MA5204 Commutative and Homological Algebra

Thang Pang Ern

Contents

1 Ring Theory and Module Theory **2**
1.1 Ring Theory . . . 2
1.2 Module Theory . . . 14

2 Basic Commutative Algebra **16**
2.1 Exact Sequences of Modules . . . 16
2.2 Localization . . . 21
2.3 Tensor Products . . . 26

3 Some Classes of Rings **36**
3.1 Noetherian Rings . . . 36
3.2 Dimension Theory . . . 39
3.3 Integral Dependence and Integral Rings . . . 40
3.4 Completions . . . 47
3.5 Artinian Rings . . . 51
3.6 Euclidean Domains, Principal Ideal Domains and Unique Factorisation Domains . . . 55
3.7 Primary Decomposition . . . 56
3.8 Discrete Valuation Rings . . . 57
3.9 Dedekind Domains . . . 59
3.10 Fractional Ideals . . . 59
3.11 Projective Modules . . . 62
3.12 Links with Algebraic Geometry . . . 64

4 Introduction to Homology **67**
4.1 Chain Complexes . . . 67

References

1 Atiyah, M., Macdonald, I. (1994). *Introduction to Commutative Algebra*. CRC Press.
2 Matsumura, H. (1986). *Commutative Ring Theory*. Cambridge University Press.
3 Eisenbud, D. (1995). *Commutative Algebra*. Springer, Berlin.

Chapter 1
Ring Theory and Module Theory

1.1
Ring Theory

Definition 1.1 (ring). A ring R is a set with distinct elements $1,0 \in R$ equipped with two binary maps which are multiplication and addition respectively.

$$R \times R \to R \text{ where } (r,r') \mapsto rr' \quad \text{and} \quad R \times R \times R \text{ where } (r,r') \mapsto r+r'.$$

The following conditions are satisfied:

(i) $(R,+,0)$ is an Abelian group, i.e. for all $r,r' \in R$,

$$r+r' = r'+r \quad \text{and} \quad 0+r = r = r+0$$

(ii) Distributivity and associativity holds, i.e. for all $r,s,s_1,s_2,t \in R$,

$$r(s_1+s_2) = rs_1+rs_2 \quad \text{and} \quad r(st) = (rs)t$$

(iii) Existence of multiplicative identity, i.e. $1r = r1 = r$ for all $r \in R$

We say that R is an associative ring with unity.

Definition 1.2 (commutative ring). If we further assume that $rs = sr$ for all $r,s \in R$ in Definition 1.1, we obtain a commutative ring with unity.

Remark 1.1. In this course, we take rings to be *commutative rings with unity*.

Definition 1.3 (unit). Let $x \in R$. If

$$\text{there exists } y \in R \text{ such that } xy = 1 \quad \text{then} \quad x \text{ is a unit.}$$

Here, $y = 1/x$.

Proposition 1.1. The set of units of R, denoted by $R^\times$, forms an Abelian group under $\times$.

Definition 1.4 (field). A ring R is a field if $R^\times = R \setminus \{0\}$.

Definition 1.5 (ring homomorphism). A ring homomorphism $\varphi : R \to S$ is a map of sets such that

(i) $\varphi(0_R) = 0_S$

(ii) $\varphi(1_R) = 1_S$

(iii) $\varphi(r+r') = \varphi(r) + \varphi(r')$

(iv) $\varphi(rr') = \varphi(r)\varphi(r')$

Definition 1.6 (ideal). Let R be a ring. An ideal of R is a subset $I \subseteq R$ such that

(i) $I \leq (R, 0, +)$, i.e.

$$0 \in I \quad \text{and} \quad \text{for all } i_1, i_2 \in I \text{ we have } i_1 + i_2 \in I$$

(ii) For all $r \in R$ and $i \in I$, we have $ri \in I$

Example 1.1 (integer multiples). For any fixed integer $n \in \mathbb{Z}$,

$$n\mathbb{Z} = \{\text{all multiples of n}\} \subseteq \mathbb{Z} \quad \text{is an ideal.}$$

Example 1.2. More generally, given any $x \in R$, the subset

$$(x) = \{\text{all elements in } R \text{ of the form } xr : r \in R\} \subseteq R \quad \text{is an ideal.}$$

Proposition 1.2. If $I \subseteq R$ is an ideal, then the set

$$R/I = \text{quotient of } R \text{ by I as Abelian groups} = \text{the set of cosets } r + I \subseteq R$$

naturally has a ring structure.

Proof. Let $r_1, r_2 \in R$. We have

$$(r_1 + I) + (r_2 + I) = r_1 + r_2 + I \quad \text{and} \quad (r_1 + I)(r_2 + I) = r_1 r_2 + I.$$

Also, $1 = 1_R + I$ and $0 = 0_R + I$. Note that by construction, there exists a natural surjective ring homomorphism $R \to R/I$, i.e. any surjective ring homomorphism $f : R \to S$ arises from such a construction if we set $I = f^{-1}(0)$, so $S \cong R/I$. □

Example 1.3. Let $R = \mathbb{Z}$ and $I = (n)$. Then,

$$R/I = \mathbb{Z}/(n) = \{0, 1, \ldots, n-1\} \quad \text{which is precisely the integers modulo } n.$$

A simple fact from MA1100 states that that $\mathbb{Z}/(n)$ is a field if and only if n is some prime p.

Definition 1.7 (integral domain). A ring R is a integral domain if

$$\text{for all } x, y \in R, \text{ we have } xy = 0 \quad \text{implies} \quad x = 0 \text{ or } y = 0.$$

Definition 1.8 (prime ideal). Let A be a ring. An ideal $I \subseteq A$ is prime if

$$\text{for all } x, y \in A, \text{ we have } xy \in I \quad \text{implies} \quad x \in I \text{ or } y \in I.$$

Proposition 1.3. Let A be a ring. Given any $I \subseteq A$,

$$A/I \text{ is an integral domain} \quad \text{if and only if} \quad I \text{ is a prime ideal.}$$

Proof. We only prove the reverse direction. The proof of the forward direction is similar. Anyway, given $x, y \in A$ for some ring A, suppose I is a prime ideal. Say $\bar{x} \cdot \bar{y} = 0$. This holds if and only if $xy \in I$. Equivalently, $x \in I$ or $y \in I$, i.e. $\bar{x} = 0$ or $\bar{y} = 0$. As such, A/I is an integral domain. □

Definition 1.9 (maximal ideal). An ideal $I \subset A$ (proper subset inclusion) is maximal if

$$\text{there does not exist} \quad \text{any ideals } I \subset J \subset A.$$

Proposition 1.4. Let A be a ring. Then,

$$\text{an ideal } I \subset A \text{ is maximal} \quad \text{if and only if} \quad A/I \text{ is a field.}$$

Proof. Note that given any ring homomorphism $\varphi : A \twoheadrightarrow A/I$ in A, there is a natural inclusion-preserving bijection between

$$\{\text{ideals } I \subseteq J \subseteq A\} \quad \text{and} \quad \left\{\text{ideals } \overline{J} \subseteq A/I\right\}.$$

The map is given by $J \mapsto J/I = \overline{J}$ such that $\overline{J} \mapsto \varphi^{-1}\left(\overline{J}\right)$ since φ is bijective, hence invertible.

Now, consider the following chain of implications:

$$\begin{aligned} J \subset A \text{ is maximal} \quad &\text{if and only if} \quad \text{the only ideals of } A/I \text{ are } A/I \text{ and } (0) \\ &\text{if and only if} \quad \text{any } 0 \neq x \in A/I \text{ satisfies } (x) = A/I \\ &\text{if and only if} \quad \text{any } 0 \neq x \in A/I \text{ is a unit} \\ &\text{if and only if} \quad A/I \text{ is a field} \end{aligned}$$

The result follows. □

Proposition 1.5. Any non-zero ring A has a maximal ideal.

Proof. Recall Zorn's lemma which states that if $S \neq \emptyset$ is a partially ordered set such that any chain in S admits an upper bound, then S has a maximal element. Recall that a chain C is a subset of S such that

$$\text{for all } x, y \in S \quad \text{we have} \quad x \leq y \text{ or } y \leq x.$$

Now, fix a non-zero ring A. Let S denote the set of proper ideals $I \subset A$ with the inclusion being the partial order relation. Note that $S \neq \emptyset$ since $(0) \in S$. Next, if $C \subseteq S$ is a chain, then

$$\bigcup_{s \in C} I_s \quad \text{is a proper ideal.}$$

Thus, the aforementioned union is contained in S and is an upper bound for the chain C.

As such, Zorn's lemma aplies so S has a maximal element if and only if A has a maximal ideal. □

Corollary 1.1. For any ring A,

$$\text{any proper ideal } I \subset A \quad \text{is} \quad \text{contained in some maximal ideal.}$$

Proof. Suppose I is a proper ideal of A. Then, $A/I \neq 0$, which implies that there exists a maximal ideal $\mathfrak{m}$ properly contained in A/I. So, the preimage of $\mathfrak{m}$ in A is maximal and contains I. □

Definition 1.10 (nilpotent element). Let A be a ring. An element $x \in A$ is nilpotent if

$$\text{there exists } n \in \mathbb{N} \quad \text{such that} \quad x^n = 0.$$

Example 1.4. 0 is always nilpotent.

Example 1.5. $2 \in \mathbb{Z}/(4)$ is non-zero and nilpotent.

Example 1.6 (Atiyah and Macdonald p. 10 Question 2). Let A be a ring and let $A[x]$ be the ring of polynomials in an indeterminate x, with coefficients in A. Let

$$f = a_0 + a_1 x + \ldots + a_n x^n \in A[x].$$

Prove that:

(i) f is a unit in $A[x]$ if and only if a_0 is a unit in A and $a_1, \ldots, a_n$ are nilpotent
Hint: If $b_0 + b_1 x + \cdots + b_m x^m$ is the inverse of f, prove by induction on r that $a_n^{r+1} b_{m-r} = 0$. Hence show that a_n is nilpotent, and then use the following fact: if x a nilpotent element of a ring A, then $1 + x$ is a unit of A, for which it follows that the sum of a nilpotent element and a unit is a unit.

(ii) f is nilpotent if and only if $a_0, a_1, \ldots, a_n$ are nilpotent

(iii) f is a zero-divisor if and only if there exists $a \neq 0$ in A such that $af = 0$
Hint: Choose a polynomial $g = b_0 + b_1 x + \cdots + b_m x^m$ of least degree m such that $fg = 0$. Then $a_n b_m = 0$, hence $a_n g = 0$ (because a_n annihilates f and has degree $< m$). Now show by induction that $a_n^r g = 0$ $(0 \leq r \leq n)$.

(iv) f is said to be primitive if $(a_0, a_1, \ldots, a_n) = (1)$. Prove that if $f, g \in A[x]$, then

$$fg \text{ is primitive} \quad \text{if and only if} \quad f \text{ and } g \text{ are primitive.}$$

Solution.

(i) We only prove the forward direction. The proof of the reverse direction follows from the hint (which is actually Question 1 of the same exercise set) and **(ii)** of this exercise. Suppose f is a unit in $A[x]$. Let $g = b_0 + b_1 x + \ldots + b_m x^m$ be the inverse of f. Then,

$$fg = (a_0 + a_1 x + \ldots + a_n x^n)(b_0 + b_1 x + \ldots + b_m x^m)$$

Since the constant term must be 1, then $a_0 b_0 = 1$, so a_0 is a unit in A. Recall the convolution formula that

$$fg = c_0 + c_1 x + \ldots + c_k x^k,$$

where $c_0 = a_0 b_0$ (discussed earlier),

$$c_1 = a_0 b_1 + a_1 b_0 = 0$$
$$c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0 = 0$$

and so on. One can deduce that $a_1, \ldots, a_n$ are nilpotent.

(ii) For the forward direction, suppose f is nilpotent. Then, one can apply induction to n to show that all of its coefficients are nilpotent. To demonstrate this, note that the $n = 1$ case is trivial. For the general case, the leading coefficient will be a_n^k for some $k \in \mathbb{N}$, so a_n is nilpotent. By the inductive hypothesis, $a_0, \ldots, a_{n-1}$ are nilpotent as well.

For the reverse direction, if $a_0, \ldots, a_n$ are nilpotent, define $d \in \mathbb{N}$ such that

$$a_i^d = 0 \quad \text{for all } 0 \leq i \leq n.$$

In other words, d is the sum of the orders of all the orders of the coefficients. As such, $f^d = 0$.

(iii) For the forward direction, suppose f is a zero divisor. Then, let g be a polynomial of minimal order such that $fg = 0$. Suppose $g = b_0 + b_1 x + \ldots + b_m x^m$ such that $\deg g > 0$. Then, $a_n b_m = 0$, i.e. $a_n g$ annihilates f but $\deg(a_n g) < m$, which is a contradiction. As such,

$$\deg g = 0 \quad \text{or in other words} \quad \text{there exists } a \in A \text{ such that } af = 0.$$

The reverse direction follows by the definition of a zero-divisor (recall MA3201).

(iv) The reverse direction is essentially Gauss' lemma (MA3201); for the forward direction, if fg is primitive, then $(c_0, \ldots, c_{n+m}) = (1)$, where the c_i's are the coefficients of fg. This means that $\gcd(c_0, \ldots, c_{n+m}) = 1$, or equivalently, there does not exist $d > 1$ which divides all the c_i's.

Suppose on the contrary that neither f nor g is primitive. Then, say $\gcd(a_0, \ldots, a_n) > 1$. Then, because of the convolution formula

$$c_k = \sum_{i+j=k} a_i b_j \quad \text{(look at the dependence between } a_i \text{ and } c_k\text{)},$$

it forces the existence of some $d > 1$ which divides all the c_i's, leading to a contradiction! □

Proposition 1.6 (nildradical). The set of nilpotent elements in any ring A is an ideal. We call this the

$$\text{nilradical of } A \quad \text{which is denoted by } \mathfrak{N}_A.$$

Proof. Suppose $x \in A$ is nilpotent, i.e.

$$\text{there exists } n \in \mathbb{N} \quad \text{such that} \quad x^n = 0.$$

Then, for any $r \in A$, we have

$$(rx)^n = r^n x^n = r^n \cdot 0 = 0.$$

For compatibility regarding addition, suppose $x, y \in A$ are nilpotent. Then,

$$\text{there exist } n, m \in \mathbb{N} \quad \text{such that} \quad x^n = 0 \text{ and } y^m = 0.$$

We use the binomial theorem to obtain

$$(x+y)^{n+m} = x^{n+m} + \binom{n+m}{1} x^{n+m-1} y + \ldots + \binom{n+m}{m} x^n y^m + \ldots + \binom{n+m}{n+m-1} x y^{n+m-1} + y^m$$

which is 0 (*not surprising anyway*). □

Definition 1.11 (reduced ring). A ring A is reduced if it contains no non-zero nilpotent elements.

