auslander-Buchsbaum-Serre theorem, consists the proving the following inequalities assuming $\operatorname{projdim}_A k < +\infty$

$$\dim A \leq \operatorname{embdim} A \leq \operatorname{projdim}_A k = \operatorname{depth}_A A \leq \dim A$$

Definition 11.2.2 (cotangent space, embedding dimension)
Let $(A, \mathfrak{m}, k)$ be a Noetherian local ring, then $\mathfrak{m}/\mathfrak{m}^2$ is a k-vector space and called cotangent space. Define the embedding dimension of A by

$$\operatorname{embdim} A = \dim_k \mathfrak{m}/\mathfrak{m}^2$$

Remark 11.2.3
Embedding dimension of A is also the least [a] number of generators $s \geq 0$ of $\mathfrak{m}$. Since $\mathfrak{m}$ is minimal over itself, by KHT

$$\dim A = \operatorname{ht} \mathfrak{m} \leq s = \operatorname{embdim} A$$

[a] that is also the rank of $\mathfrak{m}$ as an A-module

Proof. A is Noetherian, so $\mathfrak{m}$ is finitely generated. Let s be the least number so that $x_1, ..., x_s$ generates $\mathfrak{m}$, so $\bar{x}_1, ..., \bar{x}_s$ also generates $\mathfrak{m}/\mathfrak{m}^2$, so $\operatorname{embdim} A \leq s$. On the other hand, pick a basis $y_1, ..., y_r$ on the k-vector space $\mathfrak{m}/\mathfrak{m}^2$, by Nakayama lemma, the lifts $\tilde{y}_1, ..., \tilde{y}_r$ also generates $\mathfrak{m}$, hence $\operatorname{embdim} A \geq s$.

□

Definition 11.2.4 (I-depth)
Let I be an ideal in a ring A, then I-depth of an A-module M is defined by the maximal length of a M-regular sequence contained in I, or equivalently

$$\operatorname{depth}_I M = \inf\{i \geq 0 : \operatorname{Ext}^i_A(A/I, M) \neq 0\}$$

When $(A, \mathfrak{m})$ is a Noetherian local, we write $\operatorname{depth}_A M = \operatorname{depth}_{\mathfrak{m}} M$

Remark 11.2.5
If $A = k[[x_1, ..., x_n]]$ for some field k, then $x_1, ..., x_n$ is a A-regular sequence, then

$$\operatorname{depth}_A A \geq n$$

Theorem 11.2.6
Let $(A, \mathfrak{m}, k)$ be a Noetherian local ring, then $\operatorname{depth}_A A \leq \dim A$

Proof. We will prove by induction
base case: If $\dim A = 0$, since A is Noetherian local of dimension 0, A is Artinian local, so $\mathfrak{m}$ is nilpotent, that is, element every element of A must be either a unit or a zero-divisor. We need to show that $\operatorname{depth}_A A = 0$, that is there is no A-regular sequence in A. Suppose there is an A-regular sequence $x_1, ..., x_r$, then x_1 cannot be unit since $A/(x_1, ..., x_r)A \neq 0$. Moreover, x_1 cannot be zero divisor since $x_1 : A \to A$ is injective. So, no A-regular sequence exists in A, hence $\operatorname{depth}_A A = 0$
induction case: when $\dim A = n > 0$, if $\operatorname{depth}_A A = 0$, we are done. If $\operatorname{depth}_A A = r > 0$, pick a maximal A-regular sequence $a_1, a_2, ..., a_r \in A$. Note that, $\frac{A/(a_1)}{(a_2,...,a_i)A/(a_1)} = \frac{A}{(a_1,a_2,...,a_i)}$, so $\frac{A}{(a_1,...,a_r)} \neq 0$ and each $a_i : A/(a_1, ..., a_i) \to A/(a_1, ..., a_i)$ injective imply $\bar{a}_2, ..., \bar{a}_r \in A/(a)$ is a $A/(a)$-regular sequence, then

$$\operatorname{depth}_A A - 1 \leq \operatorname{depth}_{A/(a)} A/(a)$$

Since a is not a zero divisor, $\dim A/(a) \leq \dim A - 1 = n-1$, by induction hypothesis for $A/(a)$

$$\operatorname{depth}_{A/(a)} A/(a) \leq \dim A/(a) \leq \dim A - 1$$

Hence,

$$\operatorname{depth}_A A \leq \dim A$$

□

Theorem 11.2.7 (Auslander–Buchsbaum formula)

Let $(A, \mathfrak{m}, k)$ be a Noetherian local ring and M be a finitely generated module with $\operatorname{projdim}_A M < +\infty$, then

$$\operatorname{projdim}_A M + \operatorname{depth}_A M = \operatorname{depth}_A A$$

In particular, $\operatorname{projdim}_A M < +\infty \implies \operatorname{projdim}_A k = \operatorname{depth}_A A$

Proposition 11.2.8

Let $(A, \mathfrak{m}, k)$ be any Noetherian local ring, let $s = \operatorname{embdim} A$, then

$$\dim_k \operatorname{Tor}_i^A(k,k) \geq \binom{s}{i}$$

for every $i = 0, ..., s$. Recall that

$$\operatorname{projdim}_A M = \sup\{i \geq 0 : \operatorname{Tor}_i^A(M,k) \neq 0\} \leq \operatorname{projdim}_A k$$

Then, $\operatorname{Tor}_i^A(k,k) \neq 0$ for every $i = 0, ..., s$, hence $\operatorname{embdim} A \leq \operatorname{projdim}_A k$

Definition 11.2.9 (Koszul complex)

Let A be a ring and $x_1, ..., x_n \in A$, define the chain complex $K_\bullet = K_\bullet(x_1, ..., x_n; A)$ as follows: for each $p = 0, ..., n$, let

$$K_p = \bigoplus_{i=\{i_1<...<i_p\}} Ae_i$$

where each i is a ordered subset of $\{1, ..., n\}$ of size p, denoted by $i = \{i_1 < ... < i_p\}$. Otherwise, if $p \neq 0, ..., n$, then $K_p = 0$. The differentials are defined by

$$\begin{aligned} d_p : K_p &\to K_{p-1} \\ e_{\{i_1<...<i_p\}} &\mapsto \sum_{r=1}^{p} (-1)^{r-1} e_{\{i_1<...<\hat{i}_r<...<i_p\}} \end{aligned}$$

where $\{i_1 < ... < \hat{i}_r < ... < i_p\} = \{i_1 < ... < i_{r-1} < i_{r+1} < ... < i_p\}$ is the original set dropping i_r

Remark 11.2.10
Let $(A, \mathfrak{m}, k)$ be a Noetherian local ring, $s = \operatorname{embdim} A$ and let $(x_1, ..., x_s) = \mathfrak{m}$, then there exists maps

$$f_\bullet : K_\bullet(x_1, ..., x_s; A) \to L_\bullet$$

realizing K_i as a summand of L_i since $\operatorname{rank} K_i = \binom{s}{i}$

11.2.2 REGULAR IMPLIES FINITE PROJECTIVE DIMENSION

Definition 11.2.11 (regular system of parameters (RSoP))
Let $(A, \mathfrak{m}, k)$ be a regular Noetherian local ring of dimension n, we can choose a system of parameters $x_1, ..., x_n$ generating $\mathfrak{m}$, such a system of parameters is called a regular system of parameters.

Remark 11.2.12
$k[[x_1, ..., x_n]]$ is regular Noetherian local ring with $x_1, ..., x_n$ being a regular system of parameters

Proposition 11.2.13
Let $(A, \mathfrak{m}, k)$ be a regular Noetherian local ring of dimension n, let $x_1, ..., x_i \in \mathfrak{m}$ for $i \le n$, then the following are equivalent

1. $x_1, ..., x_i$ can be extended into a regular system of parameters
2. $\operatorname{im}(x_1, ..., x_i)$ in $\mathfrak{m}/\mathfrak{m}^2$ as a k-vector space are linear independent
3. $A/(x_1, ..., x_i)$ is regular Noetherian local of dimension $n - i$

Theorem 11.2.14
If A is regular Noetherian local ring then A is a domain

Corollary 11.2.15
A regular Noetherian local ring with $x_1, ..., x_n$ being a regular system of parameters, then $x_1, ..., x_n$ is also a A-regular sequence.

Lemma 11.2.16
If $0 \to M_1 \to M_2 \to M_3 \to 0$ is a short exact sequence, then

$$\operatorname{projdim}_A M_3 \le \max\{\operatorname{projdim}_A M_2, 1 + \operatorname{projdim}_A M_1\}$$

11.3 REGULAR NOETHERIAN RING

Definition 11.3.1
A Noetherian ring A is regular if $A_{\mathfrak{p}}$ is regular for every prime $\mathfrak{p}$ if and only if $A_{\mathfrak{m}}$ is regular for every maximal $\mathfrak{m}$

Remark 11.3.2
Some remarks on regular ring

1. if A is regular so are $A[x]$ and $A[[x]]$
2. if A is local, let $\hat{A}$ denote the $\mathfrak{m}$-adic completion, then
$$A \text{ is regular} \iff \hat{A} \text{ is regular}$$
3. if A is local and $\mathfrak{m}$-adic complete, then
$$A \cong R[[x_1, ..., x_n]]/I$$
for R being either a field or discrete valuation ring. Moreover if A is regular, then
$$A \cong R[[x_1, ..., x_n]]$$
this is called Cohen structure theorem

Chapter 12

HOMEWORK 1

Problem 12.0.1 (chapter 1 problem 1)
Let x be a nilpotent element of a ring A. Show that $1 + x$ is a unit of A. Deduce that the sum of a nilpotent element and a unit is a unit.

Proof. Let $x \in \eta_R$, then $-x \in \eta_R$, that is $(-x)^n = 0$ for some $n > 0$. We have

$$1 = 1 - (-x)^n = (1 + x)(1 + (-x) + (-x)^2 + ... + (-x)^{n-1})$$

Hence, $1 + x$ is a unit. Now let $uv = 1$ for $u, v \in R$, we have

$$(u + x)(v + x) = uv + ux + xv + x^2 = 1 + (ux + xv + x^2)$$

Since η_R is an ideal, $ux + xv + x^2 \in \eta_R$, therefore, $1 + (ux + xv + x^2)$ is a unit. Let $w \in R$ be the inverse of $1 + (ux + xv + x^2)$, we have

$$(u + x)(v + x)w = 1$$

Hence, both $u + x$ and $v + x$ are units. □

Problem 12.0.2 (chapter 1 problem 2)
Let A be a ring and let $A[x]$ be the ring of polynomials in an indeterminate x with coefficients in A. Let $f = a_0 + a_1x + ... + a_nx^n \in A[x]$. Prove that

1. f is a unit in $A[x]$ $\iff$ a_0 is a unit in A and $a_1, ..., a_n$ are nilpotent.
2. f is nilpotent $\iff$ $a_0, a_1, ..., a_n$ are nilpotent
3. f is a zero divisor $\iff$ there exists $a \neq 0$ in A such that $af = 0$
4. f is said to be primitive if $(a_0, a_1, ..., a_n) = (1)$. Prove that if $f, g \in A[x]$, then fg is primitive $\iff$ f and g are primitive

Proof.

1. (f is a unit in $A[x]$ $\iff$ a_0 is a unit in A and $a_1, a_2, ..., a_n$ are nilpotent) The statement is true for degree zero polynomials. Suppose $n \geq 1$

   ($\implies$) Let the inverse of $f(x)$ be polynomial $g(x) = b_0 + b_1x + b_2x^2 + ...$ of degree m, that is $b_m \neq 0$ and $b_{m+1} = b_{m+2} = ... = 0$, then $f(x)g(x) = 1$ implies $a_0b_0 = 1$, hence a_0 is a unit. We will show that $a_n^{r+1}b_{m-r} = 0$

for all $r = 0, 1, ..., m$ by induction. The statement is true when $r = 0$ since $a_n b_m = 0$. When $0 < r \le m$, assume that the statement is true for all $0, 1, ..., r-1$, that is

$$a_n b_m = 0$$
$$a_n^2 b_{m-1} = 0$$
$$...$$
$$a_n^r b_{m-r+1} = 0$$

We want to show that $a_n^{r+1} b_{m-r} = 0$. The degree $n + m - r$ coefficient of $f(x)g(x)$ is zero, that is

$$a_n b_{m-r} + a_{n-1} b_{m-r+1} + ... + a_0 b_{m-r+n} = 0$$

Multiply both sides by a_n^r, we have

$$a_n^{r+1} b_{m-r} + a_{n-1} a_n^r b_{m-r+1} + ... + a_0 a_n^r b_{m-r+n} = 0$$

By the induction assumption, we induce that $a_n^{r+1} b_{m-r} = 0$ for all $r = 0, 1, ..., m$. Let $r = m$, then $a_n^{m+1} b_0 = 0$. Since b_0 is a unit, $a_n^{m+1} = 0$, that is, $a_n \in \eta_A$. Note that $a_n \in \eta_{A[x]}$ is also nilpotent in the ring $A[x]$. Therefore, $f(x) - a_n x^n$ is a sum of a unit and a nilpotent element which is a unit in $A[x]$. Hence, using the same proof, $a_{n-1} \in \eta_A$. Inductively, all $a_1, a_2, ..., a_n \in \eta_A$

($\Longleftarrow$) If a_0 is a unit and $a_1, ..., a_n \in \eta_A$, then a_0 is also a unit in $A[x]$ and $a_1 x, ..., a_n x^n \in \eta_{A[x]}$. Therefore, $f(x) = a_0 + a_1 x + ... + a_n x^n$ is a sum of a unit and a nilpotent element which is a unit in $A[x]$

2. (f is nilpotent $\iff$ $a_0, a_1, ..., a_n$ are nilpotent)

   ($\Longrightarrow$) If $f(x)$ is nilpotent, $1 + f(x) = (1 + a_0) + a_1 x + a_2 x^2 + ...$ is a unit. Then, $1 + a_0$ is a unit and $a_1, ..., a_n \in \eta_A$. Moreover, $f(x)^m = 0$ for some $m > 0$. That implies $a_0^m = 0$ for some $m > 0$. Hence, a_0 is also nilpotent.

   ($\Longleftarrow$) If $a_0, a_1, ..., a_n \in \eta_A$, then $a_0^m = a_1^m = ... = a_n^m = 0$ for some $m > 0$. $f(x)^{(n+1)m}$ is a sum of terms, where each term is a product of $(n+1)m$ elements from the set

   $$\{a_0, a_1 x, ..., a_n x^n\}$$

   By pigeonhole principle, for every term, there is an element appearing at least m times. Hence, $f(x)^{(n+1)m}$ is a zero polynomial, that is, $f(x) \in \eta_{A[x]}$

3. (f is a zero divisor $\iff$ there exists $a \neq 0$ in A such that $af = 0$)

   ($\Longrightarrow$) Let $g(x) = b_0 + b_1 x + b_2 x^2 + ... \in A[x]$ such that $f(x)g(x) = 0$. The degree zero term of $f(x)g(x)$ is zero, that is, $a_0 b_0 = 0$, we will show that $a_r b_0^{r+1} = 0$ for all r by induction. Suppose the statement is true for all $0, 1, ..., r-1$, that is

   $$a_0 b_0 = 0$$
   $$a_1 b_0^2 = 0$$
   $$...$$
   $$a_{r-1} b_0^r = 0$$

We want to show that $a_r b_0^{r+1} = 0$. The degree r coefficient of $f(x)g(x)$ is zero, that is

$$a_0 b_r + a_1 b_{r-1} + ... + a_r b_0 = 0$$

Multiply both sides by b_0^r, we have

$$a_0 b_0^r b_r + a_1 b_0^r b_{r-1} + ... + a_r b_0^{r+1} = 0$$

By the induction assumption, we induce that $a_r b_0^{r+1} = 0$ for all r. Then, $f(x) b_0^{n+1} = 0$

($\Longleftarrow$) by the premise

4. (if $f, g \in A[x]$, then fg is primitive $\iff$ f and g are primitive)

($\Longrightarrow$) Let $g(x) = b_0 + b_1 x + ... + b_m x^m$. If $f(x)g(x)$ is primitive, then

$$1 = c_0(a_0 b_0) + c_1(a_0 b_1 + a_1 b_0) + c_2(a_0 b_2 + a_1 b_1 + a_2 b_0) + ... + c_{n+m}(a_n b_m)$$

for some $c_0, c_1, ..., c_{n+m} \in A$. Hence, 1 can be written as a linear combination of the finite set $\{a_0, a_1, ..., a_n\}$ with coefficients in A, that is $f(x)$ is primitive. Similarly, $g(x)$ is also primitive.

($\Longleftarrow$) Suppose $f(x)g(x)$ is not primitive, let the maximal ideal containing the ideal generated by coefficients of $f(x)g(x)$ be $\mathfrak{m}$. Then, in $(A/\mathfrak{m})[x]$, $0 = \overline{f(x)g(x)} = \overline{f(x)}\ \overline{g(x)}$. Since $\mathfrak{m}$ is maximal that is prime, $A/\mathfrak{m}$ is a domain, then $(A/\mathfrak{m})[x]$ is a domain. On the other hand, $f(x)$ is primitive, then the coefficients of $f(x)$ generate the whole ring A, therefore, there exists an $a_i \notin \mathfrak{m}$, if not $A = (a_0, a_1, ..., a_n) \subseteq \mathfrak{m}$. Hence, $\overline{f(x)} \neq 0$ in $(A/\mathfrak{m})[x]$. Similarly, $\overline{g(x)} \neq 0$ in $(A/\mathfrak{m})[x]$. This contradicts with $(A/\mathfrak{m})[x]$ being a domain.

□

Problem 12.0.3 (chapter 1 problem 8)
Let A be a ring $\neq 0$. Show that the set of prime ideals of A has minimal elements with respect to inclusion.

Proof. The collection of prime ideals of A is a partially ordered set with respect to inclusion. Moreover, given any chain of prime ideals $\{\mathfrak{p}_i : i \in I\}$ under inclusion, the intersection $\mathfrak{p} = \bigcap_{i \in I} \mathfrak{p}_i$ is a prime ideal and a lowerbound (note that, this is only true for arbitrary collection of prime ideals. (2) and (3) are prime in $\mathbb{Z}$ but $(6) = (2) \cap (3)$ is not prime). Suppose, $xy \in \mathfrak{p}$ but $x \notin \mathfrak{p}$ and $y \notin \mathfrak{p}$. Let $x \notin \mathfrak{p}_x$ and $y \notin \mathfrak{p}_y$. Since the collection is a chain, without loss of generality, assume $\mathfrak{p}_x \subseteq \mathfrak{p}_y$. Therefore, both $x, y \notin \mathfrak{p}_x$ but $xy \in \mathfrak{p} \subseteq \mathfrak{p}_x$. Contradiction. Thus, $\mathfrak{p}$ is prime. By Zorn lemma, there is a minimal prime ideal. □

Problem 12.0.4 (chapter 1 problem 10)
Let A be a ring, η_A is its nilradical. Show that the following are equivalent:

1. A has exactly one prime ideal
2. every element of A is either a unit or nilpotent.
3. A/η_A is a field

Proof.
$(1 \implies 2)$ If A has exactly one prime ideal, namely η_A the intersection of all prime ideals. Since any maximal ideal is prime, η_A is the unique maximal ideal in A. Therefore, any element $x \in A$, if $x \in \eta_A$ then x is nilpotent, if $x \notin \eta_A$ and x is a not unit then x is contained in a maximal ideal other than η_A. Contradiction.

($2 \implies 3$) If $\bar{x} \in A/\eta_A$ is non-zero for some $x \in A$, then $x \notin \eta_A$, thus x is a unit, hence $\bar{x}$ is a unit. Therefore, A/η_A is a field.
($3 \implies 1$) A/η_A is a field, then η_A is maximal. Since η_A is the intersection of all prime ideals, but it is maximal, it can not be a proper subset of any ideal. Hence, η_A is the unique prime ideal of A □

Problem 12.0.5 (chapter 1 problem 12)
A local ring contains no idempotent $\neq 0, 1$

Proof. Let A be a local ring with $\mathfrak{m}$ be its unique maximal ideal. Suppose $a \neq 0, 1$ such that $a^2 = a$, then $a(a-1) = a^2 - a = 0$, that is, a and $a-1$ are zero divisors. Since a and $a-1$ are not a unit, $a, a-1 \in \mathfrak{m}$ but $1 = a - (a-1) \notin \mathfrak{m}$ which is a contradiction. □

Problem 12.0.6 (chapter 1 problem 15 - Zariski topology)
Let A be a ring and let X be the set of all prime ideals of A. For each subset E of A, let $V(E)$ denote the set of all prime ideals of A which contain E. Prove that

1. if $\mathfrak{a}$ is the ideal generated by E, then $V(E) = V(\mathfrak{a}) = V(\sqrt{\mathfrak{a}})$
2. $V(0) = X, V(1) = \varnothing$
3. if $(E_i)_{i \in I}$ is any family of subsets of A, then
$$V\left(\bigcup_{i \in I} E_i\right) = \bigcap_{i \in I} V(E_i)$$
4. $V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}\mathfrak{b}) = V(\mathfrak{a}) \cup V(\mathfrak{b})$ for any ideals $\mathfrak{a}, \mathfrak{b}$ of A

Proof.

1. (if $\mathfrak{a}$ is the ideal generated by E, then $V(E) = V(\mathfrak{a}) = V(\sqrt{\mathfrak{a}})$)

   Since $E \subseteq \mathfrak{a}$, $V(E) \supseteq V(\mathfrak{a})$. By definition of ideal generated by set, $\mathfrak{a}$ is the smallest ideal containing E, therefore any prime ideal containing E must contain $\mathfrak{a}$, hence $V(E) \subseteq V(\mathfrak{a})$.

   Since $\mathfrak{a} \subseteq \sqrt{\mathfrak{a}}$, $V(\mathfrak{a}) \supseteq V(\sqrt{\mathfrak{a}})$. We want to show the other direction $V(\mathfrak{a}) \subseteq V(\sqrt{\mathfrak{a}})$, that is any prime ideal containing $\mathfrak{a}$ must contain $\sqrt{\mathfrak{a}}$. Let $\mathfrak{b} \supseteq \mathfrak{a}$ be a prime ideal, for any element, $x \in \sqrt{\mathfrak{a}}$, $x^n \in \mathfrak{a} \subseteq \mathfrak{b}$ for some $n > 0$.Then, $xx^{n-1} \in \mathfrak{b}$ therefore, either $x \in \mathfrak{b}$ or $x^{n-1} \in \mathfrak{b}$. The induction argument on n implies $x \in \mathfrak{b}$. Hence, $\mathfrak{b} \supseteq \sqrt{\mathfrak{a}}$

2. ($V(0) = X, V(1) = \varnothing$)

   Every prime ideal contains 0, hence $V(0) = X$. Every prime ideal is proper, hence it cannot contain 1, then $V(1) = \varnothing$

3. ($V\left(\bigcup_{i \in I} E_i\right) = \bigcap_{i \in I} V(E_i)$)

   Let $\mathfrak{a}$ be an ideal. Then,

   $\mathfrak{a} \in V\left(\bigcup_{i \in I} E_i\right) \iff \mathfrak{a} \supseteq E_i$ for all $i \in I \iff \mathfrak{a} \in V(E_i)$ for all $i \in I \iff \mathfrak{a} \in \bigcap_{i \in I} V(E_i)$

4. ($V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}\mathfrak{b}) = V(\mathfrak{a}) \cup V(\mathfrak{b})$ for any ideals $\mathfrak{a}, \mathfrak{b}$ of A)

Note that, if $E, F \subseteq A$, then $E \subseteq F \implies V(E) \supseteq V(F)$. Since $\mathfrak{ab} \subseteq \mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{a}$, then

$$V(\mathfrak{ab}) \supseteq V(\mathfrak{a} \cap \mathfrak{b}) \supseteq V(\mathfrak{a}) \cup V(\mathfrak{b})$$

We will show that $V(\mathfrak{ab}) \subseteq V(\mathfrak{a}) \cup V(\mathfrak{b})$. Suppose $\mathfrak{p} \in V(\mathfrak{ab})$ but $\mathfrak{p} \notin V(\mathfrak{a}) \cup V(\mathfrak{b})$. $\mathfrak{p} \notin V(\mathfrak{a})$ implies there exists $a \in \mathfrak{a}$ such that $a \notin \mathfrak{p}$. $\mathfrak{p} \notin V(\mathfrak{b})$ implies there exists $b \in \mathfrak{b}$ such that $b \notin \mathfrak{p}$. But $ab \in \mathfrak{ab} \subseteq \mathfrak{p}$. This is a contradiction since $\mathfrak{p}$ is prime.