Example 1.7. A nice observation: for $n \neq 0$,

$$\mathbb{Z}/(n) \text{ is reduced} \quad \text{if and only if} \quad n \text{ is squarefree.}$$

Proposition 1.7. For any non-zero A, we have

$$\mathfrak{N}_A = \bigcap_{\mathfrak{p} \subset A} \mathfrak{p},$$

where $\mathfrak{p}$ denotes a prime ideal of A.

Proof. We first prove the forward inclusion. Suppose $x \in A$ is nilpotent. Then, $\overline{x} \in A/\mathfrak{p}$ is nilpotent, so $\overline{x} = 0$ in $A/\mathfrak{p}$ since $A/\mathfrak{p}$ is an integral domain. As such, $x \in \mathfrak{p}$ for all $\mathfrak{p} \subset A$.

For the reverse direction, fix $x \notin \mathfrak{N}_A$. We wish to find a prime ideal $\mathfrak{p}$ such that $x \notin \mathfrak{p}$. Let

$$\Sigma = \{I \subset A : x^n \notin I \quad \text{for all } n \in \mathbb{N}\}.$$

Then, $\Sigma \neq \emptyset$ as $(0) \in \Sigma$ by assumption on x. By applying the same argument as before, any chain in Σ has an upper bound. By Zorn's lemma, Σ has a maximal element $\mathfrak{p}$. It suffices to show that $\mathfrak{p}$ is a prime ideal. Suppose $y, z \in A \backslash \mathfrak{p}$. We wish to show that $yz \notin \mathfrak{p}$. Note that

$$\mathfrak{p} \subset (\mathfrak{p}, y) \quad \text{and} \quad \mathfrak{p} \subset (\mathfrak{p}, z).$$

These imply the following respectively: there exist $n, m \in \mathbb{N}$ such that $x^n \in (\mathfrak{p}, y)$ and $x^m \in (\mathfrak{p}, z)$. So,

$$x^n = p_1 + yr_1 \quad \text{and} \quad x^m = p_2 + zr_2 \quad \text{for } p_1, p_2 \in \mathfrak{p} \text{ and } r_1, r_2 \in A.$$

Multiplying both elements, we obtain

$$\mathfrak{p} \not\ni x^{n+m} = p_1 p_2 + p_1 z r_2 + p_2 y r_1 + yz r_1 r_2 \in yz r_1 r_2 + \mathfrak{p}.$$

Hence, $yzr_1r_2 \notin \mathfrak{p}$ and the result follows. □

Example 1.8 (Atiyah and Macdonald p. 11 Question 8). Let A be a ring $\neq 0$. Show that the set of prime ideals of A has a minimal element with respect to inclusion.

Solution. Note that every descending chain of prime ideals $\mathfrak{p}$ has a lower bound, which is their intersection. By Zorn's lemma, the set of prime ideals of A has at least one minimal element. □

Remark 1.2. Similar to Example 1.13, the set of prime ideals of A in Example 1.8 is actually called the prime spectrum of A or $\operatorname{Spec}(A)$.

Given two ideals $I, J \subseteq R$, we can construct some *new* ideals (Proposition 1.8).

Proposition 1.8 (constructing new ideals). Fix a ring R. Suppose we are given ideals $I, J \subseteq R$. Then, the following are also ideals of R:

(i) $I \cap J$

(ii) $I + J = \{i + j : i \in I, j \in J\}$

(iii) $IJ = \{i_1 j_1 + \ldots + i_k j_k : i_m \in I, j_n \in J\}$

We have obvious generalisations to ideals $I_1, \ldots, I_n \subseteq R$.

Proposition 1.9. If $x_1,\ldots,x_n \in R$ are given, we call

$$(x_1,\ldots,x_n) = (x_1)+\ldots+(x_n) \quad \text{the ideal generated by } x_1,\ldots,x_n.$$

Example 1.9. Let $R=\mathbb{Z}$, i.e. the ring of integers and consider the ideals $I=(n)$ and $J=(m)$. Then,

$$\begin{aligned} IJ &= (nm) \\ I+J &= (\gcd(m,n)) \\ I\cap J &= (\operatorname{lcm}(m,n)) \end{aligned}$$

Proposition 1.10. Fix a ring R. Suppose we have ideals $I,J\subseteq R$. Then, the following hold:

(i) $IJ\subseteq I\cap J\subseteq I+J$

(ii) In general, we have $(I+J)(I\cap J)\subseteq IJ$. In fact, if I and J are coprime (that is $I+J=R$), then $IJ=I\cap J$.

Proposition 1.11. Let R be a ring. Suppose we have ideals $I,J\subseteq R$. Consider the ring multiplication

$$\varphi : R\to R/I\times R/J.$$

Then, the following hold:

(i) $\ker\varphi = I\cap J$

(ii) If $I+J=R$, i.e. I and J are coprime, then φ is surjective

(iii) If I and J are coprime, then we have the isomorphism

$$R/IJ \cong R/(I\cap J) \cong R/I\times R/J$$

In fact, the Chinese remainder theorem states that $R/IJ\cong R/I\times R/J$.

Proof. We will only prove **(ii)** and **(iii)** as the proof of **(i)** is obvious. For **(ii)**, choose $\overline{x}\in R/I$ and $\overline{y}\in R/J$. Since $I+J=R$, then we can write

$$1 = i+j \quad \text{for some } i\in I, j\in J.$$

Note that

$$\varphi(i)=(0,1) \quad \text{and} \quad \varphi(j)=(1,0).$$

Since φ is a ring homomorphism, then

$$\varphi(jx+iy)=(\overline{x},\overline{y}) \quad \text{which shows that } \varphi \text{ is surjective.}$$

Moreover, $\ker\varphi = I\cap J = IJ$. Thus, the isomorphism in **(iii)** holds. □

Proposition 1.12 (extension and contraction)**.** Suppose $\varphi : R\to S$ is a ring homomorphism. We have

$$J\subseteq S \text{ is an ideal} \quad \text{implies} \quad \varphi^{-1}(J)\subseteq R \text{ is an ideal.}$$

This is often called the contraction of I. However, if $I \subseteq R$ is an ideal, then $\varphi(I) \subseteq S$ need not be an ideal. So, we can consider $\varphi(I)S$ to be the ideal generated by $\varphi(I)$ (called the extension of I along φ), where

$$\varphi(I)S = \{s_1\varphi(i_1) + \ldots + s_k\varphi(i_k) : s_m \in S, i_m \in I\}$$

Example 1.10. Given the inclusion map $\varphi : \mathbb{Z} \hookrightarrow$, the zero ideal is maximal in , but its pre-image is not maximal in $\mathbb{Z}$. Thus the pre-image of a maximal ideal is not necessarily maximal.

Proposition 1.13. Let $\varphi : R \to S$ be a ring homomorphism. Then,

$$\mathfrak{p} \subseteq S \text{ is a prime ideal} \quad \text{implies} \quad \varphi^{-1}(\mathfrak{p}) \subseteq R \text{ is also a prime ideal.}$$

Proof. The following diagram commutes:

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & S \\ \downarrow & & \downarrow \\ R/\varphi^{-1}(\mathfrak{p}) & \longrightarrow & S/\mathfrak{p} \end{array}$$

and the lower horizontal arrow is injective. That is, we have $R/\varphi^{-1}(\mathfrak{p}) \hookrightarrow S/\mathfrak{p}$. Then, $\mathfrak{p}$ is prime if and only if $S/\mathfrak{p}$ is an integral domain, and equivalently, $R/\varphi^{-1}(\mathfrak{p}) \subseteq S/\mathfrak{p}$ is an integral domain. We conclude that $\varphi^{-1}(\mathfrak{p})$ is a prime ideal. □

Definition 1.12 (prime spectrum). For any ring R, let $\operatorname{Spec} R$ denote the set of all prime ideals of R. That is,

$$\operatorname{Spec} R = \{\mathfrak{p} \subseteq R : \mathfrak{p} \text{ is prime}\}.$$

Proposition 1.13 implies that for any ring homomorphism $\varphi : R \to S$, there exists an induced homomorphism $\varphi^* : \operatorname{Spec} S \to \operatorname{Spec} R$, where $\varphi^*(\mathfrak{p}) = \varphi^{-1}(\mathfrak{p})$. We can *upgrade* $\operatorname{Spec} R$ to a topological space by defining the closed sets of $\operatorname{Spec} R$ to be the sets of the form $V(I) = \{\mathfrak{p} : I \subseteq \mathfrak{p}\}$. This defines a topology because

$$V(I) \cap V(J) = V(I+J) \quad \text{and} \quad V(I) \cup V(J) = V(I \cap J).$$

We now define V formally.

Definition 1.13 (vanishing set). Let A be a ring. For each subset E of A, let

$$V(E) \quad \text{denote} \quad \text{the set of all prime ideals of } A \text{ which contain } E.$$

Definition 1.14 (radical). Let R be a ring. Given any $I \subseteq R$, set

$$\sqrt{I} = \{x \in R : x^n \in I \quad \text{for some } n \text{ depending on } x\}.$$

We call this the radical of I.

Example 1.11. We have $\sqrt{(4)} = (2)$.

Example 1.12. We have $\mathfrak{N}_R = \sqrt{(0)}$.

Proposition 1.14. Let I and J be ideals of a ring R. The following are fun to check:

(i) $\sqrt{\sqrt{I}} = \sqrt{I}$

(ii) $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$

(iii) $\sqrt{I} = R$ if and only if $I = R$

(iv) $\sqrt{I+J} = \sqrt{\sqrt{I} + \sqrt{J}}$

(v) If $\mathfrak{p}$ is prime, then $\sqrt{\mathfrak{p}^n} = \mathfrak{p}$

(vi) $\sqrt{I} = \bigcap_{\substack{I \subseteq \mathfrak{p} \\ \mathfrak{p} \text{ prime}}} \mathfrak{p}$

Proposition 1.15. Let I and J be ideals of a ring R. Then,

$$\sqrt{I} + \sqrt{J} = R \quad \text{implies} \quad I + J = A.$$

Proof. We have $\sqrt{I+J} = \sqrt{\sqrt{I} + \sqrt{J}} = \sqrt{R} = R$ so $I + J = R$. □

Example 1.13 (Atiyah and Macdonald p. 12 Question 15). Let A be a ring and let X be the set of all prime ideals of A. For each subset E of A, let

$$V(E) \quad \text{denote} \quad \text{the set of all prime ideals of } A \text{ which contain } E.$$

Prove the following:

(a) If $\mathfrak{a}$ is the ideal generated by E, then $V(E) = V(\mathfrak{a}) = V(r(\mathfrak{a}))$ (here, $r((\mathfrak{a}))$ denotes the radical of the ideal generated by $\mathfrak{a}$ in the ring);

(b) $V(0) = X$, $V(1) = \emptyset$;

(c) If $(E_i)_{i \in I}$ is any family of subsets of A, then

$$V\left(\bigcup_{i \in I} E_i\right) = \bigcap_{i \in I} V(E_i);$$

(d) $V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}\mathfrak{b}) = V(\mathfrak{a}) \cup V(\mathfrak{b})$ for any ideals $\mathfrak{a}, \mathfrak{b}$ of A.

Solution.

(a) By definition, $V(E) = \{\mathfrak{p} \in X : E \subseteq \mathfrak{p}\}$. Let $\mathfrak{a}$ be the ideal generated by E. Then, $\mathfrak{a}$ is the smallest ideal of A containing E. Hence,

$$\mathfrak{p} \text{ contains } E \quad \text{if and only if} \quad \mathfrak{p} \text{ contains } \mathfrak{a}.$$

As such, $V(E) = V(\mathfrak{a})$. We then prove that $V(\mathfrak{a}) = V(r(\mathfrak{a}))$. Recall Definition 1.14 which states that $r(\mathfrak{a}) = \{x \in A : x^n \in \mathfrak{a} \text{ for some } n\}$. By **(i)** of Proposition 1.14, $\mathfrak{p}$ is closed under taking radicals so a prime ideal $\mathfrak{p}$ contains $\mathfrak{a}$ if and only if it contains $r(\mathfrak{a})$ and the result follows.

(b) We have

$$V(0) = \{\mathfrak{p} \in A : 0 \in \mathfrak{p}) \quad \text{and} \quad V(1) = \{\mathfrak{p} \in A : 1 \in \mathfrak{p}).$$

So, $V(0)$ contains all prime ideals $\mathfrak{p}$ such that $0 \in \mathfrak{p}$. This is clearly X. Also, no prime ideal contains 1 as 1 generates the entire ring A. It follows that $V(1) = \emptyset$.

(c) We first prove the forward inclusion. Let

$$\mathfrak{p} \in V\left(\bigcup_{i\in I} E_i\right) \quad \text{so} \quad \bigcup_{i\in I} E_i \in \mathfrak{p}.$$

So, $E_i \subseteq \mathfrak{p}$ for all $i \in I$, and it follows that $\mathfrak{p}$ is contained in the intersection. The proof of the reverse inclusion is similar.

(d) For any prime ideal $\mathfrak{p}$, it contains the ideal $\mathfrak{a}\cap\mathfrak{b}$ if and only if it contains the ideals $\mathfrak{a}$ and $\mathfrak{b}$ of A, or equivalently $\mathfrak{ab}$ by **(i)** of Proposition 1.10 since $\mathfrak{ab} \subseteq \mathfrak{a}\cap\mathfrak{b}$ and both ideals generate the same radical in this case. So, $V(\mathfrak{a}\cap\mathfrak{b}) = V(\mathfrak{ab})$.

Next, we note that a prime ideal $\mathfrak{p}$ contains $\mathfrak{ab}$ if and only if $\mathfrak{p}$ contains either $\mathfrak{a}$ or $\mathfrak{b}$. This follows from the definition of a prime ideal. Hence, $V(\mathfrak{a}\cap\mathfrak{b}) = V(\mathfrak{a})\cup V(\mathfrak{b})$. □

Remark 1.3. The results in Example 1.13 show that the sets $V(E)$ satisfy the axioms for closed sets in a topological space. The resulting topology is called the *Zariski topology*. The topological space X is called the *prime spectrum of* A, and is written $\operatorname{Spec}(A)$.

Example 1.14 (Atiyah and Macdonald p. 12 Question 17). For each $f \in A$, let X_f denote the complement of $V(f)$ in $X = \operatorname{Spec}(A)$. The sets X_f are open. Show that they form a basis of open sets for the Zariski topology, and that

(i) $X_f \cap X_g = X_{fg}$;

(ii) $X_f = \emptyset$ if and only if f is nilpotent;

(iii) $X_f = X$ if and only if f is a unit;

(iv) $X_f = X_g$ if and only if $r((f)) = r((g))$ (here, $r((f))$ denotes the radical of the ideal generated by f in the ring);

(v) X is quasi-compact, i.e. every open covering of X has a finite subcovering;

(vi) More generally, each X_f is quasi-compact

(vii) An open subset of X is quasi-compact if and only if it is a finite union of sets X_f. The sets X_f are called *basic open sets* of $X = \operatorname{Spec}(A)$

Hint: To prove **(v)**, remark that it is enough to consider a covering of X by basic open sets X_{f_i}, where $i \in I$. Show that the f_i generate the unit ideal and hence that there is an equation of the form

$$1 = \sum_{i\in J} g_i f_i \quad g_i \in A$$

where J is some finite subset of I. Then the X_{f_i}, where $i \in J$, cover X.

Solution. We first show that the collection of X_f forms a basis of open sets for the Zariski topology. Given a ring A, let $f \in A$ and define

$$X_f = \{\mathfrak{p} \in \operatorname{Spec}(A) : f \notin \mathfrak{p}\}.$$

For any ideal $I \subseteq A$, we define $V(I) = \{\mathfrak{p} \in \operatorname{Spec}(A) : I \subseteq \mathfrak{p}\}$ as the closed sets. The complement of $V(f)$ is X_f, which as mentioned, is open. So, any open set in the Zariski topology is the union of such complements. Hence, the X_f form a basis.

(i) By definition,

$$X_f \cap X_g = \{\mathfrak{p} \in \operatorname{Spec}(A) : f \notin \mathfrak{p} \text{ and } g \notin \mathfrak{p}\} = \{\mathfrak{p} \in \operatorname{Spec}(A) : fg \notin \mathfrak{p}\} = X_{fg}$$

and the result follows.

(ii) For the forward direction, suppose $X_f = \emptyset$. Then, $f \in \mathfrak{p}$ for all $\mathfrak{p} \in \operatorname{Spec}(A)$, so f is nilpotent. For the reverse direction, if f is nilpotent, there exists $n \in \mathbb{N}$ such that $f^n = 0$. So, for every prime ideal $\mathfrak{p}$, we have $f \in \mathfrak{p}$ so $X_f = \emptyset$.

(iii) If f is a unit, then $f \notin \mathfrak{p}$ for all $\mathfrak{p} \in \operatorname{Spec}(A)$, so $X_f = X$. For the forward direction, if $X_f = X$, then $f \notin \mathfrak{p}$ for all $\mathfrak{p}$. Hence, f is not contained in any maximal ideal, which implies f is a unit.

(iv) Equivalent to saying that $V(f) = V(g)$.

(v) Let $\mathcal{S} = \{X_{f_i} : i \in I\}$ be an open cover of X. Since

$$X = \bigcup_{i \in I} X_{f_i} \quad \text{it implies} \quad \text{the } f_i \text{ generate the unit ideal } 1 = \sum_{i \in J} g_i f_i \text{ for some finite } J \subseteq I.$$

The result follows.

(vi) Note that X_f can be covered by open sets X_{f_i} so we then apply the same argument as **(v)**.

(vii) Trivial. □

Recall from Definition 1.11 that a ring R is reduced if there exists no non-zero nilpotent elements, i.e. $\mathfrak{N}_A = (0)$. As such, we have the following proposition.

Proposition 1.16. For $I \subseteq R$,

$$R/I \text{ is reduced} \quad \text{if and only if} \quad I = \sqrt{I}, \text{ i.e. } I \text{ is a radical ideal.}$$

Definition 1.15 (Jacobson radical)**.** Given a ring R, define

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

In other words, the Jacobson radical of R is the intersection of all maximal ideals $\mathfrak{m}$.

Proposition 1.17. $\mathfrak{N}_R \subseteq J(R)$

Proposition 1.18. We have

$$x \in J(R) \quad \text{if and only if} \quad 1 + yx \text{ is a unit for all } y \in R.$$

Proof. For the forward direction, choose $x \in J(R)$. Suppose on the contrary that $1 + xy$ is not a unit. Then, $1 + xy \in \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$. As $x \in \mathfrak{m}$, then $xy \in \mathfrak{m}$, so $1 \in \mathfrak{m}$, which is a contradiction.

For the reverse direction, suppose on the contrary that $x \notin \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$. Then, $(x) + \mathfrak{m} = R$, so we can write $1 = rx + m$ for some $m \in \mathfrak{m}$. Then, $m = 1 - rx$ is not a unit. The result follows. □

Definition 1.16 (ring of polynomials)**.** Given a ring R, consider the polynomial ring in one variable X, denoted by $R[X]$. It is defined as follows:

$$R[X] = \left\{\text{polynomials } \sum r_i X^i : r_i \in R \quad \text{and} \quad r_i = 0 \text{ for sufficiently large } i\right\}$$

Polynomial addition and multiplication (Cauchy product) are defined the obvious way.

Definition 1.17 (formal Laurent series)**.** Let R be a ring. The ring of formal Laurent series in the variable X over R (often denoted by $R[[X]]$ is defined as follows:

$$R[[X]] = \left\{ \sum_{i=N}^{\infty} r_i X^i : N \in \mathbb{Z}, r_i \in R \text{ for all } i, \text{finitely many negative indices } i \text{ for which } r_i \neq 0 \right\}.$$

In other words, although the sum can extend infinitely in the positive direction, it can only extend finitely in the negative direction.

Definition 1.16 can be generalised to multiple indeterminates.

Example 1.15 (construction of $\mathbb{C}$ by taking quotient of maximal ideal)**.** $\mathbb{R}[x]/(x^2+1) = \mathbb{C}$

Example 1.16 (Gaussian integers)**.** Let

$$\mathbb{Z}[i] = \{a+bi : a,b \in \mathbb{Z}\} \quad \text{denote the set of Gaussian integers.}$$

Then, $\mathbb{Z}[x]/(x^2+1) = \mathbb{Z}[i]$.

Example 1.17. Consider $(5) \subseteq \mathbb{Z}$. Then

$$\mathbb{Z}[i]/(5) = \mathbb{Z}[x]/(x^2+1,5) = \mathbb{F}_5[x]/(x^2+1) = \mathbb{F}_5[X]/((x-2)(x-3)) = \mathbb{F}_5 \times \mathbb{F}_5,$$

which is not an integral domain! Here, $\mathbb{F}_5$ is the finite field of 5 elements. Therefore, $(5)\mathbb{Z}[i] \subseteq \mathbb{Z}[i]$ is not prime[†].

Definition 1.18 (local ring)**.** A ring R is local if it has a unique maximal ideal $\mathfrak{m}$.

Example 1.18. Fields are local rings. To see why, the only ideals of any field F are $\{0\}$ and F. Since $\{0\}$ is the only proper ideal in F, it is the unique maximal ideal.

Proposition 1.19. If k is an arbitrary field, then

$$k[[X]] \text{ is a local ring} \quad \text{as} \quad \text{its only maximal ideal is } (X).$$

Proof. To show that any $f \notin (X)$ is invertible, write f as

$$f = r_0 + Xg, \quad \text{where } r_0 \neq 0 \text{ and } g \in k[[X]$$

We need to find $h \in k[[X]]$ such that $f \cdot h = 1$. Using formal power series, define

$$h = \frac{1}{r_0 + Xg}.$$

Using the geometric series expansion, this can be rewritten as

$$h = \frac{1}{r_0} \cdot \frac{1}{1 + X_g/r_0} = \frac{1}{r_0} \sum_{i=0}^{\infty} \left(-\frac{Xg}{r_0} \right)^i.$$

Since $Xg \in k[[X]]$, the series converges in the formal sense, and we obtain

$$h = r_0^{-1} \sum_{i=0}^{\infty} X^i g^i r_0^{-i}.$$

Thus, h is a formal power series and $f \cdot h = 1$, proving that f is invertible. □

[†]Prof. David Hansen mentioned that he did not want to delve too deep into MA5202 with the introduction of number fields, etc.

Example 1.19 (Atiyah and Macdonald p. 11 Question 10)**.** Let A be a ring and $\mathfrak{N}$ be its nilradical. Show that the following are equivalent:

(i) A has exactly one prime ideal;

(ii) every element of A is either a unit or nilpotent;

(iii) $A/\mathfrak{N}$ is a field

Solution. Recall from Proposition 1.6 that we defined the nilradical to be the set of nilpotent elements of A. We first prove that **(i)** implies **(ii)**. Consider a maximal ideal of A, which must be prime, say $\mathfrak{p}$, since A has exactly one prime ideal. By Definition 1.18, A is a local ring. So, every element of A is a unit or nilpotent.

To prove **(ii)** implies **(iii)**, it suffices to show that every element of $A/\mathfrak{N}$ is invertible. Take any $x+\mathfrak{N} \in A/\mathfrak{N}$ that is non-zero. So, $x \notin \mathfrak{N}$, i.e. x is not nilpotent. As such, x is a unit in A. Hence, there exists $y \in A$ such that $xy = 1$. In $A/\mathfrak{N}$, this means that

$$(x+\mathfrak{N})(y+\mathfrak{N}) = xy+\mathfrak{N} = 1+\mathfrak{N}.$$

Hence, $x+\mathfrak{N}$ is invertible in $A/\mathfrak{N}$.

Lastly, we prove **(iii)** implies **(i)**. Suppose $A/\mathfrak{N}$ is a field. As such, the nilradical is maximal, and thus prime. As

$$\mathfrak{N} = \bigcap_{\mathfrak{p}\in \operatorname{Spec} A} \mathfrak{p} \quad \text{it implies} \quad \text{every prime ideal contains } \mathfrak{N}.$$

Since $\mathfrak{N}$ is maximal, then every prime ideal coincides with $\mathfrak{N}$. We conclude that A only has one prime ideal. □

Example 1.20 (Atiyah and Macdonald p. 44 Question 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?

Solution. Suppose A has a non-zero nilpotent element x. Then, x belongs to all prime ideals $\mathfrak{p}$ of A, and so do all of its powers x^n, for every $n \in \mathbb{N}$. Let $\mathfrak{p}$ be a prime ideal. Then, $(x/1) \in A_\mathfrak{p}$ is nilpotent. As such, for every $\mathfrak{p}$, $x \in \mathfrak{p}$ so x belongs to the intersection of all prime ideals of A. As such, $\operatorname{Spec}(A) = \mathfrak{N}_A$. However, this contradicts the fact that $A_\mathfrak{p}$ has no non-zero nilpotent elements.

The second part is false. Take $A = \mathbb{Z}/6\mathbb{Z}$ which is not an integral domain. The prime ideals of A are $\mathfrak{p}_2 = (2/6)$ and $\mathfrak{p}_3 = (3/6)$ which correspond to 2 and 3 in $\mathbb{Z}$. We can then construct the local rings

$$A_{\mathfrak{p}_2} \cong \mathbb{Z}/2\mathbb{Z} \quad \text{and} \quad A_{\mathfrak{p}_3} \cong \mathbb{Z}/3\mathbb{Z} \quad \text{which are integral domains as they are fields.}$$

So, the second part is indeed false. □

1.2 Module Theory

Definition 1.19 (R-module)**.** Let R be a ring. An R-module M is an Abelian group $(M,+,0)$ equipped with a map of sets

$$R \times M \to M \quad \text{where} \quad (r,m) \mapsto m$$

such that the following properties hold:

(i) $(r_1+r_2)m = r_1m + r_2m$

(ii) $r(r'm) = (rr')m$
(iii) $r(m_1 + m_2) = rm_1 + rm_2$
(iv) $1_R \cdot m = m$

Definition 1.20 (R-module homomorphism)**.** Given R-modules M and N, we have an obvious notion of an R-module homomorphism $f : M \to N$. Given any such f, we can generate some new R-modules, namely

$$\ker f \subseteq M \quad \operatorname{im} f \subseteq N \quad \subseteq N \twoheadrightarrow \operatorname{coker} f.$$

Example 1.21. An ideal $I \subseteq R$ is an R-submodule of R.

Example 1.22. Let M and N be R-modules. Then,

$$\operatorname{Hom}_R(M,N) = \{R\text{-module maps } f : M \to N\}.$$

This is a natural R-module as

$$(f_1 + f_2)(m) = f_1(m) + f_2(m) \quad \text{and} \quad (rf)(m) = f(rm) = rf(m).$$

Example 1.23. We have $\operatorname{Hom}_R(R,M) = M$ by sending $f \mapsto f(1)$ and $f(1) \mapsto (r \mapsto rm)$.

Example 1.24. Given $I \subseteq R$, we have $\operatorname{Hom}_R(R/I,M) = M[I]$. Here, $M[I]$ refers to the torsion submodule of M associated with I, where we define

$$M[I] = \{m \in M : \text{there exists } i \in I \quad \text{such that } im = 0\}.$$

Example 1.25 (Atiyah and Macdonald p. 44 Question 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

$$S^{-1}B \text{ and } T^{-1}B \quad \text{are isomorphic as } S^{-1}A\text{-modules.}$$

Solution. Consider the

$$S^{-1}A\text{-module homomorphism } \phi : S^{-1}B \to T^{-1}B \quad \text{defined by} \quad b/s \mapsto b/f(s).$$

This map has an obvious inverse, i.e. the map that sends $b/f(s)$ to b/s, so we conclude that ϕ is an isomorphism. □

Definition 1.21 (submodule)**.** For a ring R with an ideal $I \subseteq R$, and an R-module M, IM denotes the submodule of M generated by the expressions of the form $i_1m_1 + \ldots + i_jm_j$.

Example 1.26. If $M = R$ then we have $IR = I$.

Chapter 2
Basic Commutative Algebra

2.1
Exact Sequences of Modules

Definition 2.1 (complex and exact sequences). Fix a ring R. A sequence of R-module homomorphisms

$$\ldots \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} M_{i+1} \xrightarrow{f_{i+1}} M_{i+2} \xrightarrow{f_{i+2}} \ldots$$

(i) is *complex* if $\operatorname{im} f_i \subseteq \ker f_{i+1}$ for all i, i.e. $f_{i+1} \circ f_i = 0$ for all i;
(ii) is an *exact sequence* if $\operatorname{im} f_i = \ker f_{i+1}$

We will often be in a situation where $M_i = 0$ for all but finitely many i.

Example 2.1. In the sequence of R-module homomorphisms $0 \to M \xrightarrow{f} N$, f is injective as $\ker f = \{0\}$.

Example 2.2. In the sequence of R-module homomorphisms $N \xrightarrow{g} Q \to 0$, g is surjective.

Example 2.3. The sequence of R-module homomorphisms

$$0 \to M \xrightarrow{\mathrm{id}} 0 \quad \text{is always exact.}$$

Definition 2.2 (short exact sequence). Suppose the sequence of R-module homomorphisms

$$0 \to M \xrightarrow{f} N \xrightarrow{g} Q \to 0 \quad \text{is exact.}$$

This is equivalent to saying that f is injective, g is surjective, and $\operatorname{im} f = \ker g$.