□

Problem 12.0.7 (chapter 1 problem 17 - a basis for Zariski topology)
For each $f \in A$, let X_f denote the complement of $V(f)$ in $X = \operatorname{Spec} A$. The set X_f are open. Show that they form a basis of open sets for the Zariski topology, and that

1. $X_f \cap X_g = X_{fg}$
2. $X_f = \varnothing \iff f$ is nilpotent
3. $X_f = X \iff f$ is a unit
4. $X_f = X_g \iff \sqrt{(f)} = \sqrt{(g)}$
5. X is quasi-compact
6. each X_f is quasi-compact
7. an open subset of X is quasi-compact if and only if it is a finite union of set X_f

Proof.
(X_f form a basis for Zariski topology) Given any ideal I, the open set $X - V(I)$ can be written as a union of X_f

$$X - V(I) = X - \bigcap_{f \in I} V(f) = \bigcup_{f \in I} (X - V(f)) = \bigcup_{f \in I} X_f$$

1. ($X_f \cap X_g = X_{fg}$)

$$\begin{aligned} X_f \cap X_g &= (X - V(f)) \cap (X - V(g)) \\ &= X - (V(f) \cup V(g)) \\ &= X - (V((f)) \cup V((g))) \\ &= X - V((fg)) \\ &= X - V(fg) \\ &= X_{fg} \end{aligned}$$

2. ($X_f = \varnothing \iff f$ is nilpotent)

$$X_f = \varnothing \iff V(f) = X \iff f \in \mathfrak{p} \text{ for every prime ideal } \mathfrak{p} \iff f \in \eta_A$$

3. ($X_f = X \iff f$ is a unit)

$$X_f = X \iff V(f) = \varnothing \iff f \notin \mathfrak{m} \text{ for every maximal ideal } \mathfrak{m} \iff f \text{ is a unit}$$

The last $\iff$ is true because f is a unit implies f is not in any maximal ideal and f is not a unit implies f is contained in some maximal ideal.

4. $(X_f = X_g \iff \sqrt{(f)} = \sqrt{(g)})$

$$X_f = X_g \iff V(f) = V(g) \iff V((f)) = V((g))$$

By definition, $\sqrt{(f)} = \bigcap_{\mathfrak{p} \in V((f))} \mathfrak{p}$ and $\sqrt{(g)} = \bigcap_{\mathfrak{p} \in V((g))} \mathfrak{p}$, then

$$V((f)) = V((g)) \implies \sqrt{(f)} = \sqrt{(g)}$$

On the other hand,

$$\sqrt{(f)} = \sqrt{(g)} \implies V(\sqrt{(f)}) = V(\sqrt{(g)}) \implies V((f)) = V((g))$$

5. (X is quasi-compact)

It is sufficient to prove that given any open cover by basic open sets $\{X_{f_i}\}_{i \in I}$, then there exists a finite subcover $\{X_{f_j}\}_{j \in J}$ for finite subset $J \subseteq I$. We have

$$\bigcup_{i \in I} X_{f_i} = \bigcup_{i \in I} (X - V(f_i)) = X - \bigcap_{i \in I} V(f_i)$$

That is, $\bigcup_{i \in I} X_{f_i} = X \iff \bigcap_{i \in I} V(f_i) = \varnothing$. Moreover,

$$\bigcap_{i \in I} V(f_i) = \varnothing \iff \text{there is no prime ideal containing } \{f_i\}_{i \in I} \iff (f_i)_{i \in I} = A$$

where $(f_i)_{i \in I}$ denotes the ideal generated by $\{f_i\}_{i \in I}$. The second $\iff$ is due to every prime ideal is contained is a maximal ideal. Then, $(f_i)_{i \in I} = A$ implies

$$1 = \sum_{j \in J} a_j f_j$$

for some finite subset $J \subseteq I$. Hence, $(f_j)_{j \in J} = A$. That implies $\bigcup_{j \in J} X_{f_j} = X$ by the same argument for index set J

6. (each X_f is quasi-compact)

Let $\{X_{f_i}\}_{i \in I}$ be an open cover for X_f by basic open sets. We have

$$X_f \subseteq \bigcup_{i \in I} X_{f_i} \iff V(f) \supseteq \bigcap_{i \in I} V(f_i) = V((f_i)_{i \in I})$$

If $\bigcap_{i \in I} V(f_i) = \varnothing$, this falls back to the previous case. Suppose $V((f_i)_{i \in I}) = \bigcap_{i \in I} V(f_i) \neq \varnothing$, we have

$$\mathfrak{p} \in V((f_i)_{i \in I}) \implies \mathfrak{p} \in V(f) \implies f \in \mathfrak{p}$$

Therefore

$$f \in \sqrt{(f_i)_{i \in I}} = \bigcap_{\mathfrak{p} \in V((f_i)_{i \in I})} \mathfrak{p}$$

That is, $f^n \in (f_i)_{i \in I}$ for some $n > 0$, then

$$f^n = \sum_{j \in J} a_j f_j$$

for some finite subset $J \subseteq I$. As $f^n \in (f_j)_{j \in J}$, then $V(f^n) \supseteq V((f_j)_{j \in J})$, we have

$$\mathfrak{p} \in V((f_j)_{j \in J}) \implies \mathfrak{p} \in V(f^n) \implies f^n \in \mathfrak{p}$$

Since $\mathfrak{p}$ is prime, $f^n \in \mathfrak{p} \implies f \in \mathfrak{p}$. Therefore,

$$\mathfrak{p} \in V((f_j)_{j \in J}) \implies \mathfrak{p} \in V(f^n) \implies f^n \in \mathfrak{p} \implies f \in \mathfrak{p} \implies \mathfrak{p} \in V(f)$$

Thus, $V(f) \supseteq V((f_j)_{j \in J})$, that is, X_f is covered by a finite subcollection

$$X_f \subseteq \bigcup_{j \in J} X_{f_j}$$

7. (an open subset of X is quasi-compact if and only if it is a finite union of set X_f)

   ($\Longleftarrow$) finite union of quasi-compact sets is quasi-compact since we can pick a finite subcollection for each set, the total is still a finite subcollection.

   ($\implies$) if U is an open set in X, then U can be written as $U = \bigcup_{i \in I} X_{f_i}$ since $\{X_f\}$ form a basis for X. By compactness of U, U can be cover by a finite union $U \subseteq \bigcup_{j \in J} X_{f_j} \subseteq \bigcup_{i \in I} X_{f_i} = U$. Hence, $U = \bigcup_{j \in J} X_{f_j}$

$\square$

Problem 12.0.8 (chapter 2 problem 9)
Let $0 \longrightarrow A \xhookrightarrow{i} B \xrightarrow{p} C \longrightarrow 0$ be an exact sequence of R-modules. If A and C are finitely generated, then so is B

Proof. If $b \in \ker p = \operatorname{im} i$, since i is injective, we can write $i^{-1}(b) = r_1 a_1 + r_2 a_2 + ... + r_n a_n$ where $\{a_1, a_2, ..., a_n\}$ generates A and $r_1, r_2, ..., r_n \in R$. Therefore,

$$b = r_1 i(a_1) + r_2 i(a_2) + ... + r_n i(a_n)$$

That is, $\{i(a_1), i(a_2), ..., i(a_n)\}$ generates $\ker p$. Let $\{c_1, c_2, ..., c_m\}$ generates C. Since p is surjective, pick $\{b_1, b_2, ..., b_m\} \subseteq B$ so that $p(b_i) = c_i$ for all $i = 1, 2, ..., m$. Now, if $b \in B - \ker p$, we can write

$$p(b) = s_1 c_1 + s_2 c_2 + ... + s_m c_m$$

for some $s_1, s_2, ..., s_m \in R$. Let

$$b' = s_1 b_1 + s_2 b_2 + ... + s_m b_m$$

Then, $p(b - b') = 0$, that is, $b - b' \in \ker p$, hence $b - b'$ can be written as a linear combination of $\{i(a_1), i(a_2), ..., i(a_n)\}$. Thus, the set $\{i(a_1), i(a_2), ..., i(a_n)\} \cup \{b_1, b_2, ..., b_m\}$ generates B $\square$

Problem 12.0.9 (chapter 2 problem 10)
Let A be a ring and $\mathfrak{a}$ be an ideal contained in the Jacobson radical of A. Let M be an A-module and N be finitely generated A-module, let $u : M \to N$ be a homomorphism. If the induced homomorphism $M/\mathfrak{a}M \to N/\mathfrak{a}N$ is surjective, then u is surjective

Proof. We will show that $N = \mathfrak{a}N + \operatorname{im} u$ so that Nakayama lemma version 2 implies $N = \operatorname{im} u$. Let $\{y_1, y_2, ..., y_n\}$ generates N, then $\{y_1 + \mathfrak{a}N, y_2 + \mathfrak{a}N, ..., y_n + \mathfrak{a}N\}$ generates $N/\mathfrak{a}N$. For each $i = 1, 2, ..., n$, since $u^* : M/\mathfrak{a}M \to N/\mathfrak{a}N$ is surjective, there is $x_i \in M$ such that

$$u^*(x_i + \mathfrak{a}M) = y_i + \mathfrak{a}N$$

That is, $z_i = u(x_i) - y_i \in \mathfrak{a}N$. Now, for each $y \in N$, we have

$$y = \sum_{i=1}^{n} a_i y_i = \sum_{i=1}^{n} a_i (u(x_i) - z_i)$$

for some $a_1, a_2, ..., a_n \in A$. $\mathfrak{a}N + \operatorname{im} u$ being a submodule of N and $u(x_i) - z_i \in \mathfrak{a}N + \operatorname{im} u$ implies $a_i(u(x_i) - y_i) \in \mathfrak{a}N + \operatorname{im} u$. Hence, $y \in \mathfrak{a}N + \operatorname{im} u$. Thus, $N \subseteq \mathfrak{a}N + \operatorname{im} u \subseteq N$, hence $N = \mathfrak{a}N + \operatorname{im} u$ ☐

Problem 12.0.10 (chapter 2 problem 12)
Let M be a finitely generated A-module and $\phi : M \to A^n$ a surjective homomorphism. Show that $\ker \phi$ is finitely generated.

Proof. Since $\phi : M \to A^n$ is surjective, the first row is exact

$$\begin{tikzcd}
0 \arrow[r] & \ker\phi \arrow[r, hook] & M \arrow[r, two heads, "\phi"] & A^n \arrow[r] & 0 \\
& & & A^n \arrow[u, "1_{A^n}"'] \arrow[ul, dashed, "\psi"] &
\end{tikzcd}$$

A^n is projective since it is free, hence the map $1_{A^n} : A^n \to A^n$ factors through the surjective map $M \to A^n$ by a map $\psi : A^n \to M$. In particular, let $e_1, e_2, ..., e_n$ be the canonical basis for A^n, for each e_i pick $u_i \in M$ such that $\phi(u_i) = e_i$. Define the map $\psi : A^n \to M$ by

$$\psi : A^n \to M$$
$$e_i \mapsto u_i$$

so that $\phi\psi = 1_{A^n}$. Thus, the sequence splits, by Five lemma, there is an isomorphism $f : M \to \ker\phi \oplus A^n$. Both M and A^n being finitely generated, so is $\ker\phi$.
Indeed, if $f : M \to N \oplus P$ is an isomorphism with M and N being finitely generated. Let $\{x_1, x_2, ..., x_m\}$ generate M and $\{y_1, y_2, ..., y_n\}$ generate N. For each $i = 1, 2, ..., m$, then

$$f(x_i) = \left(\sum_{j=1}^{n} a_j y_j, p_i \right)$$

for some $a_1, a_2, ..., a_n \in A$ and $p_i \in P$. Let $p \in P$, then there are some $b_1, b_2, ..., b_m \in A$ such that

$$f\left(\sum_{i=1}^{m} b_i x_i \right) = (0, p)$$

Then,

$$(0, p) = f\left(\sum_{i=1}^{m} b_i x_i \right) = \sum_{i=1}^{m} b_i f(x_i) = \sum_{i=1}^{m} b_i \left(\sum_{j=1}^{n} a_j y_j, p_j \right) = \left(\sum_{i=1}^{m} \sum_{j=1}^{n} b_i a_j y_j, \sum_{i=1}^{m} b_i p_i \right)$$

Thus, $\{p_1, p_2, ..., p_m\}$ generates P. ☐

Problem 12.0.11 (chapter 3 problem 5)
Let A be a ring. Suppose that for each prime ideal $\mathfrak{p}$, the local ring $A_\mathfrak{p}$ has no nilpotent element $\neq 0$. Show that A has no nilpotent element $\neq 0$. If each $A_\mathfrak{p}$ is an integral domain, is A necessarily an integral domain?

Proof.
(A has no nilpotent element $\neq 0$) Suppose $x \in A$ such that $x \neq 0$ and $x^n = 0$ for some $n > 0$. The ideal $(\{a \in A : ax = 0\})$ is proper since if $r_1a_1 + r_2a_2 + ... + r_ma_m = 1$, then $0 = r_1a_1x + r_2a_2x + ... + r_ma_mx = x$. Let $\mathfrak{p}$ be the maximal ideal of A containing $(\{a \in A : ax = 0\})$. For any $s \in A - \mathfrak{p}$, $\frac{x}{s}$ is nilpotent in $A_\mathfrak{p}$ since

$$\left(\frac{x}{s}\right)^n = \frac{x^n}{s^n} = \frac{0}{s^n} = \frac{0}{1} = 0$$

Moreover, $\frac{x}{s} \neq 0$ in $A_\mathfrak{p}$ since if $\frac{x}{s} = 0$ in $A_\mathfrak{p}$, then there exists $t \in A - \mathfrak{p}$ so that $tx = 0$, by construction of $\mathfrak{p}$, this is a contradiction.
(If each $A_\mathfrak{p}$ is an integral domain, is A necessarily an integral domain?) Let $A = \mathbb{Z}_6$, $\mathbb{Z}_6$ is not a domain since $2 \times 3 = 0 \mod 6$. The prime ideals of $\mathbb{Z}_6$ are $\{(2), (3)\}$, we have

$$S_2 = \mathbb{Z}_6 - (2) = \{1, 3, 5\}$$
$$S_3 = \mathbb{Z}_6 - (3) = \{1, 2, 4, 5\}$$

The zeros in $S_2^{-1}A$ are a/s where $s \in S_2$ and $a \in \mathbb{Z}_6$ such that $ta = 0 \mod 6$ for $t \in S_2$, that is

$$\left\{\frac{0}{s}, \frac{2}{s}, \frac{4}{s} : s \in S\right\}$$

The zeros in $S_3^{-1}A$ are a/s where $s \in S_3$ and $a \in \mathbb{Z}_6$ such that $ta = 0 \mod 6$ for $t \in S_3$, that is

$$\left\{\frac{0}{s}, \frac{3}{s} : s \in S\right\}$$

In $S_2^{-1}A$, if $\frac{a}{s}\frac{b}{r} = \frac{ab}{sr} = 0$, then $ab \in \{0, 2, 4\}$. Hence one of a or b must be in $\{0, 2, 4\}$. In In $S_3^{-1}A$, if $\frac{a}{s}\frac{b}{r} = \frac{ab}{sr} = 0$, then $ab \in \{0, 3\}$. Hence one of a or b must be in $\{0, 3\}$. Thus, both $S_2^{-1}A$ and $S_3^{-1}A$ are domain but A is not. ☐

Problem 12.0.12 (chapter 3 problem 6)
Let A be a ring $\neq 0$ and let Σ be the set of all multiplicatively closed subsets S of A such that $0 \notin S$. Show that Σ has maximal elements and that $S \in \Sigma$ is maximal if and only if $A - S$ is a minimal ideal of A.

Proof. As Σ forms a partially ordered set under inclusion and union of arbitrary number of sets in Σ is also in Σ. By Zorn lemma, Σ has a maximal element. Let $S \in \Sigma$, there is a minimal prime ideal $\mathfrak{p}_S$ in the ring $S^{-1}R$, let $\mathfrak{p}$ be the extension of $\mathfrak{p}_S$ in R so that $\mathfrak{p} \cap S = \varnothing$. Since $\mathfrak{p}$ is prime, $A - \mathfrak{p}$ is a multiplicatively closed that that contains S.
($S \in \Sigma$ is maximal $\implies A - S$ is a minimal prime ideal of A)
By maximality of S, $S = A - \mathfrak{p}$. Suppose there is a prime ideal $\mathfrak{q}$ contained properly in $\mathfrak{p}$, the contraction $\mathfrak{q}^c$ of $\mathfrak{q}$ is contained (not necessarily proper) in the contraction $\mathfrak{p}^c = \mathfrak{p}_S$ of $\mathfrak{p}$. As $\phi_S : \operatorname{Spec} S^{-1}R \to \operatorname{Spec} R$ is injective, the containment is proper, $\mathfrak{q}^c \subsetneq \mathfrak{p}_S$, this contradicts the minimality of $\mathfrak{p}_S$. Hence, $\mathfrak{p} = A - S$ is minimal in A
($S \in \Sigma$ is maximal $\impliedby A - S$ is a minimal prime ideal of A)
S is contained in a maximal multiplicatively closed set S_1 in Σ. Then, $A - S_1$ is a minimal prime ideal of A. Suppose S is a proper subset of S_1, then the minimal prime ideal $A - S$ contains properly a smaller prime ideal $A - S_1$, that is a contradiction. ☐

Chapter 13

HOMEWORK 2

Problem 13.0.1 (chapter 2 problem 1)
Show that $\frac{\mathbb{Z}}{m\mathbb{Z}} \otimes_{\mathbb{Z}} \frac{\mathbb{Z}}{n\mathbb{Z}} = 0$ if m, n are coprime

Proof. If m, n are coprime, $m\mathbb{Z} + n\mathbb{Z} = \mathbb{Z}$ as sum of ideals in $\mathbb{Z}$

$$\frac{\mathbb{Z}}{m\mathbb{Z}} \otimes_{\mathbb{Z}} \frac{\mathbb{Z}}{n\mathbb{Z}} = \frac{\mathbb{Z}}{m\mathbb{Z} + n\mathbb{Z}} = \frac{\mathbb{Z}}{\mathbb{Z}} = 0$$

□

Problem 13.0.2 (chapter 2 problem 2)
Let A be a ring, $\mathfrak{a}$ be an ideal of A and M be an A-module. Show that $A/\mathfrak{a} \otimes_A M$ is isomorphic to $M/\mathfrak{a}M$

Proof. The top sequence is exact with the canonical inclusion and projection. By right exactness of tensor product, the bottom sequence is also exact

$$\begin{tikzcd} 0 \arrow[r] & \mathfrak{a} \arrow[r, hook, "i"] & A \arrow[r, two heads, "p"] & A/\mathfrak{a} \arrow[r] & 0 \end{tikzcd}$$

$$\begin{tikzcd} \mathfrak{a} \otimes M \arrow[r, "i\otimes 1"] & A \otimes M \arrow[r, two heads] & A/\mathfrak{a} \otimes M \arrow[r] & 0 \end{tikzcd}$$

Then, $A/\mathfrak{a} \otimes M \cong \operatorname{coker}(i \otimes 1)$. On the other hand, $A \otimes M \xrightarrow{\sim} M$ and the image of $\mathfrak{a} \otimes M$ in M under $i \otimes 1$ is $\mathfrak{a}M$

$$\begin{tikzcd} \mathfrak{a} \otimes M \arrow[r, "i\otimes 1"'] \arrow[rr, bend left, "i\otimes 1"] & A \otimes M \arrow[r, "\sim"] & M \end{tikzcd}$$

$$\sum_i a_i \otimes m_i \longmapsto \sum_i a_i \otimes m_i \longmapsto \sum_i a_i m_i$$

Hence, $\operatorname{coker}(i \otimes 1) = \frac{A \otimes M}{(i\otimes 1)(\mathfrak{a} \otimes M)} \cong \frac{M}{\mathfrak{a}M}$ □

Problem 13.0.3 (chapter 2 problem 3)
Let A be a local ring, M and N be finitely generated A-modules. Prove that if $M \otimes_A N = 0$, then $M = 0$ or $N = 0$

Proof. Let $\mathfrak{m}$ be an ideal of A and $k = A/\mathfrak{m}$. If $M \otimes_A N = 0$, then

$$0 = (M \otimes_A N) \otimes_A k \otimes_A k \cong (k \otimes_A M) \otimes_A (k \otimes_A N)$$

By exercise 2, $k \otimes_A M \cong M/\mathfrak{m}M = M_k$ and $k \otimes_A N \cong N/\mathfrak{m}N = N_k$, then

$$M_k \otimes_A N_k = 0$$

Note that, given any ring A ideal $\mathfrak{a}$ and an $A/\mathfrak{a}$-module M, then M also carries A-module structure defined by

$$\begin{aligned} A \times M &\to M \\ (a, m) &\mapsto \bar{a}m \end{aligned}$$

$M_k \otimes_k N_K \cong M_k \otimes_A N_k$ by the following A-module isomorphism

$$\begin{aligned} M_k \otimes_k N_K &\xrightarrow{\sim} M_k \otimes_A N_k \\ \bar{x} \otimes_k \bar{y} &\mapsto \bar{x} \otimes_A \bar{y} \end{aligned}$$

Hence, $M_k \otimes_k N_k = 0$. Let $\mathfrak{m}$ be the unique maximal ideal of the local ring A, then k is a field, hence $M_k = 0$ or $N_k = 0$. By Nakayama lemma version 1, $\mathfrak{m} \subseteq J(A)$, $\mathfrak{m}M = M$ or $\mathfrak{m}N = 0$ implies $M = 0$ or $N = 0$ ☐

Problem 13.0.4 (chapter 2 problem 8)

.

1. If M and N are flat A-modules, then so is $M \otimes_A N$
2. If B is a flat A-algebra and N is a flat B-module, then N is a flat as an A-module

Proof.
(1) Let $f : X \to Y$ be an injective A-module morphism and f_1 be the induced map by the functor $((- \otimes_A M) \otimes_A N)$. Let f_2 be the induced map by the functor $(- \otimes_A (M \otimes_A N))$. There is a natural isomorphism $g : ((- \otimes_A M) \otimes_A N) \to (- \otimes_A (M \otimes_A N))$ as follows:

$$\begin{tikzcd}
(X \otimes_A M) \otimes_A N \arrow[rrr, "f_1"] \arrow[ddd, "g_X"'] & & & (Y \otimes_A M) \otimes_A N \arrow[ddd, "g_Y"] \\
& (x \otimes m) \otimes n \arrow[r, mapsto] \arrow[d, mapsto] & (f(x) \otimes m) \otimes n \arrow[d, mapsto] & \\
& x \otimes (m \otimes n) \arrow[r, mapsto] & f(x) \otimes (m \otimes n) & \\
X \otimes_A (M \otimes_A N) \arrow[rrr, "f_2"] & & & Y \otimes_A (M \otimes_A N)
\end{tikzcd}$$

The square commutes since

$$\begin{aligned} g_Y f_1((x \otimes m) \otimes n) &= g_Y((f(x) \otimes m) \otimes n) = f(x) \otimes (m \otimes n) \\ f_2 g_X((x \otimes m) \otimes n) &= f_2(x \otimes (m \otimes n)) = f(x) \otimes (m \otimes n) \end{aligned}$$

for all $x \in X, m \in M, n \in N$. f_1 being injective implies f_2 being injective. Hence $M \otimes_A N$ is flat.

(2) Note that B and N are (A,B)-bimodules, hence given any A-module M

$$M \otimes_A N \cong M \otimes_A (B \otimes_B N) \cong (M \otimes_A B) \otimes_B N$$

We will show the following: (2a) $(-\otimes_A B)$ is an exact functor from A-module into (A,B)-bimodule (2b) $((-\otimes_A B)\otimes_B N)$ is an exact functor from A-module into (A,B)-bimodule (2c) $((- \otimes_A B) \otimes_B N)$ is naturally isomorphic to $(- \otimes_A N)$
(2a) Let $f : X \to Y$ be an injective A-module morphism and f_1 be the induced A-module map by the functor $(- \otimes_A B)$

$$\begin{aligned} f &: X \to Y \\ f_1 &: X \otimes_A B \to Y \otimes_A B \end{aligned}$$

$X \otimes_A B$ and $Y \otimes_A B$ canonically carry B-module structure (extension of scalars under the map $a \mapsto a1_B$) defined by

$$\begin{aligned} B \times (X \otimes_A B) &\to X \otimes_A B \\ (b_1, x \otimes_A b) &\mapsto x \otimes_A b_1 b \end{aligned}$$

Under that B-module structure, f_1 is also a B-module map because

$$f_1(b_1(x \otimes_A b)) = f_1(x \otimes_A b_1 b) = f(x) \otimes_A b_1 b = b_1(f(x) \otimes_A b) = b_1 f_1(x \otimes_A b)$$

Since B is flat as an A-module, f_1 as an A-module map is injective, so is f_1 as an (A,B)-bimodule map. Hence, $(- \otimes_A B)$ is an exact functor from A-module into (A,B)-bimodule
(2b) Let f_2 be the induced B-module map by the functor $((- \otimes_A B) \otimes_B N)$

$$\begin{aligned} f &: X \to Y \\ f_1 &: X \otimes_A B \to Y \otimes_A B \\ f_2 &: (X \otimes_A B) \otimes_B N \to (Y \otimes_A B) \otimes_B N \end{aligned}$$

Since N is flat as a B-module, $((- \otimes_A B) \otimes_B N)$ is exact as a functor from A-module to B-module, that is, f_2 is injective as a B-module map. $(X \otimes_A B) \otimes_B N$ and $(Y \otimes_A B) \otimes_B N$ carry an A-module structure defined by

$$\begin{aligned} A \times ((X \otimes_A B) \otimes_B N) &\to (X \otimes_A B) \otimes_B N \\ (a, (x \otimes_A b) \otimes_B n) &\mapsto (x \otimes_A ab) \otimes_B n \end{aligned}$$

Under that A-module structure, f_2 is also an A-module map because

$$f_2(a((x \otimes_A b) \otimes_B n)) = f_2((x \otimes_A ab) \otimes_B n) = (f(x) \otimes_A ab) \otimes_B n = a((f(x) \otimes_A b) \otimes_B n) = af_2((x \otimes_A b) \otimes_B n)$$

Hence, $((- \otimes_A B) \otimes_B N)$ is an exact functor from A-module into (A,B)-bimodule.
(2c) Note that, N carries a A-module structure defined by

$$\begin{aligned} A \times N &\to N \\ (a, n) &\mapsto (a1_B)n \end{aligned}$$

Let f_3 be the induced A-module map by the functor $(- \otimes_A N)$. The natural isomorphism $g : (- \otimes_A N) \to ((- \otimes_A B) \otimes_B N)$ is defined as follows:

$$\begin{tikzcd}
X \otimes_A N \arrow[rrr, "f_3"] \arrow[ddd, "g_X"'] & & & Y \otimes_A N \arrow[ddd, "g_Y"] \\
& x \otimes_A n \arrow[r, mapsto] \arrow[d, mapsto] & f(x) \otimes_A n \arrow[d, mapsto] & \\
& (x \otimes_A 1) \otimes_B n \arrow[r, mapsto] & (f(x) \otimes_A 1) \otimes_B n & \\
(X \otimes_A B) \otimes_B N \arrow[rrr, "f_2"] & & & (Y \otimes_A B) \otimes_B N
\end{tikzcd}$$

The square commutes since

$$g_Y f_3(x \otimes_A n) = g_Y(f(x) \otimes_A N) = (f(x) \otimes_A 1) \otimes_B n$$
$$f_2 g_X(x \otimes_A n) = f_2((x \otimes_A 1) \otimes_B n) = (f(x) \otimes_A 1) \otimes_B n$$

for all $x \in X, n \in N$. f_2 being injective implies f_3 being injective. Hence, N is flat as an A-module by the above A-module structure. $\square$

Problem 13.0.5 (chapter 3 problem 4)
Let $f : A \to B$ be a homomorphism of rings and let S be a multiplicatively closed subset of A. Let $T = f(S)$. Show that $S^{-1}B$ and $T^{-1}B$ are isomorphic as $S^{-1}A$-modules.

Proof. B carries the A-module structure defined by

$$A \times B \to B$$
$$(a, b) \mapsto f(a)b$$

for $a \in A$ and $b \in B$. Hence, $S^{-1}B$ is a localization of A-module B on the multiplicatively closed subset S

$$S^{-1}B = B \times S / \sim$$

where $(b_1, s_1) \sim (b_2, s_2)$ for $b_1, b_2 \in B$ and $s_1, s_2 \in S$ if and only if there exists $s \in S$ so that $0 = s(s_2 b1 - s_1 b2) = f(s)(f(s_2)b_1 - f(s_1)b_2)$. The $S^{-1}A$-module structure on $S^{-1}B$ is defined by

$$S^{-1}A \otimes S^{-1}B \to S^{-1}B$$
$$\left(\frac{a}{s_1}, \frac{b}{s_2}\right) \mapsto \frac{ab}{s_1 s_2} = \frac{f(a)b}{s_1 s_2}$$

where $a \in A$, $b \in B$, and $s_1, s_2 \in S$. On the other hand, $T^{-1}B$ is a localization of ring B on the multiplicatively closed subset T

$$T^{-1}B = B \times T / \sim$$

where $(b_1, t_1) \sim (b_2, t_2)$ for $b_1, b_2 \in B$ and $t_1, t_2 \in T$ if and only if there exists $t \in T$ so that $0 = t(t_2 b_1 - t_1 b_2)$. We define the canonical $S^{-1}A$-module structure on $T^{-1}B$ by

$$S^{-1}A \times T^{-1}B \to T^{-1}B$$
$$\left(\frac{a}{s}, \frac{b}{t}\right) \mapsto \frac{ab}{st} = \frac{f(a)b}{f(s)t}$$

Now, we can define a pair of isomorphisms between $S^{-1}B$ and $T^{-1}B$ as $S^{-1}A$-modules as follows:

$$\begin{aligned} S^{-1}B &\to T^{-1}B \\ \phi : \frac{b}{s} &\mapsto \frac{b}{f(s)} \\ \psi : \frac{b}{s_t} &\leftarrow\!\shortmid \frac{b}{t} \end{aligned}$$

where $b \in B$, $s \in S$, $t \in T$, and $s_t = f^{-1}(t) \in S$ is any element in the preimage of t.
(ϕ is well-defined) Let $b_1/s_1 = b_2/s_2$ in $S^{-1}B$, then there exists $s \in S$, so that $0 = s(s_2b_1 - s_1b_2) = f(s)(f(s_2)b_1 - f(s_1)b_2)$, this is the condition for $\phi(b_1/s_1) = \phi(b_2/s_2)$
(ψ is well-defined) Let $s_1, s_2 \in S$ so that $b_1/f(s_1) = b_2/f(s_2)$ in $T^{-1}B$, then there exists $t \in T = f(S)$ so that $0 = t(f(s_2)b_1 - f(s_1)b_2)$. Let $s \in S$ so that $f(s) = t$, then we have $0 = f(s)(f(s_2)b_1 - f(s_1)b_2) = s(s_2b_1 - s_1b_2)$, this is the condition for $\psi(b_1/f(s_1)) = psi(b_2/f(s_2))$. Note that, this also show that the image of ψ is independent of the choice of s_t
($\phi\psi = 1$, $\psi\phi = 1$) this is clear from the definition
(ϕ and ψ are $S^{-1}A$-module maps)

$$\phi\left(\frac{a}{s_1}\frac{b_2}{s_2} + \frac{b_3}{s_3}\right) = \phi\left(\frac{f(s_3)f(a)b_2 + f(s_1)f(s_2)b_3}{s_1s_2s_3}\right) = \frac{f(s_3)f(a)b_2 + f(s_1)f(s_2)b_3}{f(s_1)f(s_2)f(s_3)} = \frac{a}{s_1}\phi\left(\frac{b_2}{s_2}\right) + \phi\left(\frac{b_3}{s_3}\right)$$

$$\psi\left(\frac{a}{s_1}\frac{b_2}{f(s_2)} + \frac{b_3}{f(s_3)}\right) = \psi\left(\frac{f(s_3)f(a)b_2 + f(s_1)f(s_2)b_3}{f(s_1)f(s_2)f(s_3)}\right) = \frac{f(s_3)f(a)b_2 + f(s_1)f(s_2)b_3}{s_1s_2s_3} = \frac{a}{s_1}\psi\left(\frac{b_2}{f(s_2)}\right) + \phi\left(\frac{b_3}{f(s_3)}\right)$$

□

Problem 13.0.6 (chapter 3 problem 12 - torsion submodule)
Let A be an integral domain and M an A-module. An element $x \in M$ is a torsion element of M if $\operatorname{ann}_A(x) = \{a \in A : ax = 0\} \neq 0$, that is if x is killed by some non-zero element of A. Show that the torsion elements of M form a submodule of M. This submodule is called the torsion submodule of M and denoted by $T(M)$. If $T(M) = 0$, the module M is said to be torsion-free. Show that

1. If M is any A-module, then $M/T(M)$ is torsion-free
2. If $f : M \to N$ is a module morphism then $f(T(M)) \subseteq T(N)$
3. If $0 \to M_l \to M \to M_r \to 0$ is an exact sequence, then the sequence $0 \to T(M_l) \to T(M) \to T(M_r)$ is exact, i.e. $T(-)$ is a left exact covariant functor
4. If M is any A-module, then $T(M)$ is the kernel of the mapping $x \mapsto 1 \otimes x$ of M into $K \otimes_A A$ where K is the field of fractions of A, i.e. $K = \operatorname{Frac}(A) = (A - 0)^{-1}A$

Proof. ($T(M)$ is a submodule of M) $0 \in T(M)$. If $x, y \in T(M)$, then $ax = 0$ and $by = 0$ for some $a, b \in A$. Hence $a(-x) = ax + a(-x) = a(x - x) = 0$ and $ab(x + y) = bax + aby = 0$. Moreover, for any $a_1 \in A$, then $a(a_1x) = a_1ax = 0$, hence $T(M)$ is a submodule of M
(1) Suppose $\bar{x} \in M/T(M)$ is nonzero and it is an element of the torsion submodule of $M/T(M)$, there exists $a \in A$ so that $0 = a\bar{x} = \overline{ax}$, hence $ax \in T(M)$, so there exists $b \in A$ so that $bax = 0$, that implies $x \in T(M)$ which contradicts the assumption of $\bar{x}$ being nonzero
(2) Let $x \in T(M)$, then there exists $a \in A$, so that $ax = 0$. Hence $0 = f(ax) = af(x)$, so $f(x) \in T(N)$

(3) $T(M_l) \to T(M)$ is injective since it is a restriction of the injective map $M_l \to M$. Moreover, by (2)

$$\ker(T(M) \to T(M_r)) = T(M) \cap \ker(M \to M_r) = T(M) \cap \mathrm{im}(M_l \to M) \supseteq \mathrm{im}(T(M_l) \to T(M))$$

Let denote the map $M_l \to M$ by $f : M_l \to M$ For any $x \in T(M) \cap \mathrm{im}(M_l \to M)$, there exists $y \in M_l$ so that $f(y) = x$. Since, $x \in T(M)$, there exists $a \in A$ so that $0 = ax = af(y) = f(ay)$. Since f is injective, $ay = 0$, i.e $y \in T(M_l)$, hence $T(M) \cap \mathrm{im}(M_l \to M) = \mathrm{im}(T(M_l) \to T(M))$

(4)

Let $S = A - 0$, then we have

$$S^{-1}A \otimes_A M \cong S^{-1}M$$

The composition $M \to S^{-1}M$ is defined by

$$\begin{aligned} M \to K \otimes M &\xrightarrow{\sim} S^{-1}M \\ x \mapsto 1 \otimes x &\mapsto \frac{x}{1} \end{aligned}$$

$$x \in \ker(M \to K \otimes M) \iff x/1 = 0 \text{ in } S^{-1}M \iff \exists a \in S, ax = 0 \iff x \in T(M)$$

Note, the suggestion in the book was really misleading and that costed me a whole night and not delivering the solution. My effort was as below

(K is a colimit of a diagram containing $A\mu$ for $\mu \in K - 0$)

Consider K as an A-module, for any $\mu \in K - 0$, $A\mu = \{\tilde{a}\mu : \tilde{a} \in A\}$ is a submodule of K, there is a canonical A-module map

$$\begin{aligned} f_{\mu\nu} : A\mu &\to A\nu \\ x &\mapsto (\nu\mu^{-1})x \end{aligned}$$

for any $\mu, \nu \in K - 0$ and $x \in A\mu$. Define

$$\begin{aligned} g_\mu : A\mu &\to K \\ x &\mapsto \mu^{-1}x \end{aligned}$$

Then, $g_\bullet$ is the colimit of the diagram consists of $f_{\bullet\bullet}$

$$\begin{tikzcd}
A\mu \arrow[rr, "f_{\mu\nu}"] \arrow[dr, "g_\mu"] \arrow[ddr, "h_\mu"'] & & A\nu \arrow[dl, "g_\nu"'] \arrow[ddl, "h_\nu"] \\
& K \arrow[d, dashed, "k"] & \\
& L &
\end{tikzcd}$$

Let h_μ and h_ν be defined so that the diagram commutes, then $k : K \to L$ is

$$\begin{aligned} k : K &\to L \\ x &\mapsto h_\mu(\mu x) \end{aligned}$$

This map is unique since if $k' : K \to L$ makes the diagram commutes, then

$$(k' - k)g_\mu = k'g_\mu - kg_\mu = 0$$

for all $\mu \in K - 0$. For any $x = a/b \in K$ for $a \in A$ and $b \in A - 0$, let $\mu = 1/b$, then $x \in A\mu$. In other words, the map $g : \coprod_{\mu \in K-0} A\mu \to K$ is surjective.

$$\begin{tikzcd} A\mu \arrow[r] \arrow[dr] & \coprod_{\mu\in K-0} A\mu = \bigoplus_{\mu\in K-0} A\mu \arrow[d, two heads] \\ & K \end{tikzcd}$$

Then, $0 = (k' - k)g_\mu(\mu x) = (k' - k)(x)$ for all $x \in K$. Hence, $k' - k$ is a zero function, so the factoring map k is unique. In particular, the diagram of $f_{\bullet\bullet}$ is a directed set, so K is the direct limit of the directed set

$$K = \operatorname{colim}_\mu A_\mu = \varinjlim_\mu A_\mu$$

(colimit are compatible with tensor product) The diagram consists of $A_\mu \otimes M$ and $g_{\mu\nu} \otimes 1 : A_\mu \otimes M \to A_\nu \otimes M$ is a directed set, A-module is a cocomplete category, hence the colimit exists

$$\operatorname{colim}_\mu (A_\mu \otimes M) = \varinjlim_\mu (A_\mu \otimes M)$$

We will show that $\operatorname{colim}_\mu (A_\mu \otimes M) \cong (\operatorname{colim}_\mu A_\mu) \otimes M$. For any A-module L, we have

$$\begin{aligned} \operatorname{Hom}(\operatorname{colim}_\mu (A_\mu \otimes M), L) &\cong \lim_\mu \operatorname{Hom}(A_\mu \otimes M, L) && (\operatorname{Hom}(-, L) \text{ is contravariant}) \\ &\cong \lim_\mu \operatorname{Hom}(A_\mu, \operatorname{Hom}(M, L)) && (\text{tensor-hom adjunction}) \\ &\cong \operatorname{Hom}(\operatorname{colim}_\mu A_\mu, \operatorname{Hom}(M, L)) && (\operatorname{Hom}(-, \operatorname{Hom}(M, L)) \text{ is contravariant}) \\ &\cong \operatorname{Hom}((\operatorname{colim}_\mu A_\mu) \otimes M, L) && (\text{tensor-hom adjunction}) \end{aligned}$$

Hence, $\operatorname{colim}_\mu (A_\mu \otimes M) \cong (\operatorname{colim}_\mu A_\mu) \otimes M$ as a consequence of Yoneda lemma. In particular

$$K \otimes M \cong \operatorname{colim}_\mu (A_\mu \otimes M)$$

(main proof)
Now, the canonical isomorphism $M \mapsto A1 \otimes M$ defined by $x \mapsto 1 \otimes x$ and the canonical map $M \to K \otimes M$ defined by $x \mapsto 1 \otimes x$ make the diagram commutes.

$$\begin{tikzcd} M \arrow[r, "\sim"] \arrow[drr] & A1 \otimes M \arrow[r, "f_{1\nu}\otimes 1"] \arrow[dr, "g_1\otimes 1"] & A\nu \otimes M \arrow[d, "f_\nu\otimes 1"] \\ & & K \otimes M \end{tikzcd}$$

Let $x \in \ker(M \to K \otimes M)$, for any $\nu \in K - 0$, the image on $A\nu \otimes M$ is

$$(f_{1\nu} \otimes 1)(1 \otimes x) = \nu \otimes x$$

Let $\nu = a/1$, then

$$(f_{1\nu} \otimes 1)(1 \otimes x) = \nu \otimes x = 1 \otimes ax$$

Pullback to M gives $ax \in \ker(M \to K \otimes M)$ ☐

Problem 13.0.7 (chapter 3 problem 16 - faithfully flat)

Let B be a flat A-algebra. Then the following conditions are equivalent

1. $\mathfrak{a}^{ec} = \mathfrak{a}$ for all ideals $\mathfrak{a}$ of A
2. $\operatorname{Spec} B \to \operatorname{Spec} A$ is surjective
3. For every maximal ideal $\mathfrak{m}$ of A, we have $\mathfrak{m}^e \neq (1)$
4. If M is any non-zero A-module, then $M_B \neq 0$ for $M_B = M \otimes_A B$
5. For every A-module M, the mapping $x \to 1 \otimes x$ of M into M_B is injective

B is said to be faithfully flat over A

Lemma 13.0.8 (chapter 2 exercise 13)

Let $f : A \to B$ be a ring map and N be a B-module, then the map $g : N \to N \otimes_A B$ defined by $y \mapsto 1 \otimes y$ is injective.

Proof.

$(1 \implies 2)$ The map $\phi^* : \operatorname{Spec} B \to \operatorname{Spec} A$ is defined by

$$\begin{aligned} \phi^* : \operatorname{Spec} B &\to \operatorname{Spec} A \\ \mathfrak{q} &\mapsto \mathfrak{q}^c \end{aligned}$$

For any prime ideal $\mathfrak{p}$ in $\operatorname{Spec} A$,

$$\mathfrak{p} = \mathfrak{p}^{ec} = \phi^*(\mathfrak{p}^e)$$

Hence, the map $\phi^* : \operatorname{Spec} B \to \operatorname{Spec} A$ is surjective

$(2 \implies 3)$ Since $\phi^* : \operatorname{Spec} B \to \operatorname{Spec} A$ is surjective, there exists a prime ideal $\mathfrak{n} \in \operatorname{Spec} B$ so that $\mathfrak{m} = \phi^*(\mathfrak{n}) = \mathfrak{n}^c$, hence

$$\mathfrak{m}^e = \mathfrak{n}^{ce} \subseteq \mathfrak{n} \subsetneq (1)$$

$(3 \implies 4)$ For any non-zero $x \in M$, let Ax be the submodule of M generated by x. Since B is flat, the top exact sequence induces the exactness of the bottom sequence

$$0 \longrightarrow Ax \longrightarrow M$$

$$0 \longrightarrow Ax \otimes_A B \longrightarrow M \otimes_A B$$

Since $Ax \otimes_A B \to M \otimes_A B$ is injective, in order to show $M \otimes_A B \neq 0$, it suffices to show that $Ax \otimes_A B \neq 0$. The module Ax generated by one element is isomorphic to $A/\mathfrak{a}$ for some ideal $\mathfrak{a}$ of A and $\mathfrak{a} \neq A$ since Ax is nontrivial. Hence,

$$Ax \otimes_A B \cong \frac{A}{\mathfrak{a}} \otimes_A B \cong \frac{B}{\mathfrak{a}B} = \frac{B}{\mathfrak{a}^e B} = \frac{B}{\mathfrak{a}^e}$$

Since $\mathfrak{a}$ belongs to some maximal ideal $\mathfrak{m}$ in A and $\mathfrak{m}^e \neq (1)$, so $\mathfrak{a}^e \neq B$. Hence, $Ax \otimes_A B \neq 0$

$(4 \implies 5)$ Let $K = \ker(M \to M \otimes_A B)$, since B is a flat A-module, then top exact sequence induces the exactness of the bottom sequence

$$
\begin{tikzcd}
0 \arrow[r] & K \arrow[r] & M \arrow[r] & M \otimes_A B
\end{tikzcd}
$$

$$
\begin{tikzcd}
0 \arrow[r] & K \otimes_A B \arrow[r] & M \otimes_A B \arrow[r, "v"] & (M \otimes_A B) \otimes_A B
\end{tikzcd}
$$

Note that, from Lemma 13.0.8 with $N = M \otimes_A B$, the composition $t : M \otimes_A B \to (M \otimes_A B) \otimes_A B$ is injective due to the natural isomorphism $(x \otimes 1) \otimes b \mapsto (x \otimes b)$, hence the induced map v from $(- \otimes_A B)$ is injective.

$$
\begin{tikzcd}
M \arrow[r] & M \otimes_A B & M \otimes_A B \arrow[r, "v"'] \arrow[rr, bend left, "t"] & (M \otimes_A B) \otimes_A B \arrow[r, "\sim"] & (M \otimes_A B) \otimes_A B \\
x \arrow[r, mapsto] & x \otimes 1 & x \otimes b \arrow[r, mapsto] & (x \otimes 1) \otimes b \arrow[r, mapsto] & (x \otimes b) \otimes 1
\end{tikzcd}
$$

So, by exactness, $K \otimes_A B = 0$. From 4, $K = 0$

$(5 \implies 1)$ We always have $\mathfrak{a}^{ec} \supseteq \mathfrak{a}$ for all ideals $\mathfrak{a}$ in A, we will show the other direction $\mathfrak{a}^{ec} \subseteq \mathfrak{a}$. Let $f : A \to B$, for any $x \in \mathfrak{a}^{ec}$, then $f(x) \in \mathfrak{a}^e \subseteq B$. Let $M = \frac{A}{\mathfrak{a}}$, so the map below is is injective

$$
\begin{aligned}
\frac{A}{\mathfrak{a}} \to \frac{A}{\mathfrak{a}} \otimes_A B \xrightarrow{\sim} \frac{B}{\mathfrak{a}^e} \\
\bar{a} \mapsto \bar{a} \otimes 1 \mapsto \overline{f(a)}
\end{aligned}
$$

Since $f(x) \in \mathfrak{a}^e$, then $\overline{f(x)} = 0$ in $\frac{B}{\mathfrak{a}^e}$, by injectivity, $\bar{x} = 0$ in $\frac{A}{\mathfrak{a}}$, hence $x \in \mathfrak{a}$

$\square$

Problem 13.0.9 (chapter 3 problem 18)
Let $f : A \to B$ be a flat homomorphism of rings (B is a flat A-module), let $\mathfrak{q}$ be a prime ideal of B and let $\mathfrak{p} = \mathfrak{q}^c$. Then $f^* : \operatorname{Spec} B_{\mathfrak{q}} \to \operatorname{Spec} A_{\mathfrak{p}}$ is surjective

Lemma 13.0.10
Let $f : A \to B$ be a ring map and $S \subseteq T$ be two multiplicative subsets of A, then

$$
T^{-1}A \cong \phi_S(T)^{-1}(S^{-1}A) \cong T^{-1}(S^{-1}A)
$$

as A-modules. Note, the result is a consequence of chapter 3 problem 4

Proof. The induced map $A_{\mathfrak{p}} \to B_{\mathfrak{q}}$ is

$$
\begin{aligned}
f_{\mathfrak{q}} : A_{\mathfrak{p}} \to B_{\mathfrak{q}} \\
\frac{a}{s} \mapsto \frac{f(a)}{f(s)}
\end{aligned}
$$

Let $S = A - \mathfrak{p}$ and $T = B - \mathfrak{q}$, then $f(S) \subseteq T$, from Lemma 13.0.10

$$
B_{\mathfrak{q}} = T^{-1}B \cong T^{-1}(f(S)^{-1}B) \cong T^{-1}(S^{-1}B) = (B_{\mathfrak{p}})_{\mathfrak{q}}
$$

The map is well-defined since $s \in A - \mathfrak{p} \iff f_{\mathfrak{q}}(s) \in B - \mathfrak{q}$. B is flat as an A-module, since flatness is a local property, $B_{\mathfrak{p}}$ is flat as an $A_{\mathfrak{p}}$-module, hence $B_{\mathfrak{q}}$ is also flat as an $A_{\mathfrak{p}}$-module because again $B_{\mathfrak{q}}$ is a localized module of $B_{\mathfrak{p}}$. Now, we will show that $B_{\mathfrak{q}}$ is faithfully flat over $A_{\mathfrak{p}}$. Let $\mathfrak{m} = \mathfrak{p}A_{\mathfrak{p}}$ be the unique maximal ideal of $A_{\mathfrak{p}}$, we have a one-to-one correspondence between prime ideals of A and $A_{\mathfrak{p}}$, of B and $B_{\mathfrak{q}}$

$$\begin{tikzcd}
A \arrow[rr] \arrow[ddd] & & B \arrow[ddd] \\
& \mathfrak{p} \arrow[r, mapsto] \arrow[d, mapsto] & \mathfrak{p}^e \arrow[d, mapsto] \\
& \mathfrak{m} = \mathfrak{p}A_{\mathfrak{p}} \arrow[r, mapsto, dashed] & m^e = \mathfrak{p}^e B_{\mathfrak{q}} \\
A_{\mathfrak{p}} \arrow[rr, dashed] & & B_{\mathfrak{q}}
\end{tikzcd}$$

Hence,

$$\mathfrak{m}^e = \mathfrak{p}^e B_{\mathfrak{q}} = \mathfrak{q}^{ce} B_{\mathfrak{q}} \subseteq \mathfrak{q} B_{\mathfrak{q}}$$

Since $\mathfrak{q}B_{\mathfrak{q}}$ is a maximal in $B_{\mathfrak{q}}$, $\mathfrak{m}^e \neq (1)$. Then $\operatorname{Spec} B_{\mathfrak{q}} \to \operatorname{Spec} A_{\mathfrak{p}}$ is surjective. $\square$

Problem 13.0.11 (chapter 3 problem 19 - support of module)
Let A be a ring and M be an A-module. The support of M is defined to be the set $\operatorname{supp}(M)$ of prime ideal $\mathfrak{p}$ of A such that $M_{\mathfrak{p}} \neq 0$. Prove the following results:

1. $M \neq 0 \iff \operatorname{supp}(M) \neq \varnothing$
2. $V(\mathfrak{a}) = \operatorname{supp}(A/\mathfrak{a})$
3. If $0 \to M^l \to M \to M^r \to 0$ is an exact sequence, then $\operatorname{supp}(M) = \operatorname{supp}(M^l) \cup \operatorname{supp}(M^r)$
4. If $M = \sum_{i \in I} M_i$, then $\operatorname{supp}(M) = \bigcup_{i \in I} \operatorname{supp}(M_i)$
5. If M is finitely generated, then $\operatorname{supp}(M) = V(\operatorname{ann}_A(M))$ (and is therefore a closed subset of $\operatorname{Spec} A$)
6. If M, N are finitely generated, then $\operatorname{supp}(M \otimes_A N) = \operatorname{supp}(M) \cap \operatorname{supp}(N)$
7. If M is finitely generated and $\mathfrak{a}$ is an ideal of A, then $\operatorname{supp}(M/\mathfrak{a}M) = V(\mathfrak{a} + \operatorname{ann}_A(M))$
8. If $f : A \to B$ is a ring homomorphism and M is a finitely generated A-module, then $\operatorname{supp}(B \otimes_A M) = (f^*)^{-1}(\operatorname{supp}(M))$ where $f^* : \operatorname{Spec} B \to \operatorname{Spec} A$ is the induced map from f

Note, $V(\mathfrak{a})$ is the set of all prime ideals in A containing $\mathfrak{a}$

Lemma 13.0.12 (chapter 3 proposition 3.7)
Let M and N be A-modules and S be a multiplicatively closed subset of A, then there is an isomorphism

$$S^{-1}M \otimes_{S^{-1}A} S^{-1}N \xrightarrow{\sim} S^{-1}(M \otimes_A N)$$

In particular, if $S = A - \mathfrak{p}$ for some prime ideal $\mathfrak{p}$, then

$$M_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} N_{\mathfrak{p}} \xrightarrow{\sim} (M \otimes_A N)_{\mathfrak{p}}$$

Lemma 13.0.13 (chapter 2 problem 3 extended)
Let A be a local ring with unique maximal ideal $\mathfrak{a}$, M and N be A-modules with $M_{\mathfrak{a}} \neq 0$ and N finitely generated. Prove that

$$M \otimes_A N \implies N = 0$$

Note, the proof is exactly in chapter 2 problem 3, except at the last step we only use Nakayama lemma version 1 for N and given $M_{\mathfrak{a}} \neq 0$, then N is zero.