Example 2.4. Consider the following sequence of Abelian groups:

$$\mathbb{Z} \xrightarrow{\times 2} \mathbb{Z} \twoheadrightarrow \mathbb{Z}/2\mathbb{Z}$$

The first homomorphism maps each element $i \in \mathbb{Z}$ to the element $2i \in \mathbb{Z}$. The second homomorphism maps each element i in $\mathbb{Z}$ to the quotient group $\mathbb{Z}/2\mathbb{Z}$, that is $j \equiv i \pmod 2$. This is an exact sequence since the image of the red homomorphism is the kernel of the blue homomorphism[†].

Proposition 2.1. Given any R-module homomorphism $f : M \to N$, we can always obtain the following two short exact sequences:

$$0 \to \ker f \to M \to \operatorname{im} f \to 0$$
$$0 \to \operatorname{im} f \to N \to \operatorname{coker} f \to 0$$

Recall that $\operatorname{coker} f$ measures how far f is from being surjective. It is defined as the quotient module $f/\operatorname{im} f$.

[†]In Category Theory *language*, the hook arrow $\hookrightarrow$ denotes an injective homomorphism so we say that it is a monomorphism; the two-headed arrow $\twoheadrightarrow$ is a surjective homomorphism so we say that it is an epimorphism.

Definition 2.3 (finitely generated module)**.** An R-module M is finitely generated if there exist elements $x_1,\ldots,x_n \in M$ such hat all $m \in M$ can be expressed as a finite linear combination, i.e.

$$\sum_{i=1}^{n} r_i m_i \quad \text{for some } r_i \in R.$$

Note that if M is a finitely generated R-modue, it is equivalent to saying that there exists an exact sequence

$$R^n \to M \to 0$$
$$e_i \mapsto x_i$$

Definition 2.4 (finitely presented module)**.** An R-module M is finitely presented if there exists an exact sequence

$$R^m \to R^n \to M \to 0 \quad \text{for some } m,n \in \mathbb{N}.$$

Example 2.5. Let k be a field. Define

$$R = k[x_1,x_2,x_3,\ldots] \quad \text{and} \quad \mathfrak{m} = (x_1,x_2,x_3,\ldots) \quad \text{so } M = R/\mathfrak{m} \cong k.$$

Then, M is finitely generated but not finitely presented as $\mathfrak{m}$ is not finitely generated as an R-module.

Example 2.6. Suppose we have a short exact sequence $0 \to M_1 \to M_2 \to M_3 \to 0$. Then, M_1 and M_3 are finitely generated, which implies M_2 is also finitely generated (in Example 2.7, we will discuss the proof of this result but for the case where the sequence is exact, i.e. no assumption of it being a short exact sequence). The same result holds if we change the term 'finitely generated' to 'finitely presented'.

Example 2.7 (Atiyah and Macdonald p. 32 Question 9)**.** Let

$$0 \to M' \to M \to M'' \to 0 \quad \text{be} \quad \text{an exact sequence of } A\text{-modules.}$$

If M' and M'' are finitely generated, then so is M.

Solution. Suppose

$$M' \text{ is generated by } x_1,\ldots,x_n \quad \text{and} \quad M'' \text{ is generated by } z_1,\ldots,z_m.$$

Suppose $u : M' \to M$ and $v : M \to M''$ are A-module homomorphisms. Let $v(y_i) = z_i$ for all $1 \le i \le m$. Also, let $x \in M$. Then, there exist $b_1,\ldots,b_m \in A$ such that $v(x) = b_1 z_1 + \ldots + b_m z_m$. Hence,

$$v(x) = b_1 v(y_1) + b_m v(y_m) \quad \text{so} \quad v(x) = v(b_1 y_1 + \ldots + b_m y_m).$$

Hence, $x - b_1 y_1 - \ldots - b_m y_m \in \ker v$. As the sequence is exact, then $\operatorname{im} u = \ker v$. So, there exist $a_1,\ldots,a_n \in A$ such that

$$x - (b_1 y_1 + \ldots + b_m y_m) = a_1 u(x_1) + a_n u(x_n)$$
$$x = b_1 y_1 + \ldots + b_m y_m + a_1 u(x_1) + a_n u(x_n)$$

so M is generated by $u(x_1),\ldots,u(x_n),y_1,\ldots,y_m$. □

Example 2.8 (Atiyah and Macdonald p. 32 Question 12)**.** Let M be a finitely generated A-module and $\varphi : M \to A^n$ be a surjective homomorphism. Show that $\ker\varphi$ is finitely generated.

Hint: Let $e_1,\ldots,e_n$ be a basis for A^n and choose $u_i \in M$ such that $\varphi(u_i) = e_i$ for all $1 \le i \le n$. Show that M is the direct sum of $\ker\varphi$ and the submodule generated by $u_1,\ldots,u_n$.

Solution. Let $m \in M$, so $\varphi(m) \in A^n$. We can write

$$\varphi(m) = a_1e_1 + \ldots + a_ne_n \quad \text{where } a_1,\ldots,a_n \in A.$$

Also, let U be a submodule of M. Since M is finitely generated, then U is also finitely generated by say $u_1,\ldots,u_n$. So, there exist $a_1,\ldots,a_n \in A$ such that

$$\begin{aligned} u &= a_1u_1 + \ldots + a_nu_n \\ \varphi(u) &= a_1\varphi(u_1) + a_n\varphi(u_n) \\ &= a_1e_1 + \ldots + a_ne_n \end{aligned}$$

Since the RHS is $\varphi(m)$, then $\varphi(u-m) = 0$, so $u - m \in \ker\varphi$. Thus, for any $m \in M$, we can decompose it as $m = (m-u) + u$, which shows that M is the sum of $\ker\varphi$ (elements of the form $m-u$) and the submodule generated by $u_1,\ldots,u_n$.

We then show that the sum is direct, i.e. $\ker\varphi \cap U = \emptyset$. Suppose $m \in \ker\varphi \cap U$. Then, $m \in \ker\varphi$ and $m \in U$. The former tells us that $\varphi(m) = 0$, whereas the latter tells us that

$$m = a_1u_1 + \ldots + a_nu_n \quad \text{where } a_1,\ldots,a_n \in A.$$

Applying φ to both sides, we obtain $0 = a_1e_1 + \ldots + a_ne_n$. Since $e_1,\ldots,e_n$ is a basis for A^n, then $a_1 = \ldots = a_n = 0$. Hence $m = 0$ and the result follows. □

Lemma 2.1 (snake lemma)**.** Suppose we are given a commutative diagram of R-modules

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \xrightarrow{a} & M & \xrightarrow{b} & M'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f''} & & \\ 0 & \longrightarrow & N' & \xrightarrow{c} & N & \xrightarrow{d} & N'' & \longrightarrow & 0 \end{array}$$

where the rows are exact. Then, there exists a natural exact sequence

$$0 \to \ker f' \to \ker f \ker f'' \xrightarrow{\delta} \operatorname{coker} f' \to \operatorname{coker} f \to \operatorname{coker} f'' \to 0.$$

Proof. It suffices to construct δ. Given $x \in M''$ such that $f''(x) = 0$, pick $y \in M$ such that $b(y) = x$. Then $0 = f''(x) = f''(b(y)) = d(f(y))$. Thus $f(y) \in \ker d = \operatorname{im} c$, so there exists a unique $z \in N'$ such that $c(z) = f(y)$. We set $\delta(x) = z + f'$.

For well-definedness, we need to see that the choice of y does not matter. If $y' \in M$ with $b(y') = x$, then $y - y' \in \ker b = \operatorname{im} a$ so $f(y) - f(y') \in \operatorname{im} c$. □

Proposition 2.2 (Nakayama's lemma, useless version)**.** Fix a ring A. Pick M to be a finitely generated A-module and $I \subseteq A$ be an ideal. Let $\varphi : M \to M$ be an A-module homomorphism such that $\varphi(M) \subseteq IM$.

Then,

$$\text{there exists} \quad \text{an equation } \varphi^n + a_1\varphi^{n-1} + a_2\varphi^{n-2} + \ldots + a_n = 0 \quad \text{where } a_i \in I.$$

Proof. Pick $x_1, \ldots, x_n \in M$ generating M. Then, $\varphi(x_i) \in IM$. Since M is finitely generated, then

$$\varphi(x_i) = \sum_{j=1}^{n} a_{ij} x_j \quad \text{for some choice of } a_{ij} \in I.$$

We can write the equation as

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

Write the above as $\mathbf{Ax} = \mathbf{0}$ so

$$A_{ij} = \delta_{ij}\varphi(x_i) - a_{ij} \quad \text{and} \quad \mathbf{x} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}.$$

Recall from MA2001 that

$$\det(\mathbf{A})\,\mathbf{I}_n = \operatorname{adj}(\mathbf{A})\,\mathbf{A} \quad \text{where} \quad \operatorname{adj}(\mathbf{A})_{ij} = (-1)^{i+j} M_{ji}.$$

Hence,

$$\begin{bmatrix} \det(\mathbf{A})\,x_1 \\ \vdots \\ \det(\mathbf{A})\,x_n \end{bmatrix} = \det(\mathbf{A})\,\mathbf{I}_n\mathbf{x} = \operatorname{adj}(\mathbf{A})\,\mathbf{Ax} = \mathbf{0}.$$

As such, $\det(\mathbf{A})\,x_i = 0$ for all $1 \leq i \leq n$. So, $\det(\mathbf{A}) = 0$ in $\operatorname{Hom}_A(M,M)$. We conclude that $\det(\mathbf{A}) = \varphi^n + a_1\varphi^{n-1} + \ldots + a_n$, where $a_i \in I$. □

Corollary 2.1. Let M be a finitely generated A-module and $I \subseteq A$ be an ideal such that $IM = M$. Then,

$$\text{there exists } a \equiv 1 \pmod{I} \quad \text{such that} \quad aM = 0.$$

Proof. If $IM = M$, then by Proposition 2.2, we have $0 = 1 + a_1 + \ldots + a_n$ as elements of $\operatorname{Hom}_A(M,M)$, where the RHS is an element of I. Setting $a = 1 + a_1 + \ldots + a_n$, the result follows. □

Proposition 2.3 (Nakayama's lemma V1). Let M be a finitely generated A-module and $I \subseteq J(A)$ be an ideal (recall that $J(A)$ is the Jacobson radical of A). If $IM = M$, then $M = 0$.

Proof. By Corollary 2.1, we obtain some $a = 1 + I$ with $aM = 0$. However, $I \subseteq J(A)$, which implies $a \in A^\star$. So, $M = a^{-1}(aM) = 0$. □

Example 2.9. Let $A = \mathbb{Z}/4\mathbb{Z}$ and M be a finitely-generated A-module. Recall that the Jacobson radical $J(A)$ is the intersection of all maximal ideals $\mathfrak{m}$ of A, for which there is only one (2). As such, $J(A) = 2A$. Setting $I = J(A)$, we have $J(A)M = M$ since $2M = M$. As such,

$$IM = M \quad \text{which implies} \quad M = 0 \text{ (the zero module)}.$$

Example 2.10 (Atiyah and Macdonald p. 32 Question 10)**.** Let A be a ring, $\mathfrak{a}$ an ideal contained in $J(A)$; let M be an A-module and N a finitely generated A-module, and let $u : M \to N$ be a homomorphism. If $M/\mathfrak{a}M \to N/\mathfrak{a}N$ is surjective, prove that u is surjective.

Solution. We will make use of V1 of Nakayama's lemma (Proposition 2.3). Define $L = N/u(M)$. We shall prove that $L = 0$, i.e. $N = u(M)$,, and consequently, u is surjective. Since

$$M/\mathfrak{a}M \to N/\mathfrak{a}N \quad \text{is surjective,}$$

then for every element $\overline{n} \in N/\mathfrak{a}N$, there exists $\overline{m} \in M/\mathfrak{a}M$ mapping to it. As such, $N/\mathfrak{a}N = (u(M) + \mathfrak{a}N)/\mathfrak{a}N$, or equivalently, $N = u(M) + \mathfrak{a}N$. As such, we have

$$L = N/u(M) = (u(M) + \mathfrak{a}N)/u(M).$$

From here, one can deduce that $L \subseteq \mathfrak{a}N/u(M)$, so $L = \mathfrak{a}L$. Since $\mathfrak{a}$ is an ideal contained in the Jacobson radical $J(A)$, then by applying Nakayama's lemma (Proposition 2.3) to the finitely-generated A-module L (since $L = \mathfrak{a}L$), then $L = 0$. The result follows. □

Example 2.11 (Atiyah and Macdonald p. 31 Question 3)**.** Let A be a local ring, M and N finitely generated A-modules. Prove that if

$$M \otimes_A N = 0 \quad \text{then} \quad M = 0 \text{ or } N = 0.$$

Hint: Let $\mathfrak{m}$ be the maximal ideal, $k = A/\mathfrak{m}$ the residue field. Let $M_k = k \otimes_A M \cong M/\mathfrak{m}M$. By Nakayama's lemma, $M_k = 0$ implies $M = 0$. But,

$$M \otimes_A N = 0 \quad \text{implies} \quad (M \otimes_A N)_k = 0 \quad \text{implies} \quad M_k \otimes_k N_k = 0 \quad \text{implies} \quad M_k = 0 \text{ or } N_k = 0$$

since M_k, N_k are vector spaces over a field.

Solution. We first regurgitate the hint. Let $\mathfrak{m}$ be the maximal ideal of A and $k = A/\mathfrak{m}$ denote its residue field. We also let

$$M_k = k \otimes_A M \cong M/\mathfrak{m}M.$$

The condition $M \otimes_A N = 0$ implies

$$k \otimes_A (M \otimes_A N) \cong (M \otimes_A N)_k = 0.$$

By the associativity of the tensor product,

$$k \otimes_A (M \otimes_A N) \cong (k \otimes_A M) \otimes_k (k \otimes_A N) \cong M_k \otimes_k N_k \quad \text{which implies} \quad M_k \otimes_k N_k = 0.$$

Note that M_k and N_k are vector spaces over the field $k = A/\mathfrak{m}$. Recall a basic fact states that if V and W are non-zero vector spaces over k, then

$$\dim_k (V \otimes_k W) = \dim_k (V) \cdot \dim_k (W).$$

Letting $V = M_k$ and $W = N_k$, it follows that

$$\dim_k (M_k \otimes_k N_k) = 0 \quad \text{so} \quad \dim_k (M_k) \cdot \dim_k (N_k) = 0.$$

Hence, either $M_k = 0$ or $N_k = 0$. By version 1 of Nakayama's lemma (Proposition 2.3, and recall that the Jacobson radical is the intersection of all maximal ideals), it follows that $M = 0$. □

Proposition 2.4 (Nakayama's lemma V2). Let M be a finitely generated A-module, $N \subseteq M$ and $I \subseteq J(A)$. Then,

$$M = IM + N \quad \text{implies} \quad M = N.$$

Proof. Applying version 1 of Nakayama's lemma (Proposition 2.3) to $Q = M/N$, we obtain

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

Again by applying Proposition 2.3, we have $Q = 0$ so $M = N$. □

Proposition 2.5 (Nakayama's lemma V3). Let $(A, \mathfrak{m})$ be a local ring and $k = A/\mathfrak{m}$ denote its residue field. If M is a finitely generated A-module and $x_1, \ldots, x_n \in M/\mathfrak{m}M$ span $M/\mathfrak{m}M$ as a k-vector space, then any choice of lifts $\widetilde{x_1}, \ldots, \widetilde{x_n} \in M$ generate M as an A-module.

Proof. Take $N \subseteq M$ to be the submodule generated by $\widetilde{x_1}, \ldots, \widetilde{x_n}$. Then, $M = N + \mathfrak{m}M$, so $M = N$ by Proposition 2.5. □

Example 2.12. Recall that every field is a local ring (Example 1.18). For any field k, let $A = k[x]$ and let $\mathfrak{m} = (x)$ be the maximal ideal in A. Take $M = A/(x^2)$ as an A-module. The residue field is $k = A/\mathfrak{m}$. The module $M/\mathfrak{m}M = (A/(x^2))/(x) = k$, which is a 1-dimensional k-vector space. Also, the element $\overline{1} \in M/\mathfrak{m}M$ spans $M/\mathfrak{m}M$ as a k-vector space. By Proposition 2.5, the lift $\widetilde{1} = 1 \in M$ generates M as an A-module. We conclude that $A/(x^2)$ is cyclic as an A-module.

2.2 Localization

Definition 2.5 (multiplicatively closed set). Fix a ring A. A subset $S \subseteq A$ is said to be multiplicatively closed if

$$1 \in S \quad \text{and} \quad \text{for all } s_1, s_2 \in S \text{ we have } s_1 s_2 \in S.$$

Example 2.13. For any ring A, the set of non-zero divisors is multiplicatively closed.

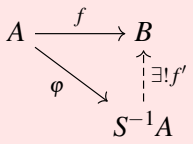
Example 2.14. For any $f \in A$, $\{1, f, f^2, \ldots\}$ is multiplicatively closed.

Example 2.15. For any prime ideal $\mathfrak{p}$ of A, the set $A \setminus \mathfrak{p}$ is multiplicatively closed.

Theorem 2.1. Given a ring A and any multiplicatively closed $S \subseteq A$, there exists a naturally associated ring $S^{-1}A$ equipped with a ring homomorphism $\varphi : A \to S^{-1}A$ ($S^{-1}A$ denotes the localization of A at S) such that for any ring homomorphism $f : A \to B$ where $f(S) \subseteq B^\times$, there exists a *unique* ring homomorphism

$$f' : S^{-1}A \to B \quad \text{such that} \quad f = f' \circ \varphi.$$

Hence, the following diagram commutes:



In other words words, $\varphi_S : A \to S^{-1}A$ is *universal* for ring homomorphisms $f : A \to B$ sending S to units.

Proof. We will first construct $S^{-1}A$ as a set. Let

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

with $(a,s) \sim (a',s')$ if and only if there exists $t \in S$ such that $t(as' - a's) = 0$. We define

$$(a,s) \cdot (a',s') = (aa',ss')$$
$$(a,s) + (a',s') = (as' + a's, ss')$$

The multiplicative identity is $(1,1)$ and the additive identity is $(0,1)$.

We will write $\frac{a}{b}$ for the equivalence class of (a,b). The universal map $\varphi_S : A \to S^{-1}A$ is defined by $a \mapsto (a,1)$. Given $f : A \to B$, suppose that $f = f' \circ \varphi_S$ for some $f' : A \to S^{-1}A$, then $f(S) \subseteq f'((S^{-1}A)^\times) \subseteq B^\times$.

Now suppose that $f(S) \subseteq B^\times$. Note that $a \in \ker \varphi_S$ if and only if there exists $s \in S$ such that $sa = 1$. Now define $f'\left(\frac{a}{s}\right) = f(a)f(s)^{-1}$. We need to show that this is well-defined, i.e. independent of the choice of representatives. If $(a,s) \sim (a',s')$ then there exists $t \in S$ such that $tas' - ta's = 0$, so applying f gives

$$f(t)f(a)f(s') = f(t)f(a')f(s) = 0,$$

whence multiplying by $(f(s)f(s')f(t))^{-1}$ gives $f(a)f(s)^{-1} - f(a')f(s')^{-1} = 0$ as required. It is clear by construction that $g' \circ \varphi_S = f$. This map is unique because $\ker \varphi_S \subseteq \ker f$. Note that $\varphi_S(s)$ is a unit for all $s \in S$, since $(s,1) = (1,s) = (1,1) = 1_{S^{-1}A}$. □

Corollary 2.2. We have

$$\varphi_S : A \to S^{-1}A \text{ is an isomorphism} \quad \text{if and only if} \quad S \subseteq A^\times.$$

Proof. For the forward direction, note that $\varphi(S) \subseteq \left(S^{-1}A\right)^\times$, but φ_S is an isomorphism, so $S \subseteq A^\times$. For the reverse direction, we use the universal property of $S^{-1}A$ on $\mathrm{id} : A \to A$ to find $f^{-1} : S^{-1}A \to A$ such that $\mathrm{id} : f \circ \varphi_S$. The result follows. □

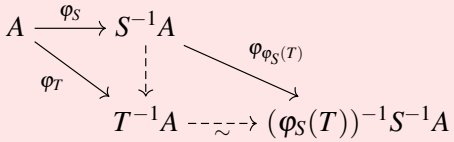
We briefly remark that φ_S is not always injective. For instance, if $A = \mathbb{Z}/6\mathbb{Z}$ and $S = \{1,2,4\}$, then $S^{-1}A = \mathbb{Z}/3\mathbb{Z}$. One checks that $S \subseteq A$. Moreover, S is a multiplicatively closed subset of A. That is to say, S is closed under multiplication. We will justify that $S^{-1}A = \mathbb{Z}/3\mathbb{Z}$ (recall that this process is known as localization, which makes the elements of S invertible). Elements of $S^{-1}A$ are of the form $\frac{a}{s}$, where $a \in A$ and $s \in S$, with the rule that

$$\frac{a}{s} = \frac{b}{t} \quad \text{if and only if} \quad \text{there exists a unit } u \text{ such that } u(sa - tb) = 0 \text{ in } A.$$

Consider $2 \in S$, which satisfies $\gcd(2,6) = 2$. So, multiplication by 2 annihilates $\overline{3}$, i.e. $2 \cdot \overline{3} = \overline{0}$. The condition 2 is invertible in the localization implies that 3 must be sent to 0. As such, the ring $\mathbb{Z}/6\mathbb{Z}$ effectively collapses as if we were also factoring the ideal generated by 3. Indeed, it is clear that 2 is invertible in $\mathbb{Z}/3\mathbb{Z}$ since $2 \cdot 2 \equiv 1 \pmod 3$.

Having said all the above, if however S does not contain any zero divisors, then φ_S is injective. In particular, if A is an integral domain, then φ_S is injective for any S and $S^{-1}A$ is also an integral domain.

Proposition 2.6. If $S \subseteq T \subseteq A$ are multiplicatively closed, then the following diagram commutes:



Example 2.16. Choose $f \in A$ and take $S = \{1, f, f^2, \ldots\}$ which is multiplicatively closed. Then, we can write $A_f = S^{-1}A$.

Proposition 2.7. We have $A_f \cong A[X]/(1 - fX)$.

Now let R be a ring, $S \subseteq R$ be multiplicatively closed, and consider $\varphi_S : R \to S^{-1}R$. If $I \subseteq R$ is an ideal of R, then $\varphi_S(I) S^{-1}R \subseteq S^{-1}R$ is an ideal of $S^{-1}R$. Likewise if $J \subseteq S^{-1}R$ is an ideal of $S^{-1}R$, then $\varphi_S^{-1} \subseteq R$ is an ideal of R. We can verify the following facts:

- $\varphi_S^{-1}\left(\varphi_S(I) S^{-1}R\right) \supseteq I$;
- $J \supseteq \varphi_S\left(\varphi_S^{-1}(J)\right) S^{-1}R$

In general, equality does not hold. But things are nicer with prime ideals.

Theorem 2.2. There exists a canonical bijection

$$\{\text{prime } \mathfrak{p} \subseteq R \mid \mathfrak{p} \cap S = \emptyset\} \cong \{\text{prime ideals } \mathfrak{q} \subseteq S^{-1}R\}$$

sending $\mathfrak{p} \to \varphi_S(\mathfrak{p}) S^{-1}R$ and $\mathfrak{q} \mapsto \varphi_S^{-1}(\mathfrak{q})$.

Definition 2.6 (saturation). Let $\mathfrak{a} \subseteq R$ be any subset. We define the *saturation* of $\mathfrak{a}$ with respect to S to be

$$\mathfrak{a}^S = \{a \in R \mid sa \in \mathfrak{a} \quad \text{for some } s \in S\}.$$

If $\mathfrak{a} = \mathfrak{a}^S$, we say that $\mathfrak{a}$ is *saturated*.

Proposition 2.8. Let R be a ring. Fix a multiplicatively closed subset $S \subseteq R$. Then, the following hold:

(i) If $\mathfrak{b} \subseteq S^{-1}R$ is an ideal, then $\varphi_S^{-1}(\mathfrak{b}) = \left(\varphi_S^{-1}(\mathfrak{b})\right)^S$ and $\mathfrak{b} = \varphi_S^{-1}(\mathfrak{b}) S^{-1}R$

(ii) If $\mathfrak{b} \subseteq R$ is an ideal, then $\varphi_S(\mathfrak{a}) S^{-1}R = \varphi_S\left(\mathfrak{a}^S\right) S^{-1}R$ and $\varphi_S^{-1}\left(\varphi_S(\mathfrak{a}) S^{-1}R\right) = \mathfrak{a}^S$

(iii) Let $\mathfrak{p} \subseteq R$ be a prime ideal with $\mathfrak{p} \cap S = \emptyset$. Then $\mathfrak{p} = \mathfrak{p}^S$ and $\varphi_S(\mathfrak{p}) S^{-1}R \subseteq S^{-1}R$ is prime.

Proof. We first prove the first part of **(i)**. Suppose $a \in \varphi_S^{-1}(\mathfrak{b})$. Then,

$$\frac{as}{1} \in \mathfrak{b} \subseteq S^{-1}R.$$

Since s is a unit in $S^{-1}R$, then we can write

$$\frac{a}{1} = \frac{as}{1} \cdot \frac{1}{s} \in \mathfrak{b} \quad \text{so} \quad \varphi_S(a) \in \mathfrak{b}.$$

As such, $a \in \varphi_S^{-1}(\mathfrak{b})$. One can deduce $\subseteq$ of the first part from here. $\supseteq$ is obvious.

We then prove the second part of **(i)**. Suppose $\varphi_S(a) \in \mathfrak{b}$, so $a \in \varphi_S^{-1}(\mathfrak{b})$. So,

$$\frac{a}{s} = \frac{a}{1} \cdot \frac{1}{s} \in \varphi_S^{-1}(\mathfrak{b}) S^{-1}R,$$

which implies $\mathfrak{b} \subseteq \varphi_S^{-1}(\mathfrak{b}) S^{-1}R$, proving $\subseteq$. Note that $\supseteq$ is obvious, so **(i)** holds.

We then prove the first part of **(ii)**. Suppose $a \in \mathfrak{a}^S$, i.e. there exists s with $sa \in \mathfrak{a}$. Thus,

$$\frac{a}{1} = \frac{as}{1} \cdot \frac{1}{s} \in \varphi_S(\mathfrak{a}) S^{-1}R.$$

Thus, $\subseteq$ follows. Note that $\supseteq$ is obvious, so the first part of **(ii)** follows. For the second part, suppose $x \in \varphi_S^{-1}\left(\varphi_S(\mathfrak{a}) S^{-1}R\right)$. Then,

$$\frac{x}{1} = \frac{a}{s} \quad \text{with} \quad a \in \mathfrak{a} \text{ and } s \in S.$$

This implies that there exists $t \in S$ such that $xst = at$ in $\mathfrak{a}$. As such, $x \in \mathfrak{a}^S$. Thus, $\varphi_S^{-1}\left(\varphi_S(\mathfrak{a}) S^{-1}R\right) \subseteq \mathfrak{a}^s$, proving the forward direction $\subseteq$. The reverse direction $\subseteq$ holds as the left side is saturated by 1. As such, the second part of **(ii)** holds, so **(ii)** holds.

Lastly, we prove **(iii)**. For the first part, take $as \in \mathfrak{p}$ for some prime ideal $\mathfrak{p} \subseteq R$. Since $\mathfrak{p} \cap S = \emptyset$, this implies $a \in \mathfrak{p}$. As such, $\mathfrak{p}^S \subseteq \mathfrak{p}$, proving $\supseteq$. The proof of the forward direction $\subseteq$ is clear.

We then prove the second part. Note that

$$\varphi_S(\mathfrak{p}) S^{-1}R \neq S^{-1}R \quad \text{because} \quad \varphi_S^{-1}\left(\varphi_S(\mathfrak{p}) S^{-1}R\right) = \mathfrak{p}^S = \mathfrak{p}.$$

The last equality follows from the first part of **(iii)**. Now, suppose we are given some element

$$\frac{a}{s} \cdot \frac{b}{t} \in \varphi_S(\mathfrak{p}) S^{-1}R.$$

Then,

$$ab \in \varphi_S^{-1}\left(\varphi_S(\mathfrak{p}) S^{-1}R\right) = \mathfrak{p}.$$

Since $\mathfrak{p}$ is a prime ideal, then either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. So,

$$\frac{a}{s} \text{ or } \frac{b}{t} \quad \text{is an element of } \varphi_S(\mathfrak{p}) S^{-1}R.$$

It follows that $\varphi_S(\mathfrak{p}) S^{-1}R$ is prime, completing the proof. □

Example 2.17. If $S = \{1, f, f^2, \ldots\}$ with $S^{-1}R = R_f$, then the induced map $\operatorname{Spec}(R_f) \to \operatorname{Spec}(rR)$ is injective with image $\{\mathfrak{p} \subseteq R \mid f \notin \mathfrak{p}\} = \operatorname{Spec}(R \setminus V(f))$. In particular, the image is an open subset.

Definition 2.7 (localization). Let A be a ring and $S \subseteq A$ be multiplicatively closed. Suppose M is an A-module. Define an $S^{-1}A$ module as follows:

$$S^{-1}M = M \times S/\sim \quad \text{where} \quad (m,s) \sim (m',s') \text{ if there exists } t \in S \text{ such that } t(s'm - sm') = 0$$

We use the notation $\frac{m}{s}$ to refer to the equivalence class (m,s). Addition and scalar multiplication are defined in the following obvious way:

$$(m,s) + (m',s') = (s'm + sm', ss') \quad \text{and} \quad (a,s) \cdot (m,t) = (am, st)$$

If $f : M \to N$ is any map of A-modules, we obtain an induced map

$$S^{-1}f : S^{-1}M \to S^{-1}N \quad \text{of } S^{-1}A\text{-modules.}$$

In Category theory, we say that $S^{-1}(\cdot)$ is a functor from an A-module to an $S^{-1}A$-module.