Proof.
(1)

$$M = 0 \iff M_{\mathfrak{p}} = 0 \text{ for all prime ideal } \mathfrak{p} \subseteq A \iff \operatorname{supp}(M) = \varnothing$$

(2) For any prime ideal $\mathfrak{p}$ in A, the following are equivalent

(a) $(A/\mathfrak{a})_{\mathfrak{p}} \neq 0$

(b) $\exists x \in A, \forall t \in A - \mathfrak{p}, tx \notin \mathfrak{a}$

(c) $\mathfrak{a} \subseteq \mathfrak{p}$

$(b \implies c)$ suppose $(b \wedge \neg c)$, that is there exists $a \in \mathfrak{a} - \mathfrak{p} \subseteq A - \mathfrak{p}$, then $ax \in \mathfrak{a}$, that is a contradiction
$(b \impliedby c)$ suppose $(\neg b \wedge c)$, note that $(\neg b)$ is $\forall x \in A, \exists t \in A - \mathfrak{p}, tx \in \mathfrak{a}$. Since $\mathfrak{p}$ is prime, that is not the whole ring, choose $x \in A - \mathfrak{p}$, then there exists $t \in A - \mathfrak{p}$, but $tx \in \mathfrak{a} \subseteq \mathfrak{p}$, that is a contraction
Hence, $p \in \operatorname{supp}(A/\mathfrak{a}) \iff \mathfrak{p} \in V(\mathfrak{a})$, that is $\operatorname{supp}(A/\mathfrak{a}) = V(\mathfrak{a})$
(3) For any prime ideal $\mathfrak{p}$ in A, the functor $((A - \mathfrak{p})^{-1} -)$ is exact, hence both sequences are exact

$$0 \longrightarrow M^l \longrightarrow M \longrightarrow M^r \longrightarrow 0$$

$$0 \longrightarrow M^l_{\mathfrak{p}} \longrightarrow M_{\mathfrak{p}} \longrightarrow M^r_{\mathfrak{p}} \longrightarrow 0$$

Then

$$\mathfrak{p} \in \operatorname{supp}(M)^c \iff M_{\mathfrak{p}} = 0 \iff M^l_{\mathfrak{p}} = 0 \text{ and } M^r_{\mathfrak{p}} = 0 \iff \mathfrak{p} \in \operatorname{supp}(M^l)^c \cap \operatorname{supp}(M^r)^c$$

Hence, $\operatorname{supp}(M)^c = \operatorname{supp}(M^l)^c \cap \operatorname{supp}(M^r)^c$, that is equivalent to $\operatorname{supp}(M) = \operatorname{supp}(M^l) \cup \operatorname{supp}(M^r)$
(4) For any prime ideal $\mathfrak{p}$ in A, the functor $((A - \mathfrak{p})^{-1} -)$ is exact, hence both sequences are exact

$$0 \longrightarrow M_i \longrightarrow M$$

$$0 \longrightarrow (M_i)_{\mathfrak{p}} \longrightarrow M_{\mathfrak{p}}$$

Then

$$\mathfrak{p} \in \operatorname{supp}(M)^c \iff M_{\mathfrak{p}} = 0 \implies (M_i)_{\mathfrak{p}} = 0 \iff \mathfrak{p} \in \operatorname{supp}(M_i)^c$$

Hence, $\operatorname{supp}(M)^c \subseteq \bigcap_{i \in I} \operatorname{supp}(M_i)^c$, that is equivalent to $\operatorname{supp}(M) \supseteq \bigcup_{i \in I} \operatorname{supp}(M_i)$. To see the other direction, let $\mathfrak{p} \in \operatorname{supp}(M)$ but $(M_i)_{\mathfrak{p}} = 0$ for all $i \in I$. Let

$$x = \sum_{j \in J} x_j \in M$$

for some finite subset $J \subseteq I$ so that $\frac{x}{s} \neq 0$ in $M_{\mathfrak{p}}$ for some $s \in A - \mathfrak{p}$. Since $(M_j)_{\mathfrak{p}} = 0$, $\frac{x_j}{1} = 0$ in $(M_j)_{\mathfrak{p}}$, so there exists $t_j \in A - \mathfrak{p}$ so that $t_j x_j = 0$. Hence, let $t = \prod_{j \in J} t_j$, then $tx = 0$, so $\frac{x}{s} = 0$, that a contradiction

(5) Let $x_1, x_2, ..., x_n$ generates M, the each Ax_i is a submodule of M that is isomorphic to $A/\mathfrak{a}_i$ for some ideal $\mathfrak{a}_i$ in A. We will show that $\bigcap_{i=1}^n \mathfrak{a}_i = \operatorname{ann}_A(M)$. If $a \in A$ so that $aM = 0$, then $a(Ax_i) = 0$ for all i, hence $x \in \mathfrak{a}_i$ for all i. On the other hand, if $a \in \mathfrak{a}_i$, then a acts on any element of Ax_i resulting zero. Hence, $aM = 0$. We have

$$\operatorname{supp}(M) = \operatorname{supp}(\sum_{i=1}^n Ax_i) = \bigcup_{i=1}^n \operatorname{supp}(Ax_i) = \bigcup_{i=1}^n \operatorname{supp}(A/\mathfrak{a}_i) = \bigcup_{i=1}^n V(\mathfrak{a}_i) = V\left(\bigcap_{i=1}^n \mathfrak{a}_i\right) = V(\operatorname{ann}_A(M))$$

(6) For any prime ideal $\mathfrak{p}$ in A, since $A_\mathfrak{p}$ is a local ring, from chapter 2 problem 3, we have

$$\mathfrak{p} \in \operatorname{supp}(M \otimes_A N)^c \iff M_\mathfrak{p} \otimes_{A_\mathfrak{p}} N_\mathfrak{p} = (M \otimes N)_\mathfrak{p} = 0 \iff M_\mathfrak{p} = 0 \text{ or } N_\mathfrak{p} = 0 \iff \mathfrak{p} \in \operatorname{supp}(M)^c \cup \operatorname{supp}(N)^c$$

Hence, $\operatorname{supp}(M \otimes_A N) = \operatorname{supp}(M) \cap \operatorname{supp}(N)$

(7)

$$\operatorname{supp}(M/\mathfrak{a}M) = \operatorname{supp}(A/\mathfrak{a} \otimes_A M) = \operatorname{supp}(A/\mathfrak{a}) \cap \operatorname{supp}(M) = V(\mathfrak{a}) \cap V(\operatorname{ann}_A(M)) = V(\mathfrak{a} \cup \operatorname{ann}_A(M)) = V(\mathfrak{a} + \operatorname{ann}_A(M))$$

where the last equality is due to $\mathfrak{a} + \operatorname{ann}_A(M)$ being the smallest ideal containing $\mathfrak{a} \cup \operatorname{ann}_A(M)$

(8) The induced map $f^* : \operatorname{Spec} B \to \operatorname{Spec} A$ is defined by

$$\begin{aligned} f^* : \operatorname{Spec} B &\to \operatorname{Spec} A \\ \mathfrak{q} &\mapsto \mathfrak{q}^c \end{aligned}$$

Let $\mathfrak{q} \in \operatorname{Spec} B$, and $\mathfrak{p} = f^*(\mathfrak{q}) = \mathfrak{q}^c$, then we have

$$\begin{aligned}
(B \otimes_A M)_\mathfrak{q} &\cong B_\mathfrak{q} \otimes_B (B \otimes_A M) \\
&\cong (B_\mathfrak{q} \otimes_B B) \otimes_A M \\
&\cong B_\mathfrak{q} \otimes_A M \\
&\cong (B_\mathfrak{q} \otimes_{A_\mathfrak{p}} A_\mathfrak{p}) \otimes_A M && (B_\mathfrak{q} \text{ is an } A_\mathfrak{p}\text{-module, Lemma 13.0.10}) \\
&\cong B_\mathfrak{q} \otimes_{A_\mathfrak{p}} (A_\mathfrak{p} \otimes_A M) \\
&\cong B_\mathfrak{q} \otimes_{A_\mathfrak{p}} M_\mathfrak{p}
\end{aligned}$$

The proof logic is as follows:

$$\begin{tikzcd}
\mathfrak{q} \in (f^*)^{-1}(\operatorname{supp}(M))^c \arrow[r, leftrightarrow] & \mathfrak{p} \in \operatorname{supp}(M)^c \arrow[r, leftrightarrow] & M_\mathfrak{p} = 0 \arrow[d, bend right] \\
\mathfrak{q} \in \operatorname{supp}_B(B \otimes_A M)^c \arrow[r, leftrightarrow] & (B \otimes_A M)_\mathfrak{q} = 0 \arrow[r, leftrightarrow] & B_\mathfrak{q} \otimes_{A_\mathfrak{p}} M_\mathfrak{p} = 0 \arrow[u, bend right]
\end{tikzcd}$$

where $B_\mathfrak{q} \otimes_{A_\mathfrak{p}} M_\mathfrak{p} = 0 \implies M_\mathfrak{p} = 0$ because $(B_\mathfrak{q})_\mathfrak{p} = B_\mathfrak{q} \neq 0$. $B_\mathfrak{q} \neq 0$ because $1/1 \neq 0$ in $B_\mathfrak{q}$ and $(B_\mathfrak{q})_\mathfrak{p} = B_\mathfrak{q}$ because $B - \mathfrak{q} \supseteq B - \mathfrak{p}^e$, localizing larger subset first then localizing smaller subset is equivalent to localizing only larger subset. □

Proof of Lemma 13.0.12.

$$\begin{aligned}
S^{-1}(M \otimes_A N) &\cong S^{-1}A \otimes_A (M \otimes_A N) \\
&\cong (S^{-1}A \otimes_A M) \otimes_A N \\
&\cong S^{-1}M \otimes_A N \\
&\cong (S^{-1}A \otimes_{S^{-1}A} S^{-1}M) \otimes_A N \\
&\cong (S^{-1}M \otimes_{S^{-1}A} S^{-1}A) \otimes_A N \\
&\cong S^{-1}M \otimes_{S^{-1}A} (S^{-1}A \otimes_A N) \\
&\cong S^{-1}M \otimes_{S^{-1}A} (S^{-1}A \otimes_A N) \\
&\cong S^{-1}M \otimes_{S^{-1}A} S^{-1}N
\end{aligned}$$

□

Problem 13.0.14 (chapter 5 problem 1)
Let $f : A \to B$ be an integral ring extension. Show that $f^* : \operatorname{Spec} B \to \operatorname{Spec} A$ is a closed mapping, that is, it maps closed sets into closed sets

Proof. Let $\mathfrak{b} \subseteq B$ be any ideal, then $V(\mathfrak{b})$ is a closed set in $\operatorname{Spec} B$ and

$$f^*V(\mathfrak{b}) = \{\mathfrak{q} \cap A : \mathfrak{q} \in V(\mathfrak{b})\}$$

is its image in $\operatorname{Spec} A$. We have

$$\mathfrak{p} \in f^*V(\mathfrak{b}) \iff \exists \mathfrak{q} \in V(\mathfrak{b}), \mathfrak{q} \cap A = \mathfrak{p} \implies \mathfrak{p} \in V(\mathfrak{b} \cap A)$$

That is, $f^*V(\mathfrak{b}) \subseteq V(\mathfrak{b} \cap A)$. On the other hand, for any $\mathfrak{p} \in V(\mathfrak{b} \cap A)$, the inclusion

$$\frac{A}{\mathfrak{b} \cap A} \hookrightarrow \frac{B}{\mathfrak{b}}$$

is an integral ring extension, $\bar{\mathfrak{p}}$ is a prime ideal in $\frac{A}{\mathfrak{b} \cap A}$, hence there exists a prime ideal $\mathfrak{q} \in V(\mathfrak{b})$ so that $\bar{\mathfrak{q}} \cap \frac{A}{\mathfrak{b} \cap A} = \bar{\mathfrak{p}}$. We have

$$\begin{aligned}
\bar{\mathfrak{q}} &= \{y + \mathfrak{b} : y \in \mathfrak{q}\} \\
\bar{\mathfrak{p}} = \bar{\mathfrak{q}} \cap \frac{A}{\mathfrak{b} \cap A} &= \{x + \mathfrak{b} \cap A : x \in A, f(x) = y\}
\end{aligned}$$

Since $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ are prime ideals of a quotient map $\mathfrak{p} = \{x \in A, f(x) = y\} = \mathfrak{q} \cap A$. Hence, $f^*V(\mathfrak{b}) = V(\mathfrak{b} \cap A)$, f^* is a closed map □

Problem 13.0.15 (chapter 5 problem 3)
Let $f : B \to B'$ be a A-algebra morphism and C be an A-algebra. If f is integral, show that $f \otimes 1 : B \otimes_A C \to B' \otimes_A C$ is integral

Proof. Since the integral closure of $B \otimes_A C$ in $B' \otimes_A C$ is a subring of $B' \otimes_A C$, it suffices to show that all every basic tensor $b' \otimes c$ is integral over $B \otimes_A C$. $f : B \to B'$ is integral, hence any $b' \in B$ satisfies a monic polynomial in B

$$(b')^n + f(b_1)(b')^{n-1} + ... + f(b_n) = 0$$

for some $b_1, ..., b_n \in B$. Note that, $(b' \otimes c)^k = (b')^n \otimes c^k$. Let c^n act on the monic polynomial, we have

$$(b' \otimes c)^n + (f(b_1) \otimes c)(b' \otimes c)^{n-1} + ... + (f(b_n) \otimes c^n) = 0$$

The coefficients $f(b_k) \otimes c^k = (f \otimes 1)(b_k \otimes c^k) \in \mathrm{im}(f \otimes 1)$. Hence, $b' \otimes c$ is integral over $B \otimes_A C$ $\square$

Problem 13.0.16 (chapter 5 problem 5)
Let $A \hookrightarrow B$ be an integral ring extension

1. If $x \in A$ is a unit in B then it is a unit in A
2. The Jacobson radical of A is the contraction of the Jacobson radical of B

Proof.
(1)
Suppose x is not a unit in A, let $\mathfrak{m}_A$ be the maximal ideal containing x, then there exists a prime ideal $\mathfrak{m}_B$ in B so that $\mathfrak{m}_B \cap A = \mathfrak{m}_A$. Since $\mathfrak{m}_A$ is maximal, then $\mathfrak{m}_B$ is also maximal, but $x \in \mathfrak{m}_A \subseteq \mathfrak{m}_B$, then x is not a unit in B, contradiction.
(2)
Using the previous argument, any maximal ideal in A is the contraction of another maximal ideal in B, hence

$$J(A) \subseteq J(B) \cap A$$

Moreover, contraction of any maximal ideal in B is maximal in A, then

$$J(B) \cap A \subseteq J(A)$$

$\square$

Problem 13.0.17 (chapter 5 problem 12)
Let G be a finite group of automorphisms of a ring A and let A^G denote the subring of G-invariants, that is

$$A^G = \{x \in A : \sigma(x) = x \text{ for all } \sigma \in G\}$$

Prove that A is integral over A^G. Let S be a multiplicative closed subset of A such that $\sigma(S) \subseteq S$ for all $\sigma \in G$, let $S^G = S \cap A^G$. Show that the action of G on A extends to an action on $S^{-1}A$ and that $(S^G)^{-1}A^G \cong (S^{-1}A)^G$

Proof. (A is integral over A^G)
For any $x \in A$, since $1_A \in G \subseteq \mathrm{Hom}(A, A)$ and $n = |G|$ is finite, x is a root of the polynomial

$$f(t) = \prod_{\sigma \in G} (t - \sigma(x)) \in A[t]$$

We will show that $f(t) \in A^G[t]$, that is

$$f(t) = a_0 + a_1 t^1 + ... + a_n t^n$$

with $a_0, ..., a_n \in A^G$. For any $\tau \in G \subseteq \mathrm{Hom}(A, A)$, it induces a $\tau \in \mathrm{Hom}(A[t], A[t])$, then

$$\tau(f(t)) = \tau\left(\prod_{\sigma\in G}(t-\sigma(x))\right) = \prod_{\sigma\in G}(t-(\tau\sigma)(x))$$

Since $\{\tau\sigma : \sigma \in G\} = G$, then $\tau(f(t)) = f(t)$, hence

$$\tau(a_k) = a_k$$

Hence, $a_k \in A^G$, thus $f(t) \in A^G[t]$

(the action of G on A extends to an action on $S^{-1}A$)

The action of G on A extends to an action of $S^1 A$ as follows:

$$G \times S^{-1}A \to S^{-1}A$$
$$\left(\sigma, \frac{a}{s}\right) \mapsto \frac{\sigma(a)}{\sigma(s)}$$

This is a well-defined group action since

$$1_A \frac{a}{s} = \frac{a}{s}$$
$$(\sigma\tau)\frac{a}{s} = \frac{\sigma\tau(a)}{\sigma\tau(s)} = \sigma\left(\tau\frac{a}{s}\right)$$

Moreover, it respects addition and multiplication on $S^{-1}A$, that is

$$\sigma\left(\frac{a_1}{s_1}\right) + \sigma\left(\frac{a_2}{s_2}\right) = \frac{\sigma a_1}{\sigma s_1} + \frac{\sigma a_2}{\sigma s_2} = \frac{\sigma(s_2a_1 + s_1a_2)}{\sigma(s_1s_2)} = \sigma\left(\frac{a_1}{s_1} + \frac{a_2}{s_2}\right)$$
$$\sigma\left(\frac{a_1}{s_1}\right)\sigma\left(\frac{a_2}{s_2}\right) = \frac{\sigma a_1}{\sigma s_1}\frac{\sigma a_2}{\sigma s_2} = \frac{\sigma(a_1a_2)}{\sigma(s_1s_2)} = \sigma\left(\frac{a_1}{s_1}\frac{a_2}{s_2}\right)$$

($(S^G)^{-1}A^G \cong (S^{-1}A)^G$)

Note that

$$(S^{-1}A)^G = \left\{\frac{a}{s} \in S^{-1}A : \sigma\left(\frac{a}{s}\right) = \frac{a}{s} \text{ for all } \sigma \in G\right\}$$

We define a pair of isomorphism as follows:

$$(S^G)^{-1}A^G \to (S^{-1}A)^G$$
$$f : \frac{a}{s} \mapsto \frac{a}{s}$$
$$g : \frac{\mu(a)}{\mu(s)} \leftarrow\!\shortmid \frac{a}{s}$$

where $\mu(x) = \sum_{\sigma\in G}\sigma(x)$ for any $x \in A$

f is well-defined since if $a \in A^G$ and $s \in S^G$, then immediately $\sigma\left(\frac{a}{s}\right) = \frac{a}{s}$, hence $f\left(\frac{a}{s}\right) \in (S^{-1}A)^G \subseteq S^{-1}A$.

g is well-defined because $\mu(a) \in A^G$ for any $a \in A$ and $\mu(s) \in S^G$ for any $s \in S$. For any $\tau \in G$, since $\{\tau\sigma : \sigma \in G\} = G$

$$\tau\mu(x) = \tau\left(\sum_{\sigma\in G}\sigma(x)\right) = \sum_{\sigma\in G}\tau\sigma(x) = \sum_{\sigma\in G}\sigma(x) = \mu(x)$$

It is clear that $gf = 1_{(S^G)^{-1}A^G}$. On the other hand, For any $\frac{a}{s} \in (S^{-1}A)^G$, $fg\left(\frac{a}{s}\right) = \frac{\mu(a)}{\mu(s)}$. For each $\sigma \in G$,

$\frac{a}{s} \in (S^{-1}A)^G$ implies that there exists $t_\sigma \in S$ so that

$$t_\sigma s\sigma(a) = t_\sigma a\sigma(s)$$

Let $t = \prod_{\sigma \in G} t_\sigma \in S$, since t_σ is one of the factor of the product t, then $ts\sigma(a) = ta\sigma(s)$ for all $\sigma \in G$, summing over all $\sigma \in G$ gives $ts\mu(a) = ta\mu(s)$. Now, multiplying both sides by $\left(\prod_{\tau \in G - \{1_A\}} \tau(t)\right)$ gives

$$\nu(t)a\mu(s) = \nu(t)s\mu(a)$$

for $\nu(t) = \prod_{\tau \in G} \tau(t)$ using the same argument as above $\prod_{\tau \in G} \tau(t) \in A^G$, moreover since $\tau(S) \subseteq S$, then $\prod_{\tau \in G} \tau(t) \in A^G \cap S = S^G$. Theforefore, $\frac{\mu(a)}{\mu(s)} = \frac{a}{s}$, that is $fg = 1_{(S^{-1}A)^G}$ ☐

Problem 13.0.18 (chapter 5 problem 13)
Let $\mathfrak{p}$ be a prime ideal of A^G and let P be the set of prime ideals of A whose contraction is $\mathfrak{p}$. Show that G act transitively on P. In particular, P is finite.

Proof.
(on a fiber of $\operatorname{Spec} A \to \operatorname{Spec} A^G$, G maps sheets into sheets)
For any $\mathfrak{q} \in P$, then $\mathfrak{q} \cap A^G = \mathfrak{p}$, for any $\sigma \in G$, since σ is an isomorphism in $\operatorname{Hom}(A, A)$, then $\sigma(\mathfrak{q} \cap A^G) = \sigma(\mathfrak{q}) \cap \sigma(A^G)$, hence

$$\mathfrak{p} = \sigma(\mathfrak{p}) = \sigma(\mathfrak{q} \cap A^G) = \sigma(\mathfrak{q}) \cap \sigma(A^G) = \sigma(\mathfrak{q}) \cap A^G$$

Thus, $\sigma(\mathfrak{q})$ is another prime ideal whose contraction is $\mathfrak{p}$
(on a fiber of $\operatorname{Spec} A \to \operatorname{Spec} A^G$, given any two sheets, there is a $\sigma \in G$ maps from one to another)
Let $\mathfrak{q}_1$ and $\mathfrak{q}_2$ be prime ideals in A so that $\mathfrak{p} = \mathfrak{q}_1 \cap A^G = \mathfrak{q}_2 \cap A^G$ but $\mathfrak{q}_2$ is not on the G-orbit of $\mathfrak{q}_1$, that is there exists $x \in \mathfrak{q}_2$ so that $x \notin \sigma(\mathfrak{q}_1)$ for any $\sigma \in G$. From previous part, we have $\nu(x) = \prod_{\sigma \in G} \sigma(x) \in A^G$, moreover x is one of the factor of the product $\nu(x)$, hence

$$\nu(x) \in \mathfrak{q}_2 \cap A^G = \mathfrak{p} \subseteq \mathfrak{q}_1$$

Hence, there at least one $\sigma \in G$ so that $\sigma(x) \in \mathfrak{q}_1$. Thus, $\sigma^{-1} \in G$ map $\sigma(x) \in \mathfrak{q}_1$ into x which is a contradiction.
(P is finite)
In particular, since G is finite, P is also finite.

☐

Problem 13.0.19 (chapter 7 problem 4)
Which is the following rings Noetherian?

1. The ring of rational functions of z having no pole on the circle $|z| = 1$
2. The ring of power series in z with a positive radius of convergence
3. The ring of power series in z with an infinite radius of convergence
4. The ring of polynomials in z whose first k derivatives vanish at the origin (k being a fixed integer)
5. The ring of polynomial in z, w all of whose partial derivatives with respect to w vanish for $z = 0$

   In all cases the coefficients are complex numbers.

Proof.
(1) $\mathbb{C}$ is Noetherian, so $\mathbb{C}[z]$ is Noetherian. Define the multiplicative closed set $S \subseteq \mathbb{C}[x]$

$$S = \{q(z) \in \mathbb{C}[z] : q(x) \neq 0 \text{ for all } x \text{ on the circle } |x| = 1\}$$

Then the rational functions of z having no pole on the circle $|z| = 1$ is precisely $S^{-1}\mathbb{C}[x]$, hence Notherian
(2) The ring of power series in z with positive radius of convergence is

$$A = \left\{\sum_{n=0}^{\infty} a_n z^n : R = \frac{1}{\limsup_{n\to\infty} |a_n|^{1/n}} > 0\right\}$$

Note that we can write any $f(z) \in \mathbb{C}[[z]]$ as

$$f(z) = z^{\operatorname{ord} f(z)} g(z)$$

If $f(z) \in A$, so is $g(z)$. Hence, $f(z) \in (z^{\operatorname{ord} f(z)})$. Therefore, any ideal I in A is generated by z^n for

$$n = \min_{f(x)\in I} \operatorname{ord} f(x)$$

(3) The ring of power series in z with infinite radius of convergence is the ring of holomorphic function $\mathcal{O}$, let

$$I_n = \{f(x) \in \mathcal{O} : 0 = f(n) = f(n+1) = f(n+2) = ...\}$$

Then the chain of ideals $I_1 \subseteq I_2 \subseteq ...$ is strictly increasing. Hence, $\mathcal{O}$ is not Noetherian
(4) The ring of polynomials in z whose first k derivatives vanish at the origin (k being a fixed integer) is

$$B = \mathbb{C} + z^{k+1}\mathbb{C}[z] = \{a_0 + a_1 z + a_2 z^2 + ... + a_k z^k + ... + a_n z^n \in \mathbb{C}[z] : a_1 = a_2 = ... = a_k = 0\}$$

$\mathbb{C}[z^{k+1}]$ is Noetherian and a subring of M and M is a $\mathbb{C}[z^{k+1}]$-module generated by $1, z, z^2, ..., z^k$. Then, M is Noetherian
(5) Let

$$I_n = (z, zw, zw^2, ..., zw^n) \subseteq \mathbb{C}[z, w]$$

Then $I_1 \subseteq I_2 \subseteq ...$ is strictly increasing ($zw^{n+1} \in I_{n+1} - I_n$). Hence The ring of polynomial in z, w all of whose partial derivatives with respect to w vanish for $z = 0$ is not Noetherian ☐

Problem 13.0.20 (chapter 7 problem 5)
Let A be a Noetherian ring and B a finitely generated A-algebra, G is a finite group of A-automorphisms of B and B^G be the set of all elements of B which are left fixed by element element of G. Show that B^G is a finitely generated A-algebra.

Lemma 13.0.21 (chapter 7 proposition 7.8)
Let $A \subseteq B \subseteq C$ be rings. Suppose A is Noetherian, that C is finitely generated as an A-algebra and C is integral over B, then B is finitely generated as an A-algebra

Proof. We know that $B^G \to B$ is an integral ring extension, B being Noether follows from Lemma 13.0.21 and the chain

$$A \subseteq B^G \subseteq B$$

☐

Problem 13.0.22 (chapter 7 problem 8)
If $A[x]$ is Noetherian, is A necessarily Noetherian?

Proof. Since $A \cong A[x]/(x)$, then quotient ring A of a Noetherian ring $A[x]$ is Noetherian $\square$

Problem 13.0.23 (chapter 7 problem 12)
Let A be a ring and B be a faithfully flat A-algebra. If B is Noetherian, show that A is also Noetherian

Proof. B is a failthfully flat A-algebra, hence under the map $A \to B$, for any ideal $\mathfrak{a} \subseteq A$, $\mathfrak{a}^{ec} = \mathfrak{a}$. Let

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq ...$$

be a chain of ideals in A. Then

$$\mathfrak{a}_1^e \subseteq \mathfrak{a}_2^e \subseteq ...$$

is a chain of ideals in B that must stablize at some point. Contracting back to A gives

$$\mathfrak{a}_1^{ec} \subseteq \mathfrak{a}_2^{ec} \subseteq ...$$

must stablize at some point. Hence, A is Noetherian $\square$

Problem 13.0.24
If A is any Noetherian ring, then also the power series ring $A[[x]]$ is Noetherian

Proof. For any power series $f(x) = a_0 + a_1 x^1 + a^2 x^2 + ... + a^n x^n + ... \in A[[x]]$, define

$$\operatorname{ord} f(x) = \min\{n \geq 0 : a_n \neq 0\}$$

Suppose $A[[x]]$ is not Noetherian, let I be an ideal in $A[[x]]$ that is not finitely generated, we will inductively construct $f_0(x), f_1(x), f_2(x), ... \in A[x]$ and ideals $I_n = (f_0(x), f_1(x), ..., f_n(x))$ as follows:
Pick a nonzero $f_0(x) \in I$ of minimal order, set

$$I_0 = (f_0(x))$$

If we already pick $f_0(x), f_1(x), ..., f_{n-1}(x)$, the we pick a nonzero $f_n(x) \in I - I_{n-1}$ of minimal order and set

$$I_n = (f_0(x), f_1(x), ..., f_n(x))$$

By construction, we have

$$\operatorname{ord} f_0(x) \leq \operatorname{ord} f_1(x) \leq \operatorname{ord} f_2(x) \leq ...$$

Let a_n be the first nonzero coefficient of $f_n(x)$ and let $J \subseteq A$ be the ideal defined by

$$J = (a_0, a_1, a_2, ...)$$

Since A is Noetherian, J is finitely generated, that is

$$J = (a_0, a_1, a_2, ..., a_N)$$

for some $N \geq 0$. Let $f(x) \in I_n - I_N$ with $N < n$, by minimality of order of $f_i(x)$, we must have $\operatorname{ord} f(x) - \max\{\operatorname{ord} f_i(x)\} \geq 0$.

We will write $f(x)$ as a $A[[x]]$-linear combination of $f_1(x), f_2(x), ..., f_N(x)$, let $a \in A$ be the first nonzero coefficient of $f(x)$, then $a = \sum_{i=0}^N r_i a_i$ for some $r_0, r_1, ..., r_N \in A$. We can write

$$f(x) = f^{(1)}(x) - \sum_{i=0}^N r_i x^{\operatorname{ord} f(x) - \operatorname{ord} f_i(x)} f_i(x) = f^{(1)}(x) - \sum_{i=0}^N h_i^{(1)}(x) f_i(x)$$

for some $f^{(1)}(x) \in A[[x]]$ with $\operatorname{ord} f^{(1)}(x) \geq \operatorname{ord} f(x) + 1$ and $\operatorname{ord} h_i(x) \geq \operatorname{ord} f(x) - \max\{\operatorname{ord} f_i(x)\} \geq 0$.
Continue this process, we can write

$$f(x) = f^{(k)}(x) - \left(\sum_{i=0}^N h_i^{(k)}(x) f_i(x) + \sum_{i=0}^N h_i^{(k-1)}(x) f_i(x) + ... + \sum_{i=0}^N h_i^{(1)}(x) f_i(x) \right)$$

because at each step, order of $f^{(k)}(x)$ increases by at least 1, so $\operatorname{ord} f^{(k)} \geq \operatorname{ord} f(x) + k$, and

$$\operatorname{ord} h_i^{(k)}(x) \geq \operatorname{ord} f^{(k)}(x) - \max\{\operatorname{ord} f_i(x)\} \geq k + \operatorname{ord} f(x) - \max\{\operatorname{ord} f_i(x)\} \geq k$$

Then we can write

$$f(x) = \sum_{i=1}^N h_i(x) f_i(x)$$

for some $h_i(x) \in A[[x]]$. Because $\operatorname{ord} h_i^{(k)}(x) \geq k$ and $\operatorname{ord} f^{(k)} \geq k$, the process gives a construction of all coeffcients of degree $< k$ of $h_i(x)$ for any k. Hence, $I \subseteq A[[x]]$ is finitely generated.
Alternate proof: show $\mathbb{C}[[x]]$ is PID □

Problem 13.0.25

If A is any ring and $\mathfrak{p} \subset A$ is any prime ideal, then $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p} \cong \operatorname{Frac}(A/\mathfrak{p})$

Proof. Since localization is exact, let $S = A - \mathfrak{p}$, we have two short exact sequences

$$0 \longrightarrow \mathfrak{p} \longrightarrow A \longrightarrow A/\mathfrak{p} \longrightarrow 0$$

$$0 \longrightarrow S^{-1}\mathfrak{p} \longrightarrow A_\mathfrak{p} \longrightarrow S^{-1}(A/\mathfrak{p}) \longrightarrow 0$$

Note that $S^{-1}\mathfrak{p} = \left\{ \frac{p}{s} : p \in \mathfrak{p}, s \in S \right\} = \mathfrak{p}A_\mathfrak{p} \subseteq A_\mathfrak{p}$ is the maximal ideal of $A_\mathfrak{p}$. The surjection $A \to A/\mathfrak{p}$ sends S into $A/\mathfrak{p} - \{0\}$, there is an isomorphism of $S^{-1}A$-modules

$$S^{-1}(A/\mathfrak{p}) \cong \operatorname{Frac}(A/\mathfrak{p})$$

Hence, by exactness of the sequence sequence

$$\frac{A_\mathfrak{p}}{\mathfrak{p}A_\mathfrak{p}} \cong \operatorname{Frac}(A/\mathfrak{p})$$

as S^{-1}-modules □

Chapter 14

HOMEWORK 3

Problem 14.0.1 (chapter 8 problem 2)
Let A be a Noetherian ring. Prove that the following are equivalent

1. A is Artinian
2. $\operatorname{Spec} A$ is discrete and finite
3. $\operatorname{Spec} A$ is discrete

Proof.
$(1 \implies 2)$ A is Artinian then every prime ideal is maximal and it has finitely many maximal ideals, so $\operatorname{Spec} A$ is finite. Moreover, every maximal ideal in $\operatorname{Spec} A$ is closed, so any subset of $\operatorname{Spec} A$ is finite hence closed. $\operatorname{Spec} A$ admits the discrete topology
$(2 \implies 3)$ by definition
$(3 \implies 1)$ Suppose $\mathfrak{p} \subsetneq \mathfrak{m}$ be a prime ideal that is properly contained in a maximal ideal $\mathfrak{m}$ in A. As $\operatorname{Spec} A$ is discrete, $\{\mathfrak{p}\}$ is closed, hence $\{\mathfrak{p}\} = V(\mathfrak{a})$ for some ideal in A, hence $\mathfrak{a} \subseteq \mathfrak{p} \subseteq \mathfrak{m}$, so $\mathfrak{m} \in V(\mathfrak{a})$, contradiction. So every prime ideal in A is maximal, $\dim(A) = 0$. Since A is Noetherian, A is also Artinian ☐

Problem 14.0.2 (chapter 8 problem 3)
Let k be a field and A be a finite-type k-algebra. Prove that the following are equivalent

1. A is Artinian
2. A is a finite k-algebra (finitely generated as k-module)

Proof.
$(2 \implies 1)$ If A is a finite k-algebra then A is a k-vector space of finite dimension. Any ideal in A is a vector subspaces. Since A is of finite dimension, any decending chain stablizes. A is Artinian
$(1 \implies 2)$ A is Artinian, then $A \cong \prod_{i=1}^m A_i$ for some Artinian local ring A_i. A is finite-type k-algebra, then there exists a surjection $k[x_1, ..., x_n] \twoheadrightarrow A$. Hence, each A_i is also finite-type k-algebra by the composition $k[x_1, ..., x_n] \twoheadrightarrow A \twoheadrightarrow A_i$. Note that each A_i is Artinian, moreover if each A_i is a finite k-algebra then A is also a finite k-algebra by taking all generators in $\{A_i\}$.
Without loss of generality, assume $(A, \mathfrak{m})$ is Artinian local. Let $K = A/\mathfrak{m}$ be the residue field, again $k[x_1, ..., x_n] \twoheadrightarrow$

$A \twoheadrightarrow K$, so K is finite-type k-algebra. Since A is Artinian, $l_A(A) = n$ finite, there exists a finite chain of submodules

$$0 = M_0 \subsetneq M_1 \subsetneq \dots \subsetneq M_n = A$$

so that each $M_i/M_{i-1} = A/\mathfrak{m}$ for some maximal ideal $\mathfrak{m}$ of A. Since A is local, each $M_i/M_{i-1} = K$. Moreover,

$$A \cong \bigoplus_{i=1}^{n} M_i/M_{i-1}$$

Hence, A is finite K-algebra. Together with Nullstellensatz, K a finite algebraic extension of k. So A is a finite k-algebra. $\square$

Problem 14.0.3 (chapter 9 problem 2)
Let A be a Dedekind domain. If $f = a_0 + a_1x + \dots + a_nx^n$ is a polynomial with coefficients in A, the content of f is the ideal $c(f) = (a_0, \dots, a_n)$ in A. Prove Gauss's lemma that $c(fg) = c(f)c(g)$

Lemma 14.0.4 (being equal submodules is local)
Let M and N be submodule of an A-module, if $M_\mathfrak{m} = N_\mathfrak{m}$ for every maximal ideal $\mathfrak{m}$ of A then $M = N$.

Proof of Lemma 14.0.4. Note that, $M \subseteq N$ if and only if $(M+N)/N = 0$. Localize at every maximal ideal $\mathfrak{m}$, $M_\mathfrak{m} \subseteq N_\mathfrak{m}$ implies $((M+N)/N)_\mathfrak{m} = (M_\mathfrak{m} + N_\mathfrak{m})/N_\mathfrak{m} = 0$ (localization commutes with sum and quotient of submodules). Since being zero is local, so $M \subseteq N$. The other direction is the same. $\square$

Proof. Let $g = b_0 + b_1x + \dots + b_mx^m$, then

$$fg = \sum_{l=0}^{m+n} \left(\sum_{i=0}^{l} a_i b_{l-i} \right) x^l$$

Localize at every maximal ideal $\mathfrak{m}$ of A, if we can show that

$$c(fg)A_\mathfrak{m} = c(f)A_\mathfrak{m} \cdot c(g)A_\mathfrak{m} = c(f)c(g)A_\mathfrak{m}$$

Then Lemma 14.0.4 implies $c(fg) = c(f)c(g)$. Note that, each $A_\mathfrak{m}$ is a DVR.
Without loss of generality, assume (A, v) is a DVR with uniformizer $y \in A$, $v(y) = 1$. Let $c(f) = (y^s)$ and $c(g) = (y^t)$ for some $s, t \geq 1$, then $c(f)c(g) = (y^{s+t})$. Since $(y^s) = (a_0, \dots, a_n)$, then y^s is a A-linear combination of $\{a_0, a_1, \dots, a_n\}$, then $s = v(y^s) \geq v(a_0)$, but $a_0 \in (y^s)$, so $v(a_0) \geq s$. Hence, $v(a_0) = s$. Similarly, $v(b_0) = t$. Hence, one of the coefficient of $c(fg)$ is a_0b_0 has valuation $v(a_0b_0) = s + t$, so $c(f)c(g) = (y^{s+t}) \subseteq c(fg)$. The other direction is shown above. Hence $c(f)c(g) = (y^{s+t}) = c(fg)$ $\square$

Problem 14.0.5 (chapter 9 problem 3)
A valuation ring (other than a field) is Noetherian if and only if it is a discrete valuation ring.

Definition 14.0.6
A domain A is a valuation ring if every nonzero $x \in K = \mathrm{Frac}(A)$, it is either $x \in A$ or $x^{-1} \in A$

Lemma 14.0.7 (some facts about valuation ring)
If A is a valuation ring

1. there is a total ordering in A by divisibility
2. there is a total ordering of ideals in A by inclustion
3. A is local
4. every finitely generated ideal is principal
5. every ideal $\mathfrak{a}$ in A, if $\mathfrak{a} \subsetneq \mathfrak{m}^k$ then $\mathfrak{a} \subseteq \mathfrak{m}^{k+1}$ for any $k \geq 1$
6. (*is this true?*) every (prime) ideal in A is of the form $\mathfrak{m}^n$

Proof of Lemma 14.0.7.
(1) For any nonzero $x, y \in A$, either $x/y \in A$ or $y/x \in A$. If $x/y \in A$, let $z/1 = x/y$ for $z \in A$. So $t(zy - x) = 0$ for some nonzero $t \in A$. Since A is a domain, $x = zy$. So either x divides y or y divides x
(2) Let $\mathfrak{a}, \mathfrak{b}$ be ideals in A. Suppose there exist $x \in \mathfrak{a} - \mathfrak{b}$ and $y \in \mathfrak{b} - \mathfrak{a}$ ($\mathfrak{a} - \mathfrak{b}$ is set elements in $\mathfrak{a}$ and not in $\mathfrak{b}$). (1) induces a contradiction.
(3) If A is not local, then two distinct maximal ideals $\mathfrak{m}, \mathfrak{n}$ must have $\mathfrak{m} \subsetneq \mathfrak{n}$ or $\mathfrak{n} \subsetneq \mathfrak{m}$. contradiction.
(4) Let $\mathfrak{a} = (a_1, ..., a_n)$ be ideal in A, then there exists a generator a_i that divides every other generator, hence $\mathfrak{a} = (a_i)$
(5) Let $\mathfrak{a} \subsetneq \mathfrak{m}^k$ be any ideal in A for some $k \geq 1$, let $x \in \mathfrak{a}$ and $y \in \mathfrak{m}^k - \{a\}$. Since A is a valuation ring and $y \notin \mathfrak{a}$, $x = ay$ for some $a \in A$. Moreover, if $a \notin \mathfrak{m}$, that is a is a unit, then $a^{-1}x = y$ contradicts with $y \notin A$. Hence, $x = ay$ for some $x \in \mathfrak{m}$. So, $x \in \mathfrak{m}^{k+1}$, $\mathfrak{a} \subseteq \mathfrak{m}^{k+1}$
(6) ☐

Main Proof.
($\Longleftarrow$) DVR is PID, PID is Noetherian since every ideal is generated by finitely many elements.
($\Longrightarrow$) The valuation ring A is Noetherian, then it is local with the unique maximal ideal $\mathfrak{m}$. Since every ideal in A is finitely generated, it is also principal, that is A is PID. A is a Noetherian, local domain with the unique maximal ideal being principal,it suffices to prove that dimension of A is 1, that is, every prime ideal is maximal.
Let $\mathfrak{m} = (y)$ and (x) be a nonzero prime ideal in A, suppose that $(x) \subsetneq (y)$, that means $y \notin (x)$. We must have $x = ay$ for some $a \in \mathfrak{m}$ (using the argument in Lemma 14.0.7). Since (x) is prime, and $y \notin (x)$, $a \in (x)$, write $a = bx$ for some nonzero $b \in A$. So

$$x = byx$$

Since A is a domain, using left cancellation, $by = 1$ that makes y a unit, contradiction. ☐

Problem 14.0.8 (chapter 9 problem 5)
Let M be a finitely generated module over a Dedekind domain. Prove that M is flat $\iff$ M is torsion-free

Definition 14.0.9
Let M be a module over a domain A, M is torsion-free if for every nonzero $x \in M$ and nonzero $a \in A$, $ax \neq 0$

Lemma 14.0.10 (chapter 3 exercise 13)
Let M be a module over a domain A, then M being torsion-free is a local property.

Lemma 14.0.11 (chapter 7 exercise 16)
Let M be a finitely generated module over a Noetherian ring A, then M is flat if and only if $M_\mathfrak{m}$ is a free $A_\mathfrak{m}$-module for every maximal ideal $\mathfrak{m}$

Lemma 14.0.12
free module of finite rank over a domain is torsion free

Proof of Lemma 15.2.1. Let $M = A^n$, then every nonzero $m \in M$ can be written as $m = (a_1, ..., a_n) \in A^n$ for some $a_1, ..., a_n \in A$ and some $a_i \neq 0$. If nonzero $r \in A$ such that $0 = rm = (ra_1, ...ra_n)$, then $ra_i = 0$, contradicts the premise A being a domain. □

Lemma 14.0.13 (Fundamental Theorem, Existence: Invariant Factor Form - Dummit Foote - chapter 12, section 12.1, theorem 5)
Let A be a PID, and M be a finitely generated A-module, then M is torsion-free implies M is free.

Proof. *TODO* □

Main Proof.
Localize at a maximal ideal $\mathfrak{m} \subseteq A$
($\Longrightarrow$) A is Dedekind domain, so A is Noetherian. Since M is finitely generated and flat, $M_\mathfrak{m}$ is a free $A_\mathfrak{m}$-module of finite rank. By Lemma 15.2.1, $M_\mathfrak{m}$ is torsion-free. Lemma 14.0.10 implies M is torsion-free.
($\Longleftarrow$) A is a domain, so $M_\mathfrak{m}$ is also torsion-free as $A_\mathfrak{m}$-module. Moreover, A is Dedekind domain, then $A_\mathfrak{m}$ is a DVR which is PID. By Lemma 15.2.2, $M_\mathfrak{m}$ is free. By Lemma 14.0.11

□

Problem 14.0.14 (chapter 9 problem 7)
Let A be a Dedekind domain and nonzero ideal $\mathfrak{a}$ in A. Show that every ideal in $A/\mathfrak{a}$ is principal. Deduce that every ideal in A can be generated by at most two elements

Proof. Every ideal $\mathfrak{a}$ in Dedekind domain admits a unique decomposition

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} ... \mathfrak{p}_n^{e_n}$$

for some prime ideals $\mathfrak{p}_i$. In dimension 1 domain A, every prime ideal is maximal, by chinese remainder theorem

$$A/\mathfrak{a} = A/\mathfrak{p}_1^{e_1} \times ... \times A/\mathfrak{p}_n^{e_n}$$

Every ideal in $A/\mathfrak{a}$ is a Cartesian product of ideals in $A/\mathfrak{p}_i^{e_i}$, so it suffices to show that ideals in $A/\mathfrak{p}_i^{e_i}$ are principal. Let $\mathfrak{p}^e$ be one of $\mathfrak{p}_1^{e_1}, ..., \mathfrak{p}_n^{e_n}$. Localize each $A/\mathfrak{p}^e$ as quotient of A-modules at $\mathfrak{p} \subseteq A$, we have

$$(A/\mathfrak{p}^e)_\mathfrak{p} = A_\mathfrak{p}/\mathfrak{p}^e A_\mathfrak{p}$$

as $A_{\mathfrak{p}}$ modules. Since A is a Dedekind domain, $A_{\mathfrak{p}}$ is a DVR. In $A_{\mathfrak{p}}$, $\mathfrak{p}A_{\mathfrak{p}}$ is the unique maximal ideal that is principal. So the the unique maximal ideal $\mathfrak{p}A_{\mathfrak{p}} \cap A_{\mathfrak{p}}/\mathfrak{p}^e A_{\mathfrak{p}} \subseteq A_{\mathfrak{p}}/\mathfrak{p}^e A_{\mathfrak{p}}$ is principal. It remains to show that $A_{\mathfrak{p}}/\mathfrak{p}^e A_{\mathfrak{p}}$ is Artinian. It is straightforward since every ideal in DVR $A_{\mathfrak{p}}$ is a power of its maximal ideal $\mathfrak{p}A_{\mathfrak{p}}$, any chain of ideals in $A_{\mathfrak{p}}$ of the form

$$\mathfrak{p}A_{\mathfrak{p}} \supsetneq \ldots \supsetneq \mathfrak{p}^e A_{\mathfrak{p}}$$

is of length at most e. So any chain of ideals in $A_{\mathfrak{p}}/\mathfrak{p}^e A_{\mathfrak{p}}$ is of length at most e

Let $\mathfrak{b} \subseteq A$ be an ideal generated by more than one element. Let $a \in \mathfrak{b}$, then $(a) \subsetneq \mathfrak{b}$. So $\mathfrak{b}/(a)$ is a nonzero ideal in $A/(a)$, hence must be principal. Let $\mathfrak{b}/(a)$ generated by $\bar{b}$ for some $b \in \mathfrak{b}$. Then for any $x \in \mathfrak{b}$, $\mathfrak{b}/(a)$ is principal ideal generated by $\bar{b}$, so $\bar{x} = \bar{y}\bar{b}$ for some $y \in A$, so $x = yb + za$ for some $z \in A$. Hence, $\mathfrak{b} = (a, b)$ ☐

Problem 14.0.15 (chapter 9 problem 8)
Let $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ be three ideals in a Dedekind domain. Prove that

$$\mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c}) = (\mathfrak{a} \cap \mathfrak{b}) + (\mathfrak{a} \cap \mathfrak{c})$$
$$\mathfrak{a} + (\mathfrak{b} \cap \mathfrak{c}) = (\mathfrak{a} + \mathfrak{b}) \cap (\mathfrak{a} + \mathfrak{c})$$

Proof. Localization commutes with finite intersection and sum of submodules, it suffices to prove for the case of DVR. Let $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ be ideals of a DVR (A, v) with uniformizer (y). Let $\mathfrak{a} = (y^a), \mathfrak{b} = (y^b), \mathfrak{c} = (y^c)$, then either case $b = c$ or $b \neq c$,

$$\mathfrak{b} + \mathfrak{c} = (y^b) + (y^c) = (y^{\min(b,c)})$$
$$\mathfrak{b} \cap \mathfrak{c} = (y^b) \cap (y^c) = (y^{\max(b,c)})$$

It is equivalent to show

$$\max(a, \min(b, c)) = \min(\max(a, b), \max(a, c))$$
$$\min(a, \max(b, c)) = \max(\min(a, b), \min(a, c))$$

Assuming $b \leq c$, then $\max(a, b) \leq \max(a, c)$ and $\min(a, b) \leq \min(a, c)$. We're done. ☐

Problem 14.0.16 (Krull–Akizuki)
Let A be a Dedekind domain with fractional field K. Let L/K be a finite degree field extension and let B be the integral closure of A in L. Prove that B is a Dedekind domain.