Proposition 2.9. If

$$M' \xrightarrow{f} M \xrightarrow{g} M'' \quad \text{is} \quad \text{exact at } M,$$

then

$$S^{-1}M \xrightarrow{S^{-1}f} S^{-1}M \xrightarrow{S^{-1}g} S^{-1}M \quad \text{is} \quad \text{exact at } S^{-1}M.$$

Proof. Note that $\operatorname{im}\left(S^{-1}f\right) \subseteq \ker\left(S^{-1}g\right)$ since

$$\left(S^{-1}g \circ S^{-1}f\right)\left(\frac{m'}{s}\right) = \frac{g\left(f\left(m'\right)\right)}{s} = \frac{0}{s} = 0.$$

Next, suppose we are given some $\frac{m}{s} \in M$ with

$$\frac{g\left(m\right)}{s} = 0 \quad \text{in } S^{-1}M''.$$

Then, there exists $t \in S$ such that $t\left(g\left(m\right)\right) = 0$ in M''. This implies $g\left(tm\right) = 0$. As such, there exists $n \in M'$ such that $f\left(n\right) = tm$. Applying $S^{-1}f$ yields

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

which is contained in $S^{-1}f$. □

Recall that localization induces an injective map $\operatorname{Spec}\left(S^{-1}A\right) \to \operatorname{Spec}^{-1}\left(A\right)$ with image $\mathfrak{q}$ such that $\mathfrak{q} \cap S = \emptyset$. If $S = A \setminus \mathfrak{p}$, then this simplifies to $\operatorname{Spec}\left(A_{\mathfrak{p}}\right) = \mathfrak{q} \subseteq A$ such that $\mathfrak{q} \subseteq \mathfrak{p}$. In particular, $A_{\mathfrak{p}}$ is a local ring with a unique maximal ideal.

Definition 2.8. Let M be an A-module. Also, let $\mathfrak{p}, \mathfrak{m}$ be a prime ideal and a maximal ideal of A respectively. Then,

$$M_{\mathfrak{p}} \text{ denotes the localization of } M \text{ at } \mathfrak{p} \quad \text{and} \quad M_{\mathfrak{m}} \text{ denotes the localization of } M \text{ at } \mathfrak{m}.$$

Proposition 2.10. Let M be an A-module. Then, the following are equivalent:

(i) $M = 0$
(ii) For all prime ideals $\mathfrak{p}$, we have $M_{\mathfrak{p}} = 0$
(iii) For all maximal ideals $\mathfrak{m}$, we have $M_{\mathfrak{m}} = 0$

Proof. **(i)** implies **(ii)** implies **(iii)** is obvious.

To prove **(iii)** implies **(i)**, suppose $M \neq 0$. Choose some non-zero $x \in M$. Then, $\operatorname{Ann}\left(x\right)$, which denotes all $a \in A$ such that $ax = 0$ (recall that this is called the annihilator of x), is a proper subset of A. Hence, there exists a maximal ideal $\mathfrak{m}$ with $\operatorname{Ann}\left(x\right) \subseteq \mathfrak{m}$.

Now, consider $\frac{x}{1} \in M_{\mathfrak{m}}$. If $\frac{x}{1} = 0$ in $M_{\mathfrak{m}}$, then $sx = 0$ for some $s \in A \setminus \mathfrak{m}$. However, $\left(A \setminus \mathfrak{m}\right) \cap \operatorname{Ann}\left(x\right) = \emptyset$. Thus, $\frac{x}{1} \neq 0$ in $M_{\mathfrak{m}}$, implying that $M_{\mathfrak{m}} \neq 0$. □

Proposition 2.11. Let $f : M \to N$ be any a A-module homomorphism. Then, the following are equivalent:

(i) f is injective

(ii) For all prime ideals $\mathfrak{p}$, $f_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ is injective

(iii) For all maximal ideals $\mathfrak{m}$, $f_{\mathfrak{m}} : M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ is injective

2.3 Tensor Products

Definition 2.9 (bilinear map). Fix a ring A. Let M, N, P be A-modules. A map $b : M \times N \to P$ is said to be bilinear if the following properties hold:

(i) $b(m+m', n) = b(m,n) + b(m',n)$ and $b(m, n+n') = b(m,n) + b(m,n')$

(ii) $b(am, n) = b(m, an) = a \cdot b(m,n)$

We let

$$\mathrm{Bil}_A(M \times N, P) \quad \text{denote} \quad \text{the set of bilinear maps } b : M \times N \to P \text{ over } A.$$

Lemma 2.2. There exists an A-module $M \otimes_A N$ together with an A-bilinear map

$$b^{\mathrm{univ}} : M \times N \to M \otimes_A N$$

such that the induced map

$$\mathrm{Hom}_A(M \otimes_A N, P) \to \mathrm{Bil}_A(M \times N, P) \quad \text{where} \quad f \to f \circ b^{\mathrm{univ}} \quad \text{is} \quad \text{an isomorphism for all } P.$$

Proof. We discuss the construction of $M \otimes_A N$ as a module. Let F be the free A-module generated by all pairs (m,n). Let $R \subseteq F$ be the A-submodule generated by all elements of the following forms:

(i) $(m_1 + m_2, n) - (m_1, n) - (m_2, n)$

(ii) $(m, n_1 + n_2) - (m, n_1) - (m, n_2)$

(iii) $(am, n) - a(m,n)$

(iv) $(m, an) - a(m,n)$

Set $M \otimes_A N = F/R$. Consider the map

$$F \to M \otimes_A N \quad \text{where} \quad (m,n) \mapsto (m \otimes n).$$

By construction, $M \otimes_A N$ is spanned by the elements $m \otimes n$ and these satisfy the following relations:

(i) $(m_1 + m_2) \otimes n = m_1 \otimes n + m_2 \otimes n$

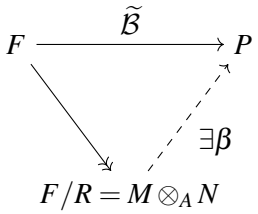
(ii) $m \otimes (n_1 + n_2) = m \otimes n_1 + m \otimes n_2$

(iii) $(am) \otimes n = a(m \otimes n) = m \otimes (an)$

Thus the map $b^{\mathrm{univ}} : M \times N \to M \otimes_A N$ sending $(m,n) \mapsto m \otimes n$ is bilinear. It is also clear that if $f : M \otimes_A N \to P$ is any A-module map, the induced map $f \circ b^{\mathrm{univ}} : M \times N \to P$ is A-bilinear. Conversely, suppose that we have a bilinear map $\mathcal{B} : M \times N \to P$. Define an A-module map $\widetilde{\mathcal{B}} : F \to P$ defined by

$$\sum a_i (m_i, n_i) \mapsto \sum a_i \mathcal{B}(m_i, n_i).$$

By the definition of bilinearity, we have $R \subseteq \ker \widetilde{B}$. Thus, $\widetilde{B}$ factors as



for some unique A-module map β. Finally, it is clear that $\beta \circ b^{\text{univ}} = \mathcal{B}$ by construction. □

Proposition 2.12. Here are some nice properties of the tensor product.

(i) $M \otimes_A A = M$

(ii) $M \otimes_A N \cong N \otimes_A M$

(iii) $(M_1 \oplus M_2) \otimes_A N \cong (M_1 \otimes_A N) \oplus (M_2 \otimes_A N)$

(iv) $(M \otimes_A N) \otimes_A K \cong M \otimes_A (N \otimes_A K)$

Here is a generalisation of **(iv)**. Suppose we are given two rings A and B. let M and N be A- and B-modules respectively and P be an (A,B)-module. Then,

$$M \otimes_A P \text{ is a } B\text{-module} \quad \text{and} \quad P \otimes_B N \text{ is an } A\text{-module.}$$

Moreover,

$$(M \otimes_A P) \otimes_B N \cong M \otimes_A (P \otimes_B N).$$

Example 2.18 (Atiyah and Macdonald p. 31 Question 1)**.** Show that

$$(\mathbb{Z}/m\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/n\mathbb{Z}) = 0 \quad \text{if } m,n \text{ are coprime.}$$

Solution. By Bézout's lemma, there exist $a,b \in \mathbb{Z}$ such that $am + bn = 1$. Hence, given

$$x \otimes y \in (\mathbb{Z}/m\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/n\mathbb{Z}),$$

it implies that

$$x \otimes y = 1(x \otimes y) = (am+bn)(x \otimes y) = am(x \otimes y) + bn(x \otimes y) = a(mx \otimes y) + b(x \otimes ny) = a(0 \otimes y) + b(x \otimes 0)$$

which is equal to 0. Since every generator is identically zero, then so is their tensor product. □

Example 2.19 (Atiyah and Macdonald p. 31 Question 2)**.** Let A be a ring, $\mathfrak{a}$ an ideal, M an A-module. Show that

$$(A/\mathfrak{a}) \otimes_A M \cong M/\mathfrak{a}M.$$

Hint: Tensor the exact sequence $0 \to \mathfrak{a} \to A \to A/\mathfrak{a} \to 0$ with M.

Solution. We tensor the exact sequence

$$0 \xrightarrow{\text{inclusion}} \mathfrak{a} \xrightarrow{\text{projection } \pi} A/\mathfrak{a} \to 0$$

so we obtain

$$\mathfrak{a} \otimes_A M \xrightarrow{\text{inclusion}\otimes 1} A \otimes_A M \xrightarrow{\pi \otimes 1} (A/\mathfrak{a}) \otimes_A M \to 0.$$

There is a standard isomorphism $A \otimes_A M \cong M$, where $a \otimes m \mapsto am$. Using this, we infer that

$$\mathfrak{a} \otimes_A M \xrightarrow{\text{inclusion}\otimes 1} M \xrightarrow{\pi \otimes 1} (A/\mathfrak{a}) \otimes_A M \to 0.$$

We can let the inclusion map be denoted by ι. Then, $\iota \otimes 1 : \mathfrak{a} \otimes_A M \to M$ sends an elementary tensor $a \otimes m$ (with $a \in \mathfrak{a}$ and $m \in M$) to am in M. The image of this map is the set

$$\{am : a \in \mathfrak{a}, m \in M\} = \mathfrak{a}M.$$

This is the submodule of M generated by products of elements in $\mathfrak{a}$ with elements of M. Hence,

$$(A/\mathfrak{a}) \otimes_A M \cong \operatorname{coker}(\iota \otimes 1) = M/\operatorname{im}(\iota \otimes 1) = \mathfrak{a}M.$$

The result follows. □

Example 2.20 (Atiyah and Macdonald p. 32 Question 8)**.**

(i) If M and N are flat A-modules, then so is $M \otimes_A N$.

(ii) If B is a flat A-algebra and N is a flat B-module, then N is flat as an A-module.

Solution.

(a) This holds because the tensor functor is associative, i.e. tensoring an exact sequence first by M and then by N is equivalent to tensoring by $M \otimes_A N$.

(b) The idea is to use the fact that flatness is preserved under base change (i.e. tensoring with a flat module preserves exact sequences) and that tensor products are associative. We start with a short exact sequence of A-modules

$$0 \to M' \to M \to M'' \to 0.$$

Since B is flat over A, tensoring the above sequence with B preserves exactness, i.e.

$$0 \to M' \otimes_A B \to M \otimes_A B \to M'' \otimes_A B \to 0.$$

Now, consider the sequence obtained in the previous step and tensor it with N over B. Since N is flat as a B-module, the following sequence remains exact:

$$0 \to \left(M' \otimes_A B\right) \otimes_B N \to (M \otimes_A B) \otimes_B N \to \left(M'' \otimes_A B\right) \otimes_B N \to 0$$

By the associativity of tensor products, we have

$$(M \otimes_A B) \otimes_B N \cong M \otimes_A (B \otimes_B N) \cong M \otimes_A N.$$

So, we can rewrite the above sequence as

$$0 \to M' \otimes_A N \to M \otimes_A N \to M'' \otimes_A N \to 0.$$

Since tensoring with N over A preserves the exactness of every short exact sequence of A-modules, N is flat as an A-module. □

Suppose M is an A-module and $\varphi : A \to B$ is a ring map, i.e. B is an A-algebra. Then, $M \otimes_A B$ is canonically a B-module, i.e.

$$b\left(\sum m_i \otimes b_i\right) = \sum m_i \otimes (bb_i).$$

This is compatible with the obvious A-module structure because

$$\varphi(a) \cdot \sum m_i \otimes n_i = \sum m_i \otimes \varphi(a) b_i = \sum am_i \otimes b_i = a\left(\sum m_i \otimes b_i\right).$$

Proposition 2.13. Fix $S \subseteq A$ and let M be an A-module. Then, there exists a canonical isomorphism of $S^{-1}A$ modules, i.e.

$$S^{-1}A \otimes_A M \cong S^{-1}M.$$

Proof. The map

$$S^{-1}A \times M \to S^{-1}M \quad \text{where} \quad \left(\frac{a}{s}, m\right) = \frac{am}{s}$$

is A-bilinear so it induces a unique A-module homomorphism as follows:

$$f : S^{-1}A \otimes_A M \to S^{-1}M \quad \text{where} \quad \sum \frac{a_i}{s_i} \otimes m_i \mapsto \sum \frac{a_i m_i}{s_i}$$

which is obviously surjective as

$$\frac{m}{s} = f\left(\frac{1}{s} \otimes m\right).$$

It suffices to prove that f is injective. Let

$$\sum \frac{a_i}{s_i} \otimes m_i \in S^{-1}A \otimes_A M \quad \text{be} \quad \text{an arbitrary element.}$$

Set

$$s = \prod s_i \quad \text{and} \quad t_i = \prod_{j \neq i} s_j.$$

Then,

$$\sum \frac{a_i}{s_i} \otimes m_i = \sum \frac{a_i t_i}{s} \otimes m_i = \sum \frac{1}{s} \otimes a_i t_i m_i = \frac{1}{s} \otimes \sum a_i t_i m_i.$$

Thus, all elements of $S^{-1}A \otimes_A M$ can be written in the form $\frac{1}{s} \otimes m$ where $m \in M$. Thus,

$$f\left(\frac{1}{s} \otimes m\right) = \frac{m}{s} = 0 \quad \text{implies} \quad \text{there exists some } t \in S \text{ such that } tm = 0.$$

But then

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

To summarise, $f\left(\frac{1}{s} \otimes m\right) = 0$ implies $\frac{1}{s} \otimes m = 0$, so f is injective. □

Proposition 2.14 (tensor-hom adjunction)**.** Let M, N, P be A-modules. Then,

$$\mathrm{Hom}_A(M \otimes_A N, P) \cong \mathrm{Hom}_A(M, \mathrm{Hom}_A(N, P)).$$

Proof. We have

$$\mathrm{Hom}_A(M \otimes_A N, P) = \mathrm{Bil}_A(M \times N, P).$$

This has the following canonical isomorphism:

$$\mathrm{Bil}_A(M \times N, P) \cong \mathrm{Hom}(M, \mathrm{Hom}_A(N, P)) \quad \text{where} \quad b \mapsto (M \to \mathrm{Hom}_A(N, P) \text{ where } m \mapsto b(m, \cdot))$$

To see this, observe that a bilinear map $b : M \times N \to P$ naturally induces a map $M \to \mathrm{Hom}_A(N, P)$ by sending $m \in M$ to the function $N \to P$ defined by $n \mapsto b(m, n)$. Since b is bilinear, then the map $M \to \mathrm{Hom}_A(N, P)$ is A-linear. Conversely, given a module homomorphism $f : M \to \mathrm{Hom}_A(N, P)$, define a bilinear map $b : M \times N \to P$ by setting $b(m, n) = f(m)(n)$. This is a bilinear map since f is linear in m and $f(m)$ is linear in n. □

Suppose $0 \to M' \to M \to M'' \to 0$ is exact and N is an A-module. Is $0 \to M' \otimes_A N \to M \otimes_A N \to M'' \otimes_A N$ still an exact sequence? The answer is no, in general, but we have something less strict as follows.