Lemma 14.0.17 (equivalent formulation for Dedekind domain)
A ring A is a Dedekind domain if and only if it is a dimension 1 Noeatherian integrally closed domain

Proof of Lemma 15.2.3. this follows from Proposition 5.13: for a domain A being integrally closed is local. ☐

Main Proof. L is a finite degree field extension of K which is a vector of finite dimension over K. $B \subseteq L$ is the integral closure of the ring extension $A \hookrightarrow L$

$$A \hookrightarrow B \hookrightarrow L$$

1. (Any ideal I of B intersects A nontrivially) Let nonzero $I \subseteq B$ be an ideal of B, let nonzero $x \in I$, then x satisfies a monic polynomial of minimal degree

$$p(x) = x^n + a_1 x^{n-1} + ...a_{n-1}x - a_n = 0$$

for some $a_1, ..., a_n \in A$. Since p is of minimal degree, $a = a_n$ is a nonzero element of the ideal $I \cap A$.

2. (I/aB is of finite length as an A-module) Now, $I/aB \subseteq B/aB$ as R-modules. It suffices to show that length B/aB is of finite length. If $aB = B = I$, there is nothing to show. Suppose a is not a unit in B

   If we can show that $a^n B \subseteq a^{n+1}B + A$ for some n, then

$$\frac{B}{aB} \cong \frac{a^n B}{a^{n+1}B} \subseteq \frac{a^{n+1}B + A}{a^{n+1}B} \cong \frac{A}{a^{n+1}B \cap A}$$

   The left isomorphism is from first isomorphism theorem of the map $a^n(-) : B \to a^n B/a^{n+1}B$ with $\ker a^n(-) = aB$ and the right isomorphism is the second isomorphism theorem for submodules over A. $A/(a^{n+1}B \cap A)$ is Artinian since $a^{n+1}B \cap A$ is nonzero, so B/aB is of finite length as an A-module, hence I/aB is of finite length

3. ($a^n B \subseteq a^{n+1}B + A$ for some n) Using the argument in Lemma 14.0.4, inclusion of submodules is a local, We can assume that A is a DVR with uniformizer $\mathfrak{m}$.

   For any nonzero $y \in B$, consider the "fractional ideal" $y^{-1}A = \{z \in L : zy \in A\} \subseteq L$ intersecting A nontrivally using the same argument as above for integral element y^{-1} over A. Since A is a DVR, the ideal $Ay^{-1} \cap A$ of A contains large power of $\mathfrak{m}$. Since $a \in \mathfrak{m}$, we choose smallest $N_1 \in \mathbb{N}$ so that $a^n y \in A$ for every $n \geq N_1$

   Consider the chain of ideals $I_n = a^n B \cap A + aA$ in A/aA. A/aA is Artinian since aA is nonzero, so it must stablize. Let $N_2 \in \mathbb{N}$ so that $I_n = I_{N_2}$ for every $n \geq N_2$.

   Note that, N_1 is dependent on y and N_2 is indepdent of y. We claim that $N_1 \leq N_2 + 1$ for every $y \in B$. Suppose the contrary that if $N_2 + 1 < N_1$, let $n = N_1 - 1$, then $I_{n+1} = I_n = I_{n-1}$, then $a^n y \notin A$ and $a^{n+1}y \in A$. Since $a^{n+1}y \in I_{n+1} = I_n = I_{n-1}$, then there exists $z \in B$ and $t \in A$ so that $a^{n-1}z \in A$ and

$$a^{n+1}y = a^n z + at \in a^{n-1}B \cap A + aA$$

   Hence, left cancellation implies $a^n y = a^{n-1}z + t \in A$, contradiction. Choose $n = N_2 + 1$, then $I_n = I_{n+1}$ and $a^n B \subseteq A$. Hence

$$a^n B \subseteq I_n = I_{n+1} \subseteq a^{n+1}B + A$$

4. (B is Noetherian) I/aB is of finite length as an A-module, if I is not finitely generated as an ideal in B, then let $I = (a, i_1, i_2, ...)$ for $i_1, i_2, ... \in B$, so the decending chain of ideals containing aB in B which is also a decending chain of submodule of I/aB as an A-module

$$(a, i_1, i_2, i_3, ...) \supseteq (a, i_2, i_3, ...) \supseteq ... \supseteq (a) \supseteq (0)$$

   has infinitely many strict inclusions, contradiction.

5. (B is of dimension 1) $A \hookrightarrow B$ is an integral ring extension with A being a domain, by going-down theorem, any chain of prime ideals of strict inclusions in B has a corresponding chain of prime ideals of strict inclusions in A by contraction. Since A is of dimension 1, by going-up theorem, all chain of prime ideals of strict inclusions in B cannot be longer than 2. Hence, since B is subring of field L, B is domain, (0) is prime, B is of dimension 1

6. (B is integrally closed) $\mathrm{Frac}(B) \subseteq L$. Any $x \in \mathrm{Frac}(B)$ is integral over B is also integral over A, so $x \in B$. Hence, B is integrally closed.

$\square$

Problem 14.0.18 (optional)
In the notation of the previous problem, if in addition L/K is a separable extension, we can always write $L = K(x)$ for some $x \in L$. Find an example where L/K is separable but we CANNOT write $B = A[x]$ for some $x \in B$

Problem 14.0.19 (optional)
Is the ring $A = \mathbb{C}[x, y]/(y^2 - x^3 - x - 1)$ a PID?

Chapter 15

HOMEWORK 4

15.1 PROBLEM 1 2 3

> **Problem 15.1.1** (problem 1)
> Let $P_\bullet$ and $Q_\bullet$ be projective resolutions of A-modules M and N, respectively. In class we proved that any A-module map $f : M \to N$ lifts to a chain complex map $\phi_\bullet : P_\bullet \to Q_\bullet$, but the lift depends on choices. Prove that any two lifts $\phi_\bullet, \psi_\bullet$ are homotopic.

Proof. Note that, the proof only requires $P_\bullet$ to be projective chain complex and $Q_\bullet$ to be exact. Recall the construction of lifts of f. Let $K_n = \ker(d : Q_n \to Q_{n-1}) = \mathrm{im}(d : Q_{n+1} \to Q_n)$, then there is a map $\alpha_n : P_{n+1} \to K_n$. Since P_{n+1} is projective, α_n lifts into $\phi_{n+1} : P_{n+1} \to Q_{n+1}$

$$\begin{tikzcd}
P_{n+2} \arrow[rr, "d"] \arrow[dr, dashed, "\alpha_n"] & & P_{n+1} \arrow[rr, "d"] \arrow[dd, dashed, "\phi_{n+1}"] \arrow[dr, "\alpha_n"] & & P_n \arrow[dd, "\phi_n"] \\
 & K_{n+1} \arrow[dr, hook] & & K_n \arrow[dr, hook] & \\
Q_{n+2} \arrow[rr, "d"] \arrow[ur, two heads] & & Q_{n+1} \arrow[rr, "d"] \arrow[ur, two heads] & & Q_n
\end{tikzcd}$$

Now, the composition $P_{n+2} \to P_{n+1} \to Q_{n+1} \to Q_n$ equals $P_{n+2} \to P_{n+1} \to P_n \to Q_n$ equals zero. Hence the map $P_{n+2} \to P_{n+1} \to Q_{n+1}$ factors through K_{n+1} by a map $\alpha_{n+1} : P_{n+2} \to Q_{n+1}$.
Let $g_n = \phi_n - \psi_n$, then $g_\bullet$ is a chain map, we will show by induction that there exists a collection of maps $\{h_i : P_{i-1} \to Q_i\}_{i \in \mathbb{N}}$ so that

$$g_i = h_i d + d h_{i+1}$$

where d are the appropriate maps on exact sequences $P_\bullet$ and $Q_\bullet$.
Induction case: Suppose we have maps $h_n : P_{n-1} \to Q_n$ and $h_{n-1} : P_{n-2} \to Q_{n-1}$ for some $n - 1 \geq 0$, so that

$$g_{n-1} = h_{n-1} d + d h_n$$

We construct $h_{n+1} : P_{n+2} \to Q_{n+1}$ as follows:

$$\begin{tikzcd}
P_n \arrow[r, "d"] \arrow[d, "g_n"'] & P_{n-1} \arrow[dl, "h_n"] \\
Q_n \arrow[r, "d"'] & Q_{n-1}
\end{tikzcd}$$

Consider the map $\beta_n = g_n - h_n d : P_n \to Q_n$ and the composition $d\beta_n : P_n \to Q_{n-1}$, we have

$$\begin{aligned}
d\beta_n &= d(g_n - h_n d) \\
&= dg_n - dh_n d && (A\text{-module is preadditive}) \\
&= dg_n - (g_{n-1} - h_{n-1}d)d && (\text{induction hypothesis}) \\
&= dg_n - g_{n-1}d + h_{n-1}dd && (A\text{-module is preadditive}) \\
&= dg_n - g_{n-1}d && (\text{top sequence is a chain complex}) \\
&= 0 && (g_\bullet \text{ is a chain map})
\end{aligned}$$

Then, β_n factors through K_n by a map $P_n \to K_n$, since P_n is projective, it factors through Q_{n+1} by a map $h_{n+1} : P_n \to Q_{n+1}$

$$\begin{tikzcd}
& & P_n \arrow[dl, dashed] \arrow[dd, "\beta_n"] \arrow[ddll, dashed, bend right, "h_{n+1}"'] & \\
& K_n \arrow[dr] & & \\
Q_{n+1} \arrow[ur, two heads] \arrow[rr, "d"'] & & Q_n \arrow[r, "d"'] & Q_{n-1}
\end{tikzcd}$$

Precisely, we have $\beta_n = dh_{n+1}$. Hence, $g_n = h_n d + dh_{n+1}$

Case case: We construct $h_0 : 0 \to Q_0$ and $h_1 : P_0 \to Q_1$ as follows:

$$\begin{tikzcd}
& P_0 \arrow[r] \arrow[dl, "h_1"'] \arrow[d, "g_0"] & 0 \arrow[dl, "h_0"] \\
Q_1 \arrow[r, two heads, "d"'] & Q_0 \arrow[r] & 0
\end{tikzcd}$$

$h_0 = 0$ is the unique zero map. P_0 is projective, so $g_0 = \phi_0 - \psi_0$ factors through Q_1 by a map $h_1 : P_0 \to Q_1$, then $g_0 = dh_1 = dh_1 + h_0 d$ ☐

Problem 15.1.2 (problem 2)

Let $P_\bullet$ and $Q_\bullet$ be projective resolution of an A-module M. Prove that they are homotopy equivalent

Proof. The lifting from a map in A-modules into chain complexes of A-modules is a functor, that is if $f_\bullet, g_\bullet$ are lifts of f, g, then $g_\bullet \circ f_\bullet$ is a lift of $g \circ f$

$$\begin{tikzcd}
L \arrow[r, "f"'] \arrow[rr, bend left, "g\circ f"] & M \arrow[r, "g"'] & N
\end{tikzcd}$$

$$\begin{tikzcd}
P_\bullet \arrow[r, "f_\bullet"] \arrow[rr, bend right, "g_\bullet\circ f_\bullet"'] & Q_\bullet \arrow[r, "g_\bullet"] & R_\bullet
\end{tikzcd}$$

Hence, the identity map $1_M : M \to M$ lifts into 2 chain maps $f_\bullet : P_\bullet \to Q_\bullet$, $g_\bullet : Q_\bullet \to P_\bullet$ as in the diagram below

$$\begin{tikzcd} M \arrow[r, "1_M"'] \arrow[rr, bend left, "1_M"] & M \arrow[r, "1_M"'] & M \end{tikzcd}$$

$$\begin{tikzcd} P_\bullet \arrow[r, "f_\bullet"] \arrow[rr, bend right, "g_\bullet \circ f_\bullet"'] & Q_\bullet \arrow[r, "g_\bullet"] & P_\bullet \end{tikzcd}$$

Then, $g_\bullet \circ f_\bullet$ is also lift of $1_M : M \to M$. On the other hand, the identity chain map $1_{P_\bullet} : P_\bullet \to P_\bullet$ is also a lift of $1_M : M \to M$, by Problem 15.1.1, $g_\bullet \circ f_\bullet \sim 1_{P_\bullet}$. Using the same argument, $f_\bullet \circ g_\bullet \sim 1_{Q_\bullet}$, hence $P_\bullet$ and $Q_\bullet$ are homotopy equivalent.

∎

Problem 15.1.3 (problem 3)
If $0 \to L \to M \to N \to 0$ is a short exact sequence of A-modules, prove that we can find a compatible short exact sequence of projective resolutions $0 \to P_\bullet \to Q_\bullet \to R_\bullet \to 0$

Proof. Pick arbitrary projective resolutions $P_\bullet$ and $R_\bullet$ of L and N respectively. We will show by induction that there exists a projective resolution $Q_\bullet$ of M so that $0 \to P_\bullet \to Q_\bullet \to R_\bullet \to 0$ is a short exact sequence.
Let $Q_n = P_n \oplus R_n$ and the canonical maps $f_n : P_n \hookrightarrow Q_n$ and $g_n : Q_n \twoheadrightarrow R_n$, we will construct maps $Q_0 \to M$ and $Q_{n+1} \to Q_n$ so that $Q_\bullet$ is a projective resolution of M. Note that, since both P_n and R_n are projective, Q_n is also projective.
Induction case: For any $n \geq 0$, suppose we have a commutative diagram as follows (does not include dash arrows), all rows are exact, all columns split

$$\begin{tikzcd} & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\ \dots \arrow[r] & P_{n+1} \arrow[r, "d"] \arrow[d, hook, "f_{n+1}"] & P_n \arrow[r, "d"] \arrow[d, hook, "f_n"] & P_{n-1} \arrow[r] \arrow[d, hook, "f_{n-1}"] & \dots \\ \dots \arrow[r, dashed] & Q_{n+1} \arrow[r, dashed, "f_n d \oplus r_n d"] \arrow[d, two heads, "g_{n+1}"] & Q_n \arrow[r, "h"] \arrow[d, two heads, "g_n"] & Q_{n-1} \arrow[r] \arrow[d, two heads, "g_{n-1}"] & \dots \\ \dots \arrow[r] & R_{n+1} \arrow[r, "d"'] \arrow[d] \arrow[u, bend left, "r_{n+1}"] & R_n \arrow[r, "d"] \arrow[d] \arrow[u, bend left, "r_n"] & R_{n-1} \arrow[r] \arrow[d] \arrow[u, bend left, "r_{n-1}"] & \dots \\ & 0 & 0 & 0 & \end{tikzcd}$$

Let the map $Q_{n+1} \to Q_n$ be $f_n d \oplus r_n d$. The sequence $Q_\bullet$ is exact at Q_n since

$$\begin{aligned} &\operatorname{im}(f_n d \oplus r_n d) \\ &= \operatorname{im}(d : P_{n+1} \to P_n) \oplus \operatorname{im}(d : R_{n+1} \to R_n) \\ &= \ker(d : P_n \to P_{n-1}) \oplus \ker(d : R_n \to R_{n-1}) \\ &= \ker h \end{aligned}$$

Base case: Since $M \twoheadrightarrow N$ is surjective and R_0 is projective, there is a map $\phi : R_0 \to M$ lifted from $\eta : R_0 \to N$. Let the map $Q_0 \to M$ be $f\epsilon \oplus \phi$

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & \\
\ldots \arrow[r] & P_0 \arrow[r, two heads, "\epsilon"] \arrow[d, hook] & L \arrow[r] \arrow[d, hook, "f"] & 0 \\
\ldots \arrow[r, dashed] & P_0 \oplus R_0 \arrow[r, dashed, two heads, "f\epsilon\oplus\phi"] \arrow[d, two heads] & M \arrow[r] \arrow[d, two heads] & 0 \\
\ldots \arrow[r] & R_0 \arrow[r, two heads, "\eta"'] \arrow[d] \arrow[ur, dashed, "\phi"] & N \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 &
\end{tikzcd}$$

It remains to show that $f\epsilon \oplus \phi$ is surjective. By snake lemma,

$$0 = \operatorname{coker} \epsilon \to \operatorname{coker}(f\epsilon \oplus \phi) \to \operatorname{coker} \eta = 0$$

is exact. Hence, $\operatorname{coker}(f\epsilon \oplus \phi) = 0$, $f\epsilon \oplus \phi$ is surjective.

□

15.2 PROBLEM 4

Lemma 15.2.1

Some basic facts about Tor

1. If L is a flat A-module, then $\operatorname{Tor}_n^A(-, L) = 0$ for $n \geq 1$
2. If P is a projective A-module, then $\operatorname{Tor}_n^A(P, -) = 0$ for $n \geq 1$.
3. If P is a projective A-module, then P is flat. Hence, $\operatorname{Tor}_n^A(-, P) = 0$ for $n \geq 1$.

Proof.

($\operatorname{Tor}_n(-, L) = 0$ for $n \geq 1$) Let $\ldots \to Q_2 \to Q_1 \to Q_0 \to 0$ be a projective resolution of N, since L is flat, $\ldots \to Q_2 \otimes L \to Q_1 \otimes L \to Q_0 \otimes L \to 0$ is exact at every $Q_n \otimes L$ for $n \geq 1$. Hence, $\operatorname{Tor}_n(-, L) = 0$ for $n \geq 1$

($\operatorname{Tor}_n(P, -) = 0$ for $n \geq 1$) A projective resolution for P is $0 \to P \to P \to 0$

(P is flat) Let $Q \oplus P$ be a free module, hence also flat. Given any injection $M \hookrightarrow N$. In the diagram below, all columns split and the middle sequence is exact

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] \\
 & M \otimes P \arrow[r] \arrow[d] & N \otimes P \arrow[d] \\
0 \arrow[r] & M \otimes (P \oplus Q) \arrow[r, hook] \arrow[d] & N \otimes (P \oplus Q) \arrow[d] \\
 & M \otimes Q \arrow[r] \arrow[d] & N \otimes Q \arrow[d] \\
 & 0 & 0
\end{tikzcd}$$

By snake lemma, $0 \to \ker(M \otimes P \to N \otimes P) \to 0$ is exact. So, $(- \otimes P)$ preserves injection

□

Lemma 15.2.2

If $0 \to M \to N \to P \to 0$ is a short exact sequence of A-modules with P being projective, then for any A-modules, the sequence

$$0 \to M \otimes J \to N \otimes J \to P \otimes J \to 0$$

is also exact

Proof. P being projective, so $1_P : P \to P$ factors through N, that is, the sequence $0 \to M \to N \to P \to 0$ splits. $N = M \oplus P$. So

$$N \otimes J = (M \otimes J) \oplus (P \otimes J)$$

The induced maps $M \otimes J \to N \otimes J$ and $N \otimes J \to P \otimes J$ from $(- \otimes J)$ are precisely the canonical injection and canonical projection

$$\begin{tikzcd}
M \arrow[r, "f"] & N \arrow[r, "g"] & P \\
m \arrow[r, mapsto, "f"] & (m,0) & \\
& (m,p) \arrow[r, mapsto, "g"] & p
\end{tikzcd}$$

$$\begin{tikzcd}
M \otimes J \arrow[r, "f\otimes 1"] & N \otimes J \arrow[r, "g\otimes 1"] & P \otimes J
\end{tikzcd}$$

$$m \otimes j_1 \xmapsto{f\otimes 1} (m,0) \otimes j_1 = (m \otimes j_1, 0)$$

$$(m \otimes j_2, p \otimes j_2) = (m,p) \otimes j_2 \xmapsto{g\otimes 1} p \otimes j_2$$

Hence, $0 \to M \otimes J \to N \otimes J \to P \otimes J \to 0$ also splits $\square$

Lemma 15.2.3

Tensor product preserves chain complex and chain homotopy, that is

1. If $C_\bullet$ is a chain complex then $C_\bullet \otimes J$

$$\ldots \to C_{n+1} \otimes J \to C_n \otimes J \to C_{n-1} \otimes J \to \ldots$$

is also a chain complex for any A-module J.

2. If $f_\bullet, g_\bullet : C_\bullet \to D_\bullet$ are chain homotopic by a chain homotopy $h_\bullet$, then

$$\begin{tikzcd}
& C_n \arrow[r, "d"] \arrow[dl, "h_{n+1}"'] & C_{n-1} \arrow[dl, "h_n"] \\
D_{n+1} \arrow[r, "d"] & D_n &
\end{tikzcd}
\qquad
\begin{tikzcd}
& C_n \otimes J \arrow[r, "Fd"] \arrow[dl, "Fh_{n+1}"'] & C_{n-1} \otimes J \arrow[dl, "Fh_n"] \\
D_{n+1} \otimes J \arrow[r, "Fd"] & D_n \otimes J &
\end{tikzcd}$$

$Fh_\bullet$ is also a chain homotopy where $F(-)$ denotes the tensor product $(- \otimes J)$ functor

Proof. We write $F(-)$ for the functor $(- \otimes J)$

(Tensor product preserves chain complex)

$$(Fd)(Fd) = F(dd) = 0$$

(Tensor product preserves chain homotopy)

$$\begin{aligned}
&(Fd)(Fh_{n+1}) + (Fh_n)(Fd) \\
&= F(dh_{n+1}) + F(h_n d) && (F \text{ is a functor}) \\
&= F(dh_{n+1} + h_n d) && (F \text{ is additive}) \\
&= F(f_n - g_n) && (f_\bullet \sim g_\bullet \text{ by } h_\bullet) \\
&= F(f_n) - F(g_n) && (F \text{ is a functor})
\end{aligned}$$

□

Lemma 15.2.4

Let $0 \to L \to M \to N \to 0$ be a short exact sequence of A-modules, then

1. (version 1) there exists a natural long exact sequence of A-modules

$$\begin{tikzcd}
& \dots \arrow[r] & \mathrm{Tor}_2(J,N) \arrow[dll] \\
\mathrm{Tor}_1(J,L) \arrow[r] & \mathrm{Tor}_1(J,M) \arrow[r] & \mathrm{Tor}_1(J,N) \arrow[dll] \\
J \otimes L \arrow[r] & J \otimes M \arrow[r] & J \otimes N \arrow[r] & 0
\end{tikzcd}$$

2. (version 2) there exists a natural long exact sequence of A-modules

$$\begin{tikzcd}
& \dots \arrow[r] & \mathrm{Tor}_2(N,J) \arrow[dll] \\
\mathrm{Tor}_1(L,J) \arrow[r] & \mathrm{Tor}_1(M,J) \arrow[r] & \mathrm{Tor}_1(N,J) \arrow[dll] \\
L \otimes J \arrow[r] & M \otimes J \arrow[r] & N \otimes J \arrow[r] & 0
\end{tikzcd}$$

Proof.