Proposition 2.15. If

$$M' \to M \to M'' \to 0 \text{ is exact} \quad \text{then} \quad M' \otimes N \to M \otimes N \to M'' \otimes N \to 0 \text{ is exact.}$$

In other words, the functor $- \otimes N$ is *right exact*.

To prove this, we need the following lemma:

Lemma 2.3. The following hold:

(i) A sequence $M' \to M \to M'' \to 0$ is exact if and only if for all A-modules P, the sequence

$$0 \to \mathrm{Hom}_A\left(M'', P\right) \to \mathrm{Hom}_A\left(M, P\right) \to \mathrm{Hom}_A\left(M', P\right) \text{ of Abelian groups of homomorphisms}$$

is exact

(ii) A sequence $0 \to M' \to M \to M''$ is exact if and only if for all A-modules P, the sequence

$$0 \to \mathrm{Hom}_A\left(P, M'\right) \to \mathrm{Hom}_A\left(P, M\right) \to \mathrm{Hom}_A\left(P, M''\right) \quad \text{is exact}$$

We now prove Proposition 2.15.

Proof. We can argue now as follows: Suppose $M' \to M \to M'' \to 0$ is exact. Since 0 is on the right, we use **(i)** of Lemma 2.3. We are going to use a *funny* choice of P, in particular, we see that the sequence

$$0 \to \mathrm{Hom}_A\left(M'', \mathrm{Hom}_A\left(N, P\right)\right) \to \mathrm{Hom}_A\left(M, \mathrm{Hom}_A\left(N, P\right)\right) \to \mathrm{Hom}_A\left(M', \mathrm{Hom}_A\left(N, P\right)\right)$$

is exact by **(i)** of Lemma 2.3. By the tensor-hom adjunction (Proposition 2.14) we get

$$0 \to \mathrm{Hom}_A\left(M'' \otimes_A N, P\right) \to \mathrm{Hom}_A\left(M \otimes_A N, P\right) \to \mathrm{Hom}_A\left(M' \otimes_A N, P\right).$$

Since this is exact for all P, using the reverse of the first part of Proposition 2.15, we get

$$0 \to M' \otimes_A N \to M \otimes_A N \to M'' \otimes_A N$$

which is exact. □

Example 2.21 (Atiyah and Macdonald p. 46 Question 19). Let A be a ring, M an A-module. The support of M is defined to be the set

$$\mathrm{Supp}(M) \text{ of prime ideals } \mathfrak{p} \text{ of } A \text{ such that } M_{\mathfrak{p}} \neq 0.$$

Prove the following results:

(i) $M \neq 0$ implies $\mathrm{Supp}(M) \neq \emptyset$

(ii) $V(a) = \mathrm{Supp}\left(A/a\right)$

(iii) If $0 \to M' \to M \to M'' \to 0$ is an exact sequence, then

$$\mathrm{Supp}\left(M\right) = \mathrm{Supp}\left(M'\right) \cup \mathrm{Supp}\left(M''\right)$$

(iv) If $M = \sum M_i$, then

$$\mathrm{Supp}\left(M\right) = \bigcup \mathrm{Supp}\left(M_i\right)$$

(v) If M is finitely generated, then

$$\operatorname{Supp}(M) = V(\operatorname{Ann}(M)) \quad \text{and} \quad \text{is therefore a closed subset of } \operatorname{Spec}(A)$$

(vi) If M, N are finitely generated, then

$$\operatorname{Supp}(M \otimes_A N) = \operatorname{Supp}(M) \cap \operatorname{Supp}(N)$$

(vii) If M is finitely generated and $\mathfrak{a}$ is an ideal of A, then

$$\operatorname{Supp}(M/\mathfrak{a}M) = V(\mathfrak{a} + \operatorname{Ann}(M))$$

(viii) If $f : A \to B$ is a ring homomorphism and M is a finitely generated A-module, then

$$\operatorname{Supp}(B \otimes_A M) = f^{-1}(\operatorname{Supp}(M))$$

Solution. First, recall that localizing at $\mathfrak{p}$ yields the module $M_\mathfrak{p} = S^{-1}M$, where $S = A \setminus \mathfrak{p}$, and localization is an exact functor.

(i) Suppose $M \neq 0$. Choose any non-zero element $m \in M$. Its annihilator, denoted by the set of all $a \in A$ such that $am = 0$, is a proper ideal of A. By Zorn's lemma, there exists a maximal ideal $\mathfrak{m}$ containing $\operatorname{Ann}(m)$. Localizing at $\mathfrak{m}$, note that $\frac{m}{1} \neq 0$ in $M_\mathfrak{m}$ because if it were zero, then some $s \notin \mathfrak{m}$ would satisfy $sm = 0$, implying $s \in \operatorname{Ann}(m) \subset \mathfrak{m}$, a contradiction. Hence, $M_\mathfrak{m} \neq 0$ and so $\mathfrak{m} \in \operatorname{Supp}(M)$.

(ii) Recall that the vanishing set V is defined to be

$$V(a) = \{\mathfrak{p} \in \operatorname{Spec}(A) : a \subseteq \mathfrak{p}\}.$$

For the A-module A/a, localizing at $\mathfrak{p}$ yields the isomorphism $(A/a)_\mathfrak{p} \cong A_\mathfrak{p}/aA_\mathfrak{p}$. This module is non-zero if and only if $aA_\mathfrak{p} \neq A_\mathfrak{p}$. But in a local ring $A_\mathfrak{p}$, the ideal $aA_\mathfrak{p}$ is proper if and only if $a \subseteq \mathfrak{p}$. Hence,

$$p \in \operatorname{Supp}(A/a) \quad \text{if and only if} \quad a \subseteq \mathfrak{p}$$

and the result follows.

(iii) If

$$0 \to M' \to M \to M'' \to 0 \quad \text{is exact,}$$

then we localize this sequence at a prime ideal $\mathfrak{p}$ to obtain

$$0 \to M'_\mathfrak{p} \to M_\mathfrak{p} \to M''_\mathfrak{p} \to 0.$$

Since localization is exact, then $M_\mathfrak{p} \neq 0$ if and only if at least one of $M'_\mathfrak{p}$ or $M''_\mathfrak{p}$ is non-zero. Thus,

$$\mathfrak{p} \in \operatorname{Supp}(M) \quad \text{if and only if} \quad \text{at least one of } M'_\mathfrak{p} \text{ or } M''_\mathfrak{p} \text{ is non-zero.}$$

Hence,

$$\mathfrak{p} \in \operatorname{Supp}(M) \quad \text{if and only if} \quad \mathfrak{p} \in \operatorname{Supp}(M') \text{ or } \mathfrak{p} \in \operatorname{Supp}(M'').$$

(iv) We localize at some prime ideal $\mathfrak{p}$ to obtain

$$M_\mathfrak{p} = \sum_i (M_i)_\mathfrak{p}.$$

Hence,

$$M_\mathfrak{p} \neq 0 \quad \text{if and only if} \quad \text{there is at least one } i \text{ such that } (M_i)_\mathfrak{p} \neq 0.$$

(v) First, note that if $\mathfrak{p} \in \operatorname{Supp}(M)$, then $M_{\mathfrak{p}} \neq 0$ and any $f \in \operatorname{Ann}(M)$ annihilates $M_{\mathfrak{p}}$. If $\operatorname{Ann}(M)$ was not contained in $\mathfrak{p}$, then there would exist an element $f \notin \mathfrak{p}$ which is invertible in $A_{\mathfrak{p}}$ and would force $M_{\mathfrak{p}} = 0$. Thus, $\operatorname{Ann}(M) \subseteq \mathfrak{p}$, so $\mathfrak{p} \in V(\operatorname{Ann}(M))$.

Conversely, assume $\mathfrak{p} \in V(\operatorname{Ann}(M))$ so that $\operatorname{Ann}(M) \subseteq \mathfrak{p}$. Since M is finitely generated, by Nakayama's lemma (Corollary 2.1), $M_{\mathfrak{p}} \neq 0$. Hence, $\mathfrak{p} \in \operatorname{Supp}(M)$. Since $V(\operatorname{Ann}(M))$ is a closed set in $\operatorname{Spec}(A)$, then the support is closed.

(vi) We localize at a prime ideal $\mathfrak{p}$. Then,

$$(M \otimes_A N)_{\mathfrak{p}} \cong M_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} N_{\mathfrak{p}}.$$

Since $A_{\mathfrak{p}}$ is a local ring and both $M_{\mathfrak{p}}, N_{\mathfrak{p}}$ are finitely generated, because the tensor product is non-zero if and only if both $M_{\mathfrak{p}}, N_{\mathfrak{p}}$ are non-zero, then

$$\mathfrak{p} \in \operatorname{Supp}(M \otimes_A N) \quad \text{if and only if} \quad \mathfrak{p} \in \operatorname{Supp}(M) \text{ and } \mathfrak{p} \in \operatorname{Supp}(N).$$

The result follows.

(vii) Note that $M/\mathfrak{a}M \cong M \otimes_A (A/\mathfrak{a})$. Hence,

$$\begin{aligned} \operatorname{Supp}(M/\mathfrak{a}M) &= \operatorname{Supp}(M \otimes_A (A/\mathfrak{a})) \\ &= \operatorname{Supp}(M) \cap \operatorname{Supp}(A/\mathfrak{a}) \quad \text{by } \textbf{(vi)} \\ &= V(\operatorname{Ann}(M)) \cap V(a) \\ &= V(a + \operatorname{Ann}(M)) \end{aligned}$$

Here we used the fact that for any two ideals I, J, $V(I) \cap V(J) = V(I+J)$[†].

(viii) For a prime ideal $\mathfrak{p} \in \operatorname{Spec}(A)$, one needs to check when the localization $(B \otimes_A M)_{\mathfrak{p}}$ is non-zero. One may verify that

$$(B \otimes_A M)_{\mathfrak{p}} \cong B_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} M_{\mathfrak{p}},$$

where $B_{\mathfrak{p}} = S^{-1}B$ with $S = A \setminus \mathfrak{p}$. The finitely generated hypothesis on M guarantees that

$$B_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} M_{\mathfrak{p}} \neq 0 \quad \text{if and only if} \quad M_{\mathfrak{p}} \neq 0.$$

On the other hand, when discussing $f^{-1}(\operatorname{Supp}(M))$, one interprets this as

$$f^{-1}(\operatorname{Supp}(M)) = \{\mathfrak{p} \in \operatorname{Spec}(A) : f(\mathfrak{p}) \in \operatorname{Supp}(M)\}.$$

Thus, a prime ideal $\mathfrak{p}$ of A belongs to the support of $B \otimes_A M$ if and only if the corresponding extension of $\mathfrak{p}$ (or its image under f) lies in the support of M. This gives the desired equality. □

Definition 2.10 (flat module). An A-module N is flat if $- \otimes_A N$ is exact. Equivalently, for every injective A-module map $M' \to M$, the induced map $M' \otimes N \to M \otimes N$ is still injective.

Since tensor products are always right exact (they preserve surjections), flatness is about ensuring that they also preserve injections (the left exactness part).

Example 2.22. Let A be a commutative ring and $S \subseteq A$ be a multiplicatively closed subset. Recall that the localizaion $S^{-1}A$ consists of elements of the form $\frac{a}{s}$, where $a \in A$ and $s \in S$. Here, the multiplication and addition

[†]Also encountered in MA4273.

operations are defined naturally.

$S^{-1}A$ is naturally an A-module via the action

$$a \cdot \frac{b}{s} = \frac{ab}{s} \quad \text{for all } a,b \in A, s \in S.$$

Next, for any A-module M, tensoring with $S^{-1}A$ defines a functor

$$M \mapsto M \otimes_A S^{-1}A.$$

By the universal property of localization, we have

$$M \otimes_A S^{-1}A \cong S^{-1}M.$$

The map $M \mapsto S^{-1}M$ is an exact functor, i.e. if we have an exact sequence of A-modules

$$0 \to M' \to M \to M'' \to 0,$$

then applying $S^{-1}(-)$ yields an exact sequence of localized modules as follows:

$$0 \to S^{-1}M' \to S^{-1}M \to S^{-1}M'' \to 0$$

since localization commutes with taking kernels and cokernels. As $- \otimes_A N$ is exact, then $- \otimes_A S^{-1}A$ is also exact, making $S^{-1}A$ a flat A-module.

Example 2.23. Let A be a ring. Suppose we are given ideals $I, J \subseteq A$. Then,

$$0 \to I \to A \to A/I \to 0 \quad \text{is exact.}$$

This is because $I \to A$ is the inclusion map which is injective, and $A \to A/I$ is the natural quotient map which is surjective. Also, the kernel of the quotient map is I, so the sequence is exact.

We then tensor this sequence with A/J, meaning we apply $- \otimes_A A/J$ to every term to obtain

$$I \otimes_A A/J \xrightarrow{\alpha} A/J \to A/I \otimes_A A/J \to 0 \quad \text{which is exact.}$$

To see why, for any element in $I \otimes_A A/J$, we have

$$\alpha\left(\sum i_j \otimes \overline{a}_j\right) = \sum \alpha\left(a_j i_j \otimes 1\right) = \sum \overline{a_j i_j}.$$

This means that elements in $I \otimes_A A/J$ get mapped to their products modulo J. $\operatorname{im}\alpha$ consists of all elements in A/J that come from sums of products of elements from I and arbitrary elements of A. A crucial observation by the second isomorphism theorem yields

$$\operatorname{im}\alpha = I/(I \cap J) \cong (I+J)/J.$$

Here, $\operatorname{coker}\alpha = A/(I+J)$. Thus, we obtain the new exact sequence

$$I \otimes_A A/J \to A/J \to A/(I+J) \to 0.$$

Note that if the sequence is exact at $I \otimes_A A/J$, then α is injective.