(version 1) Let $P_\bullet$ be a projective resolution of J, by Lemma 15.2.1 each P_n is flat, hence

$$0 \to P_\bullet \otimes L \to P_\bullet \otimes M \to P_\bullet \otimes N \to 0$$

is a short exact sequence of chain complexes (rows are exact by Lemma 15.2.1, columns are chain complexes by Lemma 15.2.3). By fundamental lemma of homological algebra, there is a natual long exact sequence

$$\begin{tikzcd}
& \dots \arrow[r] & H_2(P_\bullet \otimes N) \arrow[dll] \\
H_1(P_\bullet \otimes L) \arrow[r] & H_1(P_\bullet \otimes M) \arrow[r] & H_1(P_\bullet \otimes N) \arrow[dll] \\
H_0(P_\bullet \otimes L) \arrow[r] & H_0(P_\bullet \otimes M) \arrow[r] & H_0(P_\bullet \otimes N) \arrow[r] & 0
\end{tikzcd}$$

Since $(- \otimes L)$ and $(- \otimes M)$ are right exact, the rows in bottom diagram are exact.

$$\begin{tikzcd} & & L \arrow[d, "f"] & \\ & & M & \end{tikzcd}$$

$$\begin{tikzcd} P_1 \otimes L \arrow[r] \arrow[d] & P_0 \otimes L \arrow[r] \arrow[d] & J \otimes L \arrow[r] \arrow[d, "1\otimes f"] & 0 \\ P_1 \otimes M \arrow[r] & P_0 \otimes M \arrow[r] & J \otimes M \arrow[r] & 0 \end{tikzcd}$$

Hence,

$$H_0(P_\bullet \otimes L) = \frac{\ker(P_0 \otimes L \to 0)}{\operatorname{im}(P_1 \otimes L \to P_0 \otimes L)} = \frac{P_0 \otimes L}{\operatorname{im}(d : P_1 \otimes L \to P_0 \otimes L)} = \operatorname{coker}(P_1 \otimes L \to P_0 \otimes L) = J \otimes L$$

and the map $1 \otimes f : J \otimes L \to J \otimes M$ is precisely the induced map from $P_0 \otimes L \to P_0 \otimes M$ into its map in homology.
(version 2) Let $P_\bullet, Q_\bullet, R_\bullet$ be projective resolutions of M, N, L in Problem 15.1.3, then

$$0 \to P_\bullet \otimes J \to Q_\bullet \otimes J \to R_\bullet \otimes J \to 0$$

is also a short exact sequence of chain complexes (rows are exact by Lemma 15.2.2, columns are chain complexes by Lemma 15.2.3). By fundamental lemma of homological algebra, there is a natual long exact sequence

$$\begin{tikzcd} & \dots \arrow[r] & H_2(R_\bullet \otimes J) \arrow[dll] & \\ H_1(P_\bullet \otimes J) \arrow[r] & H_1(Q_\bullet \otimes J) \arrow[r] & H_1(R_\bullet \otimes J) \arrow[dll] & \\ H_0(P_\bullet \otimes J) \arrow[r] & H_0(Q_\bullet \otimes J) \arrow[r] & H_0(R_\bullet \otimes J) \arrow[r] & 0 \end{tikzcd}$$

Since $(- \otimes J)$ is right exact, the rows in bottom diagram are exact

$$\begin{tikzcd} P_1 \arrow[r] \arrow[d] & P_0 \arrow[r] \arrow[d] & L \arrow[r] \arrow[d, "f"] & 0 \\ Q_1 \arrow[r] & Q_0 \arrow[r] & M \arrow[r] & 0 \end{tikzcd}$$

$$\begin{tikzcd} P_1 \otimes J \arrow[r] \arrow[d] & P_0 \otimes J \arrow[r] \arrow[d] & L \otimes J \arrow[r] \arrow[d, "f\otimes 1"] & 0 \\ Q_1 \otimes J \arrow[r] & Q_0 \otimes J \arrow[r] & M \otimes J \arrow[r] & 0 \end{tikzcd}$$

Hence,

$$H_0(P_\bullet \otimes J) = \frac{\ker(P_0 \otimes J \to 0)}{\operatorname{im}(P_1 \otimes J \to P_0 \otimes J)} = \frac{P_0 \otimes J}{\operatorname{im}(P_1 \otimes J \to P_0 \otimes J)} = \operatorname{coker}(P_1 \otimes J \to P_0 \otimes J) = L \otimes J$$

and the map $(f \otimes 1) : L \otimes J \to M \otimes J$ is precisely the induced map from $P_0 \otimes J \to Q_0 \otimes J$ into its map in homology. $\square$

Problem 15.2.5 (problem 4)
For A-modules M and N, we define $\operatorname{Tor}_i^A(M, N) = H_i(P_\bullet \otimes_A N)$ where $P_\bullet$ is a projective resolution of M. Prove that $\operatorname{Tor}_i^A(M, N) \cong \operatorname{Tor}_i^A(N, M)$

Proof. Let $\ldots \to P_2 \to P_1 \to P_0 \to M \to 0$ be a projective resolution of M, we have the following diagonal short exact sequences

$$\begin{tikzcd}
0 \arrow[dr] & & & & 0 \arrow[dr] & & 0 & & & \\
& K_3 \arrow[dr, hook] & & & & K_1 \arrow[ur] \arrow[dr, hook] & & & & \\
\ldots \arrow[rr] & & P_2 \arrow[rr, "d"] \arrow[dr, two heads] & & P_1 \arrow[rr, "d"] \arrow[ur, two heads] & & P_0 \arrow[rr, "\epsilon"] \arrow[dr, two heads] & & M \arrow[r] & 0 \\
& & & K_2 \arrow[ur, hook] \arrow[dr] & & & & M \arrow[dr] & & \\
& & 0 \arrow[ur] & & 0 & & & & 0 &
\end{tikzcd}$$

where $K_1 = \ker(\epsilon : P_0 \to M)$ and $K_n = \ker(d : P_{n-1} \to P_{n-2})$. For any $n \geq 1$, the map $P_n \to K_n$ is lifted from $d : P_n \to P_{n-1}$ since the composition $P_n \to P_{n-1} \to P_{n-2}$ is zero[1]. Since $K_n = \operatorname{im}(d : P_n \to P_{n-1})$, $P_n \to K_n$ is surjective, hence every diagonal sequence is exact.

From $0 \to K_1 \to P_0 \to M \to 0$, for any $n \geq 0$, by Lemma 15.2.4 we have two exact sequences

$$0 = \operatorname{Tor}_{n+1}(P_0, N) \longrightarrow \operatorname{Tor}_{n+1}(M, N) \longrightarrow \operatorname{Tor}_n(K_1, N) \longrightarrow \operatorname{Tor}_n(P_0, N) = 0$$

$$0 = \operatorname{Tor}_{n+1}(N, P_0) \longrightarrow \operatorname{Tor}_{n+1}(N, M) \longrightarrow \operatorname{Tor}_n(N, K_1) \longrightarrow \operatorname{Tor}_n(N, P_0) = 0$$

Hence, $\operatorname{Tor}_{n+1}(M, N) = \operatorname{Tor}_n(K_1, N)$ and $\operatorname{Tor}_{n+1}(N, M) = \operatorname{Tor}_n(N, K_1)$

From $0 \to K_2 \to P_1 \to K_1 \to 0$, for any $n \geq 0$, by Lemma 15.2.4 we have two exact sequences

$$0 = \operatorname{Tor}_{n+1}(P_1, N) \longrightarrow \operatorname{Tor}_{n+1}(K_1, N) \longrightarrow \operatorname{Tor}_n(K_2, N) \longrightarrow \operatorname{Tor}_n(P_1, N) = 0$$

$$0 = \operatorname{Tor}_{n+1}(N, P_1) \longrightarrow \operatorname{Tor}_{n+1}(N, K_1) \longrightarrow \operatorname{Tor}_n(N, K_2) \longrightarrow \operatorname{Tor}_n(N, P_1) = 0$$

Similarly, we have $\operatorname{Tor}_{n+1}(K_1, N) = \operatorname{Tor}_n(K_2, N)$ and $\operatorname{Tor}_{n+1}(N, K_1) = \operatorname{Tor}_n(K_2, N)$. Hence

$$\operatorname{Tor}_{n+1}(M, N) = \operatorname{Tor}_n(K_1, N) = \operatorname{Tor}_{n-1}(K_2, N) = \ldots = \operatorname{Tor}_1(K_n, N)$$
$$\operatorname{Tor}_{n+1}(N, M) = \operatorname{Tor}_n(N, K_1) = \operatorname{Tor}_{n-1}(N, K_2) = \ldots = \operatorname{Tor}_1(N, K_n)$$

From $0 \to K_{n+1} \to P_n \to K_n \to 0$, for any $n \geq 0$, by Lemma 15.2.1 and Lemma 15.2.4 we have two exact sequences

$$\begin{tikzcd}
0 = \operatorname{Tor}_1(P_n, N) \arrow[r] \arrow[d, "\sim"] & \operatorname{Tor}_1(K_n, N) \arrow[r] \arrow[d, dashed] & K_{n+1} \otimes N \arrow[r] \arrow[d, "\sim"] & P_n \otimes N \arrow[r] \arrow[d, "\sim"] & K_n \otimes N \arrow[r] & 0 \\
0 = \operatorname{Tor}_1(N, P_n) \arrow[r] & \operatorname{Tor}_1(N, K_n) \arrow[r] & N \otimes K_{n+1} \arrow[r] & N \otimes P_n \arrow[r] & N \otimes K_n \arrow[r] & 0
\end{tikzcd}$$

By five lemma, there is an isomorphism $\operatorname{Tor}_1(K_n, N) \xrightarrow{\sim} \operatorname{Tor}_1(N, K_n)$ completing the squares. Hence

$$\operatorname{Tor}_{n+1}(M, N) \cong \operatorname{Tor}_{n+1}(N, M)$$

for any $n \geq 0$. In Lemma 15.2.4, we showed that $\operatorname{Tor}_0(M, N) = M \otimes N$. So $\operatorname{Tor}_n(M, N) \cong \operatorname{Tor}_n(N, M)$ for any $n \geq 0$. $\square$

[1] $P_{-1} = M$

Remark 15.2.6 (dimension shifting)
The technique is called *dimension shifting*, one can realize it in a different way. The exact sequence $\ldots \to P_{n+1} \to P_n \to P_{n-1} \to K_{n-1} \to 0$ is a projective resolution of K_n, tensoring with N and taking homology gives

$$\mathrm{Tor}_1(K_{n-1}, N) = \mathrm{Tor}_n(M, N)$$

since $\ldots \to P_{n+1} \to P_n \to P_{n-1} \to 0$ is an subsequence of $\ldots \to P_2 \to P_1 \to P_0 \to 0$ but shifted by n positions. More generally, let L_nF be a left derived functor of a covariant functor, we have

$$(L_nF)(M) = (L_{n-1}F)(K_0) = \ldots = (L_1F)(K_{n-1})$$

Similarly, we also have a version for right derived functor.

15.3 PROBLEM 5

Problem 15.3.1 (problem 5)
Let N be an A-module, then the following are equivalent

1. $\mathrm{Tor}_i^A(-, N) = 0$ for any $i \geq 1$
2. $\mathrm{Tor}_1^A(-, N) = 0$
3. N is flat

Proof.
$(3 \implies 1)$ Lemma 15.2.1
$(1 \implies 2)$ clear
$(2 \implies 3)$ Let $f : M \hookrightarrow L$ be an injective map, then the short exact sequence $0 \to M \to L \to \operatorname{coker} f \to 0$ induces an exact sequence

$$0 = \mathrm{Tor}_1(\operatorname{coker} f, N) \to M \otimes N \to L \otimes N$$

$\mathrm{Tor}_1(\operatorname{coker} f, N) = 0$ implies $(- \otimes N)$ preserves injective map. $\square$

15.4 PROBLEM 6

In this section, we will denote Ext_r for the version of Ext calculated using injective resolution and Ext_l for the version of Ext calculated using projective resolution

Problem 15.4.1 (problem 6)
Prove that $\mathrm{Ext}_A^i(M, N)$ can be computed using either projective resolution of M or an injective resolution of N

Proof. Let $0 \to N \to I^0 \to I^1 \to I^2 \to \ldots$ be a injective resolution of N, we have the following diagonal short exact sequences

$$
\begin{tikzcd}
 & & & 0 \arrow[dr] & & 0 & & & & 0 \\
 & & & & C^1 \arrow[ur] \arrow[dr, hook] & & & & C^3 \arrow[ur] & \\
0 \arrow[r] & N \arrow[rr, hook, "\epsilon"] & & I^0 \arrow[rr, "d"] \arrow[ur, two heads] & & I^1 \arrow[rr, "d"] \arrow[dr, two heads] & & I^2 \arrow[rr, "d"] \arrow[ur, two heads] & & ... \\
 & & N \arrow[ur, hook] & & & & C^2 \arrow[ur, hook] \arrow[dr] & & & \\
 & 0 \arrow[ur] & & & & 0 \arrow[ur] & & 0 & &
\end{tikzcd}
$$

where $C^1 = \mathrm{coker}(\epsilon : N \to I^0)$ and $C^n = \mathrm{coker}(d : I^{n-2} \to I^{n-1})$. For any $n \geq 1$, the map $C^n \to I^n$ lifted from $d : I^{n-1} \to I^n$ since the composition $I^{n-2} \to I^{n-1} \to I^n$ is zero [2]. Since

$$C^n = \frac{I^{n-1}}{\mathrm{im}(d : I^{n-2} \to I^{n-1})} = \frac{I^{n-1}}{\ker(d : I^{n-1} \to I^n)} = \mathrm{im}(d : I^{n-1} \to I^n) = \ker(d : I^n \to I^{n+1}) \hookrightarrow I^n$$

$C^n \to I^n$ is injective. Hence, every diagonal sequence is exact.

Dimension shifting 15.2.6 for right derived functor $\mathrm{Ext}_r(M, -)$

$$\mathrm{Ext}_r^{n+1}(M, N) = \mathrm{Ext}_r^n(M, C^1) = ... = \mathrm{Ext}_r^1(M, C^n)$$

From $0 \to N \to I^0 \to C^1 \to 0$ and $0 \to C^1 \to I^1 \to C^2$, we have

$$0 = \mathrm{Ext}_l^n(M, I^0) \longrightarrow \mathrm{Ext}_l^n(M, C^1) \longrightarrow \mathrm{Ext}_l^{n+1}(M, N) \longrightarrow \mathrm{Ext}_l^{n+1}(M, I^0) = 0$$

$$0 = \mathrm{Ext}_l^{n-1}(M, I^1) \longrightarrow \mathrm{Ext}_l^{n-1}(M, C^2) \longrightarrow \mathrm{Ext}_l^n(M, C^1) \longrightarrow \mathrm{Ext}_l^n(M, I^1) = 0$$

Hence, we have the same formula for Ext_l

$$\mathrm{Ext}_l^{n+1}(M, N) = \mathrm{Ext}_l^n(M, C^1) = ... = \mathrm{Ext}_l^1(M, C^n)$$

From the exact sequence $0 \to C^n \to I^n \to C^{n+1}$, we have

$$
\begin{tikzcd}
\mathrm{Hom}(M, I^n) \arrow[r] \arrow[d, "\sim"] & \mathrm{Hom}(M, C^{n+1}) \arrow[r] \arrow[d, "\sim"] & \mathrm{Ext}_r^1(M, C^n) \arrow[r] \arrow[d, dashed] & \mathrm{Ext}_r^1(M, I^n) = 0 \arrow[d, "\sim"] \\
\mathrm{Hom}(M, C^{n+1}) \arrow[r] & \mathrm{Hom}(M, C^{n+1}) \arrow[r] & \mathrm{Ext}_l^1(K_n, N) \arrow[r] & \mathrm{Ext}_l^1(P_n, N) = 0
\end{tikzcd}
$$

By five lemma, $\mathrm{Ext}_r^{n+1}(M, N) = \mathrm{Ext}_l^{n+1}(M, N)$. $\square$

[2] $I^{-1} = N$

Remark 15.4.2 (some notes on dimension shifting solution)
Given a short exact sequence $0 \to A \to B \to C \to 0$. In the above proof, we used the following results

1. Consider $\mathrm{Ext}^i_l(-,-)$ computed using projective resolution, we have
   (a) a variant of *dimension shifting* using in the proof
   (b) $\mathrm{Ext}^i_l(M, I) = 0$ for any injective module I
   (c) the two long exact sequences mentioned in class
$$0 \to \mathrm{Hom}(M, A) \to \mathrm{Hom}(M, B) \to \mathrm{Hom}(M, C) \to \mathrm{Ext}^1_l(M, A) \to \mathrm{Ext}^1_l(M, B) \to \mathrm{Ext}^1_l(M, C) \to ...$$
$$0 \to \mathrm{Hom}(C, N) \to \mathrm{Hom}(B, N) \to \mathrm{Hom}(A, N) \to \mathrm{Ext}^1_l(C, N) \to \mathrm{Ext}^1_l(B, N) \to \mathrm{Ext}^1_l(A, N) \to ...$$
2. Consider $R^iF = \mathrm{Ext}^i_r(M, -)$ computed using injective resolution as a right derived functor of the covariant functor $F = \mathrm{Hom}(M, -)$, we have
   (a) a mirror version of dimension shifting in 15.2.6 for Ext_r since if $0 \to N \to I^0 \to I^1 \to ...$ is an injective resolution for N then $0 \to C^n \to I^n \to I^{n+1} \to ...$ is an shifted injective resolution for C^n, hence
$$\mathrm{Ext}^{n+1}_r(M, N) = \mathrm{Ext}^n_r(M, C^1) = ... = \mathrm{Ext}^1_r(M, C^n)$$
   (b) $\mathrm{Ext}^i_r(M, I) = 0$ for any injective module I since $0 \to I \to I \to 0$ is an injective resolution for I
   (c) the long exact sequence for right derived functor
$$0 \to \mathrm{Hom}(M, A) \to \mathrm{Hom}(M, B) \to \mathrm{Hom}(M, C) \to \mathrm{Ext}^1_r(M, A) \to \mathrm{Ext}^1_r(M, B) \to \mathrm{Ext}^1_r(M, C) \to ...$$

An alternative solution. Since $\mathrm{Hom}(P, -)$ is exact for every projective module P and $\mathrm{Hom}(-, I)$ is exact for every injective module I, we have the double complex $\mathrm{Hom}(P_\bullet, I^\bullet)$ [3] where every column except $\mathrm{Hom}(M, I^\bullet)$ is exact and every row except $\mathrm{Hom}(P_\bullet, N)$ is exact. We can construct a map

$$\phi : \ker(\mathrm{Hom}(M, I^n) \to \mathrm{Hom}(M, I^{n+1})) \to \ker(\mathrm{Hom}(P_n, N) \to \mathrm{Hom}(P_{n+1}, N))$$

as follows: for $i + j = n$,

$$\mathrm{Hom}(M, I^n) \to \mathrm{Hom}(P_0, I^n) \to ...$$
$$... \to \mathrm{Hom}(P_i, I^j) \to \mathrm{Hom}(P_{i+1}, I^j) \to \mathrm{Hom}(P_{i+1}, I^{j-1}) \to ...$$
$$... \to \mathrm{Hom}(P_n, I^0) \to \mathrm{Hom}(P_n, N)$$

Informally, the path zig-zags on the **top right** squares of the diagonal $i + j = n$
In the first square, let $x \in \ker(\mathrm{Hom}(M, I^n) \to \mathrm{Hom}(M, I^{n+1}))$, then $bax = 0$, then $cdx = 0$, then $dx \in \ker(\mathrm{Hom}(P_0, I^n) \to \mathrm{Hom}(P_0, I^{n+1}))$, then there is a lift y of dx in $\mathrm{Hom}(P_0, I^{n-1})$

$$\begin{tikzcd}
\mathrm{Hom}(M, I^{n+1}) \arrow[r, "b"] & \mathrm{Hom}(P_0, I^{n+1}) \\
\mathrm{Hom}(M, I^n) \arrow[u, "a"] \arrow[r, "d"] & \mathrm{Hom}(P_0, I^n) \arrow[u, "c"] \\
& \mathrm{Hom}(P_0, I^{n-1}) \arrow[u, "e"]
\end{tikzcd}$$

[3] $P_{-1} = M, I^{-1} = N$

In any intermediate square ($i+j=n$) and the last square ($i=n, j=0$)

$$\begin{tikzcd}
\mathrm{Hom}(P_{i-1}, I^{j+1}) \arrow[r, "a"] & \mathrm{Hom}(P_i, I^{j+1}) \arrow[r, "b"] & \mathrm{Hom}(P_{i+1}, I^{j+1}) \\
& \mathrm{Hom}(P_i, I^j) \arrow[u, "c"] \arrow[r, "e"] & \mathrm{Hom}(P_{i+1}, I^j) \arrow[u, "d"'] \\
& & \mathrm{Hom}(P_{i+1}, I^{j-1}) \arrow[u, "f"']
\end{tikzcd}$$

Let $y \in \mathrm{Hom}(P_i, I^j)$ be a lift of $x \in \mathrm{Hom}(P_{i-1}, I^{j+1})$. Since $bax = 0$, then $bcy = 0$, then $dey = 0$, hence $ey \in \ker d$, so there exists a lift $z \in \mathrm{Hom}(P_{i+1}, I^{j-1})$ so that $fz = ey$

In the last square, let $y \in \mathrm{Hom}(P_n, N)$ be a lift of $x \in \mathrm{Hom}(P_{n-1}, I^0)$. Since $bax = 0$, then $bcy = 0$, then $dey = 0$. Since d is injective, $ey = 0$, hence $y \in \ker(\mathrm{Hom}(P_n, N) \to \mathrm{Hom}(P_{n+1}, N))$. The map ϕ is well-defined.

$$\begin{tikzcd}
\mathrm{Hom}(P_{n-1}, I^0) \arrow[r, "a"] & \mathrm{Hom}(P_n, I^0) \arrow[r, "b"] & \mathrm{Hom}(P_{n+1}, I^0) \\
& \mathrm{Hom}(P_n, N) \arrow[u, hook, "c"] \arrow[r, "e"] & \mathrm{Hom}(P_{n+1}, N) \arrow[u, hook, "d"'] \\
& 0 \arrow[u] & 0 \arrow[u]
\end{tikzcd}$$

Now we construct another map

$$\phi_0 : \mathrm{im}(\mathrm{Hom}(M, I^{n-1}) \to \mathrm{Hom}(M, I^n)) \to \mathrm{im}(\mathrm{Hom}(P_{n-1} \to N) \to \mathrm{Hom}(P_n \to N))$$

as follows: for $i+j=n$

$$\begin{aligned}
&\mathrm{Hom}(M, I^n) \to \mathrm{Hom}(P_0, I^n) \to ... \\
&... \to \mathrm{Hom}(P_i, I^j) \to \mathrm{Hom}(P_i, I^{j-1}) \to \mathrm{Hom}(P_{i+1}, I^{j-1}) \to ... \\
&... \to \mathrm{Hom}(P_n, I^0) \to \mathrm{Hom}(P_n, N)
\end{aligned}$$

Informally, the path zig-zags on the **top right** and **bottom left** squares of the diagonal $i+j=n$

In the first square, let $x \in \mathrm{im}(\mathrm{Hom}(M, I^{n-1}) \to \mathrm{Hom}(M, I^n))$, let $z \in \mathrm{Hom}(M, I^{n-1})$ so that $az = x$. Let $y = bz$

$$\begin{tikzcd}
& \mathrm{Hom}(P_0, I^{n+1}) \\
\mathrm{Hom}(M, I^n) \arrow[r, "d"] & \mathrm{Hom}(P_0, I^n) \arrow[u] \\
\mathrm{Hom}(M, I^{n-1}) \arrow[u, "a"] \arrow[r, "b"] & \mathrm{Hom}(P_0, I^{n-1}) \arrow[u, "e"]
\end{tikzcd}$$

In any intermediate square ($i+j=n$) and the last square ($i=n, j=0$)

$$\begin{tikzcd}
\mathrm{Hom}(P_{i-2}, I^{j+1}) \arrow[r, dashed] & \mathrm{Hom}(P_{i-1}, I^{j+1}) \arrow[r, "a"] & \mathrm{Hom}(P_i, I^{j+1}) \arrow[r, "b"] & \mathrm{Hom}(P_{i+1}, I^{j+1}) \\
& \mathrm{Hom}(P_{i-1}, I^j) \arrow[u, dashed] \arrow[r, dashed] & \mathrm{Hom}(P_i, I^j) \arrow[u, "c"] \arrow[r, "e"] & \mathrm{Hom}(P_{i+1}, I^j) \arrow[u, "d"'] \\
& & \mathrm{Hom}(P_i, I^{j-1}) \arrow[u, dashed] \arrow[r, dashed] & \mathrm{Hom}(P_{i+1}, I^{j-1}) \arrow[u, "f"']
\end{tikzcd}$$

Let $y \in \operatorname{Hom}(P_i, I^j)$ be a lift of $x \in \operatorname{Hom}(P_{i-1}, I^{j+1})$. Using exactly the same argument, we can construct $z \in \operatorname{Hom}(P_{i+1}, I^{j-1})$. However, this time, we also have $\tilde{x} \in \operatorname{Hom}(P_{i-2}, I^{j+1})$, $\tilde{y} \in \operatorname{Hom}(P_{i-1}, I^j)$ so that $\tilde{x}, \tilde{y}$ are mapped into x, y respectively, using the same argument, we can construct $\tilde{z} \in \operatorname{Hom}(P_i, I^{j-1})$ so that $\tilde{z}$ is mapped into z. Hence, the map ϕ_0 is well-defined.
Similarly, we can construct

$$\psi : \ker(\operatorname{Hom}(M, I^n) \to \operatorname{Hom}(M, I^{n+1})) \leftarrow \ker(\operatorname{Hom}(P_n, N) \to \operatorname{Hom}(P_{n+1}, N))$$

For any $x \in \ker(\operatorname{Hom}(M, I^n) \to \operatorname{Hom}(M, I^{n+1}))$, x and $\psi\phi x$ differ by an element in $\operatorname{im}(\operatorname{Hom}(M, I^{n-1}) \to \operatorname{Hom}(M, I^n))$. Hence, $\psi\phi$ and $\phi\psi$ are identity maps in the level of cohomology. Hence

$$H^n(\operatorname{Hom}(M, I^\bullet)) = H^n(\operatorname{Hom}(P_\bullet, N))$$

□

15.5 PROBLEM 7

Problem 15.5.1 (problem 7)
If M is flat A-module and N is an injective A-module, prove that $\operatorname{Hom}_A(M, N)$ is an injective A-module

Proof. Let

$$0 \to X \to Y$$

be exact. Since M is flat module, the covariant functor $(- \otimes M)$ is exact, so

$$0 \to X \otimes M \to Y \otimes M$$

is exact. Since N is injective module, the contravariant functor $\operatorname{Hom}(-, N)$ is exact, so

$$\operatorname{Hom}(Y \otimes M, N) \to \operatorname{Hom}(X \otimes M, N) \to 0$$

is exact. By tensor-hom adjunction

$$\operatorname{Hom}(Y, \operatorname{Hom}(M, N)) \to \operatorname{Hom}(X, \operatorname{Hom}(M, N)) \to 0$$

is exact. Hence, the contravariant function $\operatorname{Hom}(-, \operatorname{Hom}(M, N))$ is exact. So, $\operatorname{Hom}(M, N)$ is injective. □

15.6 PROBLEM 8

Lemma 15.6.1 (Baer's criterion)
An A-module M is injective if and only if every map $I \to M$ from an ideal I of A can be extended into a map $R \to M$. In particular, if A is a PID, M is injective if and only if it is divisible, that is, for every nonzero $a \in A$ and every $m \in M$, there exists $n \in M$ so that $an = m$

Proof.
(divisible $\implies$ injective) If M is divisible, for any ideal $(a) \in A$ and any map $\phi : (a) \to M$, let $m = \phi(a)$ and let $n \in M$

so that $an = m$. The extension is defined by

$$\begin{aligned} \tilde{\phi} : A &\to M \\ b &\mapsto bn \end{aligned}$$

(divisible $\impliedby$ injective) If M is injective, then for any $a \in A$, $m \in M$, define

$$\begin{aligned} \phi : (a) &\to M \\ a &\mapsto m \end{aligned}$$

Then, the extension gives $n = \tilde{\phi}(1) \in M$ so that $an = m$ ☐

Problem 15.6.2 (problem 8)
For a field k, consider the $k[x]$-module $M = k[x, x^{-1}]/xk[x]$. Prove that M is an injective $k[x]$-module

Proof. We have

$$M = \frac{k[x, x^{-1}]}{xk[x]} = \left\{ \sum_{i \in \mathbb{Z}} a_i x^i : a_i \in k \text{ and all } a_i \text{ but finitely many of nonpositive indices are zeros} \right\}$$

Any element of M can be written as

$$m(x) = a_0 + a_1 x^{-1} + ... + a_n x^{-n}$$

for some $a_0, ..., a_n \in k$ and $a_n \neq 0$. We will show that M is divisible. For any nonzero polynomial $f(x) \in k[x]$

$$f(x) = b_0 + b_1 x + ... + b_m x^m$$

for some $b_0, ..., b_m \in k$ and $b_m \neq 0$. If $b_0 = 0$, then $f(x) = x^r g(x)$ with $g(x)$ having nonzero constant term. Hence, finding $n(x) \in M$ so that $m(x) = f(x)n(x) = x^r g(x)n(x)$ is equivalent to finding $n(x)$ so that $g(x)n(x) = x^{-r}m(x)$. Hence, we can assume that $b_0 \neq 0$. Let

$$n(x) = c_0 + c_1 x^{-1} + ... \in M$$

for some $c_0, c_1, ... \in k$. We have the following system of equations

$$\begin{aligned} a_0 &= b_0 c_0 + b_1 c_1 + ... + b_m c_m \\ a_1 &= b_0 c_1 + b_1 c_2 + ... + b_m c_{m+1} \\ &... \\ a_n &= b_0 c_n + b_1 c_{n+1} + ... + b_m c_{m+n} \end{aligned}$$

Pick $c_{n+1}, ..., c_{m+n}$ arbitrarily. Using the last equation, we can solve uniquely for c_n. And from bottom to top we can solve for unique $c_{n-1}, ..., c_0$ iteratively. Hence, M is divisible, so injective.

☐

Chapter 16

HOMEWORK 5

Problem 16.0.1 (prime avoidance lemma)
Let A be a ring and let $I, J_1, J_2, ..., J_n \subseteq A$ be ideals such that at most two of $J_1, J_2, ..., J_n$ are not prime. If $I \nsubseteq J_i$ for all i, prove that $I \nsubseteq \bigcup_{1 \leq i \leq n} J_i$

Proof. We will prove by induction on n
base case: $n = 1$, clear
induction case: $n \geq 2$
Suppose that $I \subseteq \bigcup_{1 \leq i \leq n} J_i$. By induction hypothesis, for every i, we can pick an element x_i so that

$$x_i \in I \text{ and } x_i \notin \bigcup_{k \neq i} J_k$$

Assumption $I \subseteq \bigcup_{1 \leq i \leq n} J_i$ implies $x_i \in J_i$. Let

$$y = x_1 ... x_{n-1} + x_n \in I \subseteq \bigcup_{1 \leq i \leq n} J_i$$

subcase 1: $n = 2$, then $y = x_1 + x_2 \in J_1 \cup J_2$. Without loss of generality, let $y \in J_1$, then $x_2 = y - x_1 \in J_1$, this is a contradiction by construction of x_2.
subcase 2: $n \geq 3$. Without loss of generality, let J_n be prime. If $y \in J_n$, then $x_1 ... x_{n-1} = y - x_n \in J_n$, then at least one of $x_1, ..., x_{n-1}$ is an element of J_n which is a contradiction. If $y \in J_i$ for some $1 \leq i \leq n-1$, then $x_n = y - x_1 ... x_{n-1} \in J_i$ which is also a contradiction ☐

Problem 16.0.2
Problem consists of two parts

1. Let $A \hookrightarrow B$ be an integral ring extension of Noetherian rings. Prove that $\dim B = \dim A$

2. Let k be a field and let A be a finitely generated k-algebra. Recalled that we prove *Noetherian normalization* which say we can find an injective map $\phi : k[X_1, ..., X_n] \hookrightarrow A$ such that A is finitely generated as a $k[x_1, ..., x_n]$-module where $x_i = \phi(X_i)$. Prove that $\dim A = n$, so n is uniquely determined by A

Proof of part 1.
Since both A and B are Noetherian, any ascending chain of primes of strict inclusions must be finite

- $(\dim A \le \dim B)$

  For any finite chain of primes $\mathfrak{p}_0 \subsetneq ... \subsetneq \mathfrak{p}_n$ in A, by lying over theorem for integral ring extension, pick $\mathfrak{q}_0$ in B so that $\mathfrak{q}_0 \cap A = \mathfrak{p}_0$. Going-up theorem induces a chain of primes $\mathfrak{q}_0 \subseteq ... \subseteq \mathfrak{q}_n$ in B. Moreover, $\mathfrak{q}_i = \mathfrak{q}_{i+1}$ implies $\mathfrak{p}_i = \mathfrak{p}_{i+1}$. Hence, the chain of primes in B is also of strict inclusions. Hence, $\dim A \le \dim B$

- $(\dim B \le \dim A)$

  For any finite chain of primes $\mathfrak{q}_0 \subsetneq ... \subsetneq \mathfrak{q}_n$ in B, let $\mathfrak{p}_i = \mathfrak{q}_i \cap A$, then $\mathfrak{p}_0 \subseteq ... \subseteq \mathfrak{p}_n$ is a chain of primes in A. By AM Corollary 5.9, $\mathfrak{p}_i = \mathfrak{p}_{i+1}$ implies $\mathfrak{q}_i = \mathfrak{q}_{i+1}$. Hence the chain of primes in A is also of strict inclusions, so $\dim B \le \dim A$

□

Lemma 16.0.3

Given a ring extension $A \hookrightarrow B$, let $x \in B$, the following are equivalent:

1. x is integral over A
2. the ring $A[x] \subseteq B$ is finitely generated A-module
3. $A[x]$ is contained in a subring C of B such that C is also a finitely generated A-module
4. there exists a faithful $A[x]$-module M which is finitely generated as an A-module An R-module M is faithful if and only if $\operatorname{ann}_R(M) = \{r \in R : rM = 0\} = 0$ if and only if $R \to \operatorname{Hom}_R(M, M)$ is injective.

Proof of part 2. Since A is finitely generated as an $k[x_1, ..., x_n]$-module, for any $x \in A$, $k[x_1, ..., x_n][x] \subseteq A$ is also finitely generated as an $k[x_1, ..., x_n]$-module. By 2, x is integral over $k[x_1, ..., x_n]$. Therefore, $\phi : k[X_1, ..., X_n] \hookrightarrow A$ is an integral ring extension. By part 1, $\dim A = \dim k[X_1, ..., X_n] = n$ □

Problem 16.0.4

Let $\mathfrak{p}$ be a prime ideal in a Noetherian ring A. Prove that $\operatorname{ht}\mathfrak{p} + \dim A/\mathfrak{p} \le \dim A$

Proof. Since A is Noetherian, then $A/\mathfrak{p}$ is also Noetherian, let $\mathfrak{p}_0 \subsetneq ... \subsetneq \mathfrak{p}_n = \mathfrak{p}$ be a finite chain of primes in A and $\mathfrak{q}_0 \subsetneq ... \subsetneq \mathfrak{q}_m$ be a finite chain of primes in $A/\mathfrak{p}$. Let $\tilde{\mathfrak{q}}_i \subseteq A$ be a lift of $\mathfrak{q}_i$, then we have the chain of primes in A of length at least $n + m$

$$\mathfrak{p}_0 \subsetneq ... \subsetneq \mathfrak{p}_n = \mathfrak{p} \subseteq \tilde{\mathfrak{q}}_0 \subsetneq ... \subsetneq \tilde{\mathfrak{q}}_m$$

Then, $\operatorname{ht}\mathfrak{p} + \dim A/\mathfrak{p} \le \dim A$ □

Problem 16.0.5

Notation as in 3, find an example with $\dim A = 2$, $\operatorname{ht}\mathfrak{p} = 1$ and $\dim A/\mathfrak{p} = 0$. In particular, deduce that the inequality in 3 can be strict.

Proof. Consider the ideal $\mathfrak{a} = (zx, zy) = (z)(x, y)$ in $\mathbb{C}[x, y, z]$, let $A = \mathbb{C}[x, y, z]/\mathfrak{a}$. Note that (z) and (x, y) are the only minimal primes over $\mathfrak{a}$ in $\mathbb{C}[x, y, z]$, hence

$$\dim A = \max\left\{\dim \frac{\mathbb{C}[x, y, z]}{(z)}, \dim \frac{C[x, y, z]}{(x, y)}\right\} = 2$$

Let $\mathfrak{m} = (z-1, x, y) \supseteq \mathfrak{a}$ be a maximal prime in $\mathbb{C}[x, y, z]$ which is also maximal in A, then

$$A/\mathfrak{m} = \frac{\mathbb{C}[x, y, z]}{(xz, zy, z-1, x, y)} = \frac{\mathbb{C}[x, y, z]}{(z-1, x, y)} \cong \mathbb{C}$$

Hence, $\dim A/\mathfrak{m} = 0$. It remains to show that $\operatorname{ht}_A \mathfrak{m} = 1$. Since (z) and (x, y) are the only minimal primes over $\mathfrak{a}$ in $\mathbb{C}[x, y, z]$, every prime $\mathfrak{p}$ in A lifted to $\mathbb{C}[x, y, z]$ must either contain (z) or (x, y). If $\mathfrak{p} \subseteq \mathfrak{m}$ in A, because $(z) \nsubseteq \mathfrak{m}$, then $\mathfrak{p}$ must contain (x, y). Hence,

$$\operatorname{ht}_A \mathfrak{m} = \operatorname{ht}_{\mathbb{C}[x,y,z]/(x,y)} \mathfrak{m} = \operatorname{ht}_{\mathbb{C}[z]}(z-1) = 1$$

□

Problem 16.0.6

Problem consists of three parts

1. Let A be a Noetherian ring and let $x \in A$ be a non zero-divisor. Prove that $\dim A/(x) \leq \dim A - 1$
2. Prove that if moreover A is a local ring and x is not a unit, then equality holds in 1
3. Deduce that if A is any local Noetherian ring, then $\operatorname{depth}_A A \leq \dim A$

Lemma 16.0.7

If A is Noetherian and $\mathfrak{p} \subseteq A$ be a minimum prime, then any element of $\mathfrak{p}$ is a zero divisor.

Proof of part 1. (Assuming $0 < \dim A < +\infty$) Given any maximal chain of primes in $A/(x)$ of strict inclusions

$$\mathfrak{p}_0 \subsetneq \ldots \subsetneq \mathfrak{p}_n$$

the chain is lifted into a chain of primes in A of strict inclusions

$$\tilde{\mathfrak{p}}_0 \subsetneq \ldots \subsetneq \tilde{\mathfrak{p}}_n$$

Since $x \in \tilde{\mathfrak{p}}_0$ is a non zero-divisor, hence $\tilde{\mathfrak{p}}_0$ is not a minimal prime, we can extend the lifted chain in A by at least one. Hence

$$\dim A/(x) \leq \dim A - 1$$

□

Lemma 16.0.8

Let $(A, \mathfrak{m})$ be a Noetherian local ring and $x_1, \ldots, x_m$ be some elements in $\mathfrak{m}$ with $m \leq \dim A$, then the following are equivalent

1. $x_1, \ldots, x_m$ can be extended into a system of parameters
2. $\dim A/(x_1, \ldots, x_m) \leq \dim A - m$
3. $\dim A/(x_1, \ldots, x_m) = \dim A - m$

Proof of part 2. (Assuming $0 < \dim A < +\infty$) Since x is not a unit, $x \in \mathfrak{m}$. By part 1 and Lemma 16.0.8 ($2 \implies 3$), $\dim A/(x) = \dim A - 1$ □

Proof of part 3. We will prove by induction

base case: If $\dim A = 0$, since A is Noetherian local of dimension 0, A is Artinian local, so $\mathfrak{m}$ is nilpotent, that is, element every element of A must be either a unit or a zero-divisor. We need to show that $\operatorname{depth}_A A = 0$, that is there is no A-regular sequence in A. Suppose there is an A-regular sequence $x_1, ..., x_r$, then x_1 cannot be unit since $A/(x_1, ..., x_r)A \neq 0$. Moreover, x_1 cannot be zero divisor since $x_1 : A \to A$ is injective. So, no A-regular sequence exists in A, hence $\operatorname{depth}_A A = 0$

induction case: when $\dim A = n > 0$, if $\operatorname{depth}_A A = 0$, we are done. If $\operatorname{depth}_A A = r > 0$, pick a maximal A-regular sequence $a, a_2, ..., a_r \in A$ of length r. Note that,

$$\frac{A/(a)}{(a_2, ..., a_i)A/(a)} = \frac{A}{(a, a_2, ..., a_i)} \neq 0$$

and each $a_i : A/(a, ..., a_i) \to A/(a, ..., a_i)$ injective imply $\bar{a}_2, ..., \bar{a}_r \in A/(a)$ is a $A/(a)$-regular sequence of length $r-1$, then

$$\operatorname{depth}_A A - 1 \leq \operatorname{depth}_{A/(a)} A/(a)$$

Since a is not a zero divisor, $\dim A/(a) \leq \dim A - 1 = n - 1$, by induction hypothesis for $A/(a)$

$$\operatorname{depth}_{A/(a)} A/(a) \leq \dim A/(a) \leq \dim A - 1$$

Hence,

$$\operatorname{depth}_A A \leq \dim A$$

□

Problem 16.0.9

Let $(A, \mathfrak{m}, k)$ be a Noetherian local ring. In class we define $\operatorname{embdim} A = \dim_k \mathfrak{m}/\mathfrak{m}^2$ and proved that $\dim A \leq \operatorname{embdim} A$. Prove that *every* pair of nonnegative integers (r, s) with $r \leq s$ occurs at $(\dim A, \operatorname{embdim} A)$ for some A

Proof. We construct ring $A = \mathbb{C}[x_1, ..., x_s]_{(x_1, ..., x_s)}$ with $(\dim A, \operatorname{embdim} A) = (s, s)$ and ring $B = \frac{A}{(x_1^2, ..., x_{s-r}^2)}$ with $(\dim B, \operatorname{embdim} B) = (r, s)$ for every pair $r \leq s$

1. (s, s)

   Consider $\mathbb{C}[x_1, ..., x_s]$ of dimension s, $\mathfrak{m} = (x_1, ..., x_s)$ is a maximal ideal of maximal height. Localizing at $\mathfrak{m}$ gives $A = \mathbb{C}[x_1, ..., x_s]_{\mathfrak{m}}$ and A is also of dimension s. Since $\mathfrak{m}$ is generated by s elements, then $\dim A \leq \operatorname{embdim} A \leq s = \dim A$. So, $\operatorname{embdim} A = \dim A = s$

2. (r, s) for $r \leq s$

   Consider

   $$I_i = (x_1^2, ..., x_i^2)$$

   Note that, x_i^2 is not a zero divisor in $A/I_{i-1} = (\mathbb{C}[x_1, ..., x_s]/I_{i-1})_{\mathfrak{m}}$ because if a nonzero element $\bar{f}(x)/\bar{g}(x) \in (\mathbb{C}[x_1, ..., x_s]/I_{i-1})_{\mathfrak{m}}$ for some $f(x) \in \mathbb{C}[x_1, ..., x_s], g(x) \in \mathbb{C}[x_1, ..., x_s] - \mathfrak{m}$ satisfies

   $$x_i^2 \frac{f(x)}{g(x)} = 0 \in A/I_{i-1}$$

   Then, $x_i^2 f(x)h(x) \in I_{i-1}$ for some $h(x) \in \mathbb{C}[x_1, ..., x_s] - \mathfrak{m}$. But $\bar{f}(x)/\bar{g}(x)$ being nonzero implies $f(x)h(x) \notin I_{i-1}$, this is a contradiction.

Moreover, x_i^2 is not a unit in $A/I_{i-1} = (\mathbb{C}[x_1, ..., x_s]/I_{i-1})_{\mathfrak{m}}$ because if a nonzero element $\bar{f}(x)/\bar{g}(x) \in (\mathbb{C}[x_1, ..., x_s]/I_{i-1})_{\mathfrak{m}}$ for some $f(x) \in \mathbb{C}[x_1, ..., x_s], g(x) \in \mathbb{C}[x_1, ..., x_s] - \mathfrak{m}$ satisfies

$$x_i^2 \frac{f(x)}{g(x)} = 1 \in A/I_{i-1}$$

Then, $x_i^2 f(x)h(x) - g(x)h(x) \in I_{i-1}$ some $h(x) \in \mathbb{C}[x_1, ..., x_s] - \mathfrak{m} = \mathbb{C}$, this is a contradiction.

Now, for each i, from Problem 16.0.6, x_i^2 is not a zero divisor and not a unit in $\dim A/I_{i-1}$, then

$$\dim A/I_i = \dim A/I_{i-1} - 1$$

Let $B = A/I_{s-r}$, then

$$\dim B = \dim A/I_{s-r} = \dim A - s + r = r$$

We want to show that $\operatorname{embdim} B = \operatorname{embdim} A = s$, let $\mathfrak{m}_B$ denote the projection of $\mathfrak{m}$ under the map $A \twoheadrightarrow B$ and $k_B = B/\mathfrak{m}_B$. Note that, $I_{s-r} \subseteq \mathfrak{m}^2 \subseteq \mathfrak{m}$, then $\mathfrak{m}_B/\mathfrak{m}_B^2 = \mathfrak{m}/\mathfrak{m}^2$ and $k_B = B/\mathfrak{m}_B = A/\mathfrak{m} = k$ (third isomorphism theorem). So

$$\operatorname{embdim} B = \dim_{k_B} \mathfrak{m}_B/\mathfrak{m}_B^2 = \dim_k \mathfrak{m}/\mathfrak{m}^2 = \operatorname{embdim} A = s$$

□

Problem 16.0.10

Let A be a Noetherian ring. Prove that $\dim A[[x]] = \dim A + 1$

Proof. $x \in A[[x]]$ is not a zero-divisor and not a unit in the Noetherian ring $A[[x]]$, then $A \cong \frac{A[[x]]}{(x)}$ implies

$$\dim A = \dim \frac{A[[x]]}{(x)} = \dim A[[x]] - 1$$

□

Problem 16.0.11

Let k be a field and A, B be finitely generated k-algebras, so then $A \otimes_k B$ is also a finitely generated k-algebra. Prove that $\dim A \otimes_k B = \dim A + \dim B$

Lemma 16.0.12 (Noether normalization theorem)

Let k be a field and A be a finite-type k-algebra, then there exists $x_1, ..., x_n \in A$ so that

$$\begin{aligned} \phi : k[X_1, ..., X_n] &\hookrightarrow A \\ X_i &\mapsto x_i \end{aligned}$$

and A is finitely generated as a module over the image or equivalently A is integral over $k[x_1, ..., x_n]$. Moreover, $x_1, ..., x_n$ are algebraically independent over k, that is, x_i does not satisfy any nontrivial polynomial equation with coefficients in k

Lemma 16.0.13

Given an A-module M, M is flat if and only if $I \otimes M \to A \otimes M \xrightarrow{\sim} M$ induced from $I \hookrightarrow A$ is injective. In particular, if $A = k$ is a field, then every k-module is flat.

Proof. By Noether normalization theorem, and Problem 16.0.2, we have $\dim A = n, \dim B = m$ and injective maps

$$\phi_A : k[X_1, ..., X_n] \hookrightarrow A$$
$$\phi_B : k[Y_1, ..., Y_m] \hookrightarrow B$$

Every k-module is flat, $k[Y_1, ..., Y_m]$ is flat,

$$k[X_1, ..., X_n, Y_1, ..., Y_m] = k[X_1, ..., X_n] \otimes k[Y_1, ..., Y_m] \hookrightarrow A \otimes k[Y_1, ..., Y_m]$$

is injective. Every k-module is flat, A is flat

$$A \otimes k[Y_1, ..., Y_m] \hookrightarrow A \otimes B$$

is injective. Hence, the composition is injective

$$\phi : k[X_1, ..., X_n, Y_1, ..., Y_m] \hookrightarrow A \otimes B$$

Since each A and B is finitely generated as a module over $\phi(k[X_1, ..., X_n])$ and $\phi(k[Y_1, ..., Y_m])$ respectively. Hence, $A \otimes B$ is finitely generated over $\phi(k[X_1, ..., X_n, Y_1, ..., Y_m])$. By Problem 16.0.2, $\dim A \otimes B = n + m$ ☐

Problem 16.0.14

Let $(A, \mathfrak{m})$ be a Noetherian local ring, let $\hat{A}$ be the $\mathfrak{m}$-adic completion of A. Prove that $\dim A = \dim \hat{A}$

Lemma 16.0.15 (Matsumura CRT p63 - some results for local Noetherian ring)

Let $(A, \mathfrak{m})$ be a local Noetherian ring, then

1. $\bigcap_{n \geq 1} \mathfrak{m}^n = \ker(\psi : A \to \hat{A}) = 0$
2. For M a finitely generated A-module and $N \subseteq M$ a submodule
$$\bigcap_{n \geq 1} (N + \mathfrak{m}^n M) = N$$
3. The completion $\hat{A}$ of A is faithfully flat over A; hence $A \subseteq \hat{A}$ and $I\hat{A} \cap A = I$ for any ideal I of A
4. $\hat{A}$ is again a Noetherian local ring, with maximal ideal $\mathfrak{m}A$ and it has the same residue class field as A; moreover, $\hat{A}/\mathfrak{m}^n\hat{A} = A/\mathfrak{m}^n$ for all $n \geq 1$
5. If A is a complete local ring, the for any ideal $I \neq A$, A/I is afgain a complete local ring.

Lemma 16.0.16 (result from lecture April 4)
A local homomorphism of Notherian rings $(A, \mathfrak{m})$ and $(B, \mathfrak{n})$ is a ring map $\phi : A \to B$ so that $\mathfrak{m} = \mathfrak{n} \cap A$, then

$$\dim B \leq \dim A + \dim B/\mathfrak{p}B$$

if the map is flat, then the equality holds.

Proof. By Lemma 16.0.15, $A \to \hat{A}$ is a flat ring extension of Noetherian local rings. By Lemma 16.0.16 and $\mathfrak{m}\hat{A}$ is maximal in $\hat{A}$

$$\dim \hat{A} = \dim A + \dim \hat{A}/\mathfrak{m}\hat{A} = \dim A$$

□