However, the sequence may not be flat! For example, let $A = \mathbb{Z}$, $I = (10)$ and $J = (5)$, so the sequence we

tensor is

$$0 \to (10) \to \mathbb{Z} \to \mathbb{Z}/10\mathbb{Z} \to 0.$$

Tensoring with $\mathbb{Z}/5\mathbb{Z}$, we obtain

$$(10) \otimes_{\mathbb{Z}} \mathbb{Z}/5\mathbb{Z} \xrightarrow{\alpha} \mathbb{Z}/5\mathbb{Z} \to \mathbb{Z}/5\mathbb{Z} \to 0.$$

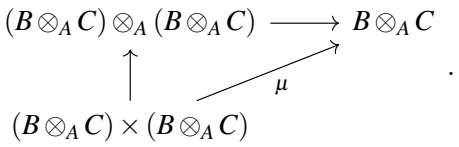
Here, $\operatorname{im}\alpha$ consists of elements of the form $10k \otimes \overline{1} \mapsto \overline{10k}$ in $\mathbb{Z}/5\mathbb{Z}$, which is in fact 0. Since every element in $(10) \otimes_{\mathbb{Z}} \mathbb{Z}/5$ is mapped to zero, then $\operatorname{im}\alpha = \{0\}$, so α is not injective, i.e. the sequence is not exact. This makes $\mathbb{Z}/5\mathbb{Z}$ not a flat $\mathbb{Z}$-module.

Suppose we are given ring homomorphisms $A \to B$ and $A \to C$. Then, $B \otimes_A C$ is canonically equipped with a ring structure and satisfies a universal property. To see why, we shall explicitly construct the tensor product. Consider the map

$$B \times C \times B \times C \to B \otimes_A C \quad \text{where} \quad (b, c, b', c') \mapsto bb' \otimes cc'.$$

This is a well-defined map of sets. Observe that this map is A-linear in each variable. We are going to spam some universal properties (of bilinear maps). We obtain the linear map

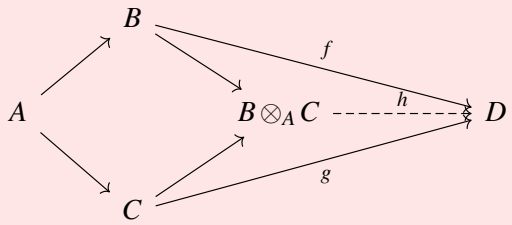
$(B \otimes_A C) \otimes_A (B \otimes_A C) \to B \otimes_A C$ such that the diagram commutes



.

Composing with the universal map from the universal property of tensors, we obtain the multiplication map.

Proposition 2.16 (universal property of pushout)**.** Given any commutative diagram of A-algebras



there exists a unique ring homomorphism $h : B \otimes_A C \to D$ making the above diagram commute.

The idea in Proposition 2.16 is that given f and g, we can consider the map

$$B \times C \to D \quad \text{where} \quad (b, c) \mapsto f(b)\, g(c)$$

This is well-defined and A-bilinear (since we are working with A-algebras), thus the universal property for bilinear maps yields the desired map $B \otimes_A C \to D$.

Example 2.24. Fix a ring A and consider ring homomorphisms $A \to B$ and $A \to A[X]$. Note that $B \otimes_A A[X] = B[X]$. Also, the following diagram commutes:

$$\begin{array}{ccc} A & \longrightarrow & B \\ \downarrow & & \downarrow \\ A[X] & \longrightarrow & B \otimes_A A[X] = B[X] \end{array}$$

To deduce this without excessive calculations, we can simply write

$$A[X] = \bigoplus_{n \in \mathbb{Z}_{\geq 0}} A$$

and use the fact that tensor products distribute across direct sums. Alternatively, we can use the universal property from before.

Example 2.25. Say we are interested in $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$. Recall from MA3201 that $\mathbb{C} = \mathbb{R}[X] / \left(X^2+1\right)$. Then by considering a previous result that $(A/J) \otimes_A B = B/JB$ (where JB is the ideal in B generated by the image of J), we let

$$A = \mathbb{R}[X] \quad \text{and} \quad J = \left(X^2+1\right) \quad \text{and} \quad B = \mathbb{C}.$$

Hence,

$$\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \cong \left(\mathbb{R}[X] \otimes_{\mathbb{R}} \mathbb{C} / \left(X^2+1\right)\right).$$

Since tensoring with $\mathbb{C}$ extends the scalars, we have

$$\mathbb{R}[X] \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{C}[X] \quad \text{which implies} \quad \mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{C}[X] / \left(X^2+1\right).$$

Over $\mathbb{C}$, the polynomial X^2+1 factors as

$$X^2+1 = (X+i)(X-i).$$

Since $(X+i)$ and $(X-i)$ are coprime in $\mathbb{C}[X]$, the Chinese remainder theorem tells us that

$$\mathbb{C}[X] / ((X+i)(X-i)) \cong \mathbb{C}[X] / (X+i) \times \mathbb{C}[X] / (X-i).$$

Evaluating each factor, we see that the quotient $\mathbb{C}[X] / (X+i)$ is isomorphic to $\mathbb{C}$ by the evaluation map $X \mapsto -i$. In a similar fashion, $\mathbb{C}[X] / (X-i)$ is isomorphic to $\mathbb{C}$ by the evaluation map $X \mapsto i$. Hence, we infer that

$$\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{C}$$

An explicit isomorphism is given by $a \times b \mapsto (\overline{a}b, ab)$. Here, the use of the complex conjugate $\overline{a}$ in the first component is a way to select one of the two embeddings of $\mathbb{C}$ into itself (corresponding to the two factors $\mathbb{C}[X] / (X+i)$ and $\mathbb{C}[X] / (X-i)$).

In fact, the same proof will work to prove that for any finite Galois extension E/F, we have $E \otimes_F E \cong E^{[E:F]}$.

Chapter 3
Some Classes of Rings

3.1
Noetherian Rings

Definition 3.1 (Noetherian ring)**.** Given a ring A, the following are equivalent:

(i) Every ascending chain of ideals $I_1 \subseteq I_2 \subseteq \dots$ stabilizes, i.e. $I_n = I_{n+1}$ for sufficiently large $n \in \mathbb{N}$

(ii) Every ideal $I \subseteq A$ is finitely generated as an A-module.

(iii) For any $N \subseteq M$ of A-modules, M is finitely generated implies N is finitely generated

If a ring satisfies any (thus all) of these conditions, we say that the ring is Noetherian.

We can also see Definition 3.1 as a proposition. We now provide a proof for it.

Proof. We first prove **(i)** implies **(ii)** by contraposition. Assume that $I \subseteq A$ is an ideal which is not finitely generated as an A-module. Then, we can pick generators $I = (a_1, a_2, ldots)$ such that $(a_1) \subset (a_1, a_2) \subseteq \dots$. This gives a chain $I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots$ that does not stabilize. Therefore **(i)** does not hold. As such, **(i)** implies **(ii)**.

We then prove **(ii)** implies **(iii)** by performing induction on the minimum number of generators of M. If M is generated by one element, then M is isomorphic to a quotient A/I of A for some ideal I. Then submodules of M are identified with ideals J of A that contain I. Since all ideals of A are finitely generated by assumption, J is finitely generated, whence $J/I \cong N$ is finitely generated.

For the induction hypothesis, suppose we are given an A-module M generated by $x_1, \dots x_n$. Let M' be a submodule generated by x_1, let $M'' = M/M'$. This yields a short exact sequence as follows:

$$0 \to M' \to M \to M'' \to 0$$

where since M' is generated by x_1, M'' must be generated by (the image in M'' of) $x_2, \dots, x_n$. Now we pick any submodule $N \subseteq M$. Then, we obtain the following diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 0 & \longrightarrow & N \cap M' & \longrightarrow & N & \longrightarrow & N/(N \cap M') & \longrightarrow & 0 \\ & & & & & & \| & & \\ & & & & & & (N+M')/M' & & \end{array}$$

Then, $N \cap M'$ is finitely generated by the base case (the case of modules generated by one element) and $N/N \cap M'$ is finitely generated by the induction hypothesis. So, N is also finitely generated by Example 2.7[†].

Lastly, we prove **(iii)** implies **(i)**. Say any submodule of a finitely generated A-module is finitely generated, then given any ascending chain of ideals $I_1 \subseteq I_2 \subseteq \dots$, the union

$$\bigcup_{n \in \mathbb{N}} I_n \subseteq A \quad \text{is} \quad \text{finitely generated as an } A\text{-module.}$$

[†]In Example 2.7, recall we proved that if the outer two modules are finitely generated, then the middle module is also finitely generated.

Thus,

$$\bigcup_{n\in\mathbb{N}} I_n = (x_1,\ldots,x_j) \quad \text{for some} \quad x_1,\ldots,x_n \in I_N,$$

where $N \in \mathbb{N}$ is sufficiently large. It follows that $I_n = I_{n+1}$ for all $n \geq N$. □

Example 3.1. $\mathbb{Z}$ is a Noetherian ring. To see why, consider any ideal $I \subseteq \mathbb{Z}$. If $I = \{0\}$, then $I = (0)$, which is generated by the single element 0. On the other hand, if $I \neq \{0\}$, then I contains non-zero elements.

Since I is a non-empty subset of $\mathbb{Z}$ and $\mathbb{N}$ satisfies the well-ordering principle, then there exists a smallest positive integer $d \in I$. One can show that $I = d\mathbb{Z}$ (show both inclusions; the forward inclusion is slightly more interesting as it uses the division algorithm). To conclude, every ideal in $\mathbb{Z}$ is generated by a single element, i.e. every ideal is finitely generated.

Example 3.2. Any field F is a Noetherian ring. We consider any ideal $I \subseteq F$. If I is the zero ideal, then the result follows (similar to Example 3.1). On the other hand, if $I \neq \{0\}$, then there exists some non-zero element $a \in I$. Since F is a field, then a^{-1} exists and it satisfies $1 = a^{-1}a \in I$. Once $1 \in I$, for any $x \in F$, we have $x = x \cdot 1 \in I$, so $I = F$. Since the ideal I is generated by a single element, then F is finitely generated, so it is a Noetherian ring.

Example 3.3. $\mathbb{C}[z]$ is a Noetherian ring. Any polynomial ring in one variable over a field is a principal ideal domain (recall from MA3201). This means that every ideal in $\mathbb{C}[z]$ is generated by a single polynomial. The result follows by **(ii)** of Definition 3.1.

Example 3.4 (Atiyah and Macdonald p. 84 Question 4)**.** Which of the following rings are Noetherian?

(i) The ring of rational functions of z having no pole on the circle $|z| = 1$
(ii) The ring of power series in z with a positive radius of convergence
(iii) The ring of power series in z with an infinite radius of convergence
(iv) The ring of polynomials in z whose first k derivatives vanish at the origin (k being a fixed integer)
(v) The ring of polynomials in z, w all of whose partial derivatives with respect to w vanish for $z = 0$

In all cases, the coefficients are complex numbers.

Solution.

(i) This ring is isomorphic to the ring of rational functions $\mathbb{C}(t)$, hence it is not Noetherian.
(ii) This set is not even a ring as it does not contain the zero power series.
(iii) This ring is isomorphic to the ring of all rational functions $\mathbb{C}(t)$, hence it is not Noetherian.
(iv) This ring is isomorphic to $\mathbb{C}[z]$, hence it is Noetherian.
(v) This ring is isomorphic to $\mathbb{C}[z,w]$, hence it is Noetherian. □

Proposition 3.1. If A is a Noetherian ring and $I \subseteq A$ is an ideal, then A/I is Noetherian.

Proof. Define the canonical surjective ring homomorphism

$$\pi : A \to A/I \quad \text{where} \quad \pi(a) = a + I.$$

Let J be an ideal in A/I. Consider its preimage under π, which is $\pi^{-1}(J) = \{a \in A : a + I \in J\}$. Since π is a ring homomorphism, then $\pi^{-1}(J)$ is an ideal in A.

As A is Noetherian, then every ideal in A is finitely generated. So, there exists $a_1,\ldots,a_n \in A$ such that $\pi^{-1}(J) = (a_1,\ldots,a_n)$. We claim that

$$J = (\pi(a_1),\ldots,\pi(a_n)).$$

We first prove the reverse inclusion. Note that because each $a_i \in \pi^{-1}(J)$, then $\pi(a_i) \in J$ for all i. So, any linear combination of the $\pi(a_i)$'s with coefficients from A/I lies in J. For the forward inclusion, note that for any $j \in J$, there exists $a \in A$ such that $\pi(a) = j$. Since $a = \pi^{-1}(J) = (a_1, \ldots, a_n)$, then there exist $r_1, \ldots, r_n \in A$ such that

$$a = r_1 a_1 + \ldots + r_n a_n.$$

Applying π to both sides yields

$$j = \pi(a) = \pi(r_1)\pi(a_1) + \ldots + \pi(r_n)\pi(a_n)$$

Thus, j is in the ideal generated by $\pi(a_1), \ldots, \pi(a_n)$. Since every ideal J in A/I is generated by finitely many elements, then quotient ring A/I is Noetherian. □

Proposition 3.2. If A is Noetherian and $S \subseteq A$ is multiplicatively closed, then $S^{-1}A$ is Noetherian.

Proof. In the localization process, every ideal $I \subseteq S^{-1}A$ is the extension of some ideal $I' \subseteq A$. This means that there is an ideal

$$I' = \left\{ a \in A : \frac{a}{1} \in I \right\} \quad \text{such that} \quad I = I'\left(S^{-1}A\right) = \left\{ \frac{a}{s} : a \in I', s \in S \right\}.$$

Since A is Noetherian, the ideal I' is finitely generated. That is, there exist elements $x_1, x_2, \ldots, x_n \in A$ such that $I' = (x_1, x_2, \ldots, x_n)$. When we extend I' to $S^{-1}A$, the generators $x_1, x_2, \ldots, x_n$ give rise to the elements

$$\frac{x_1}{1}, \frac{x_2}{1}, \ldots, \frac{x_n}{1} \quad \text{in } S^{-1}A.$$

One can show that these elements generate the ideal I in $S^{-1}A$. In other words,

$$I = \left(\frac{x_1}{1}, \frac{x_2}{1}, \ldots, \frac{x_n}{1} \right).$$

Any element of I can be written as a combination of these generators with coefficients from $S^{-1}A$. Since every ideal I in $S^{-1}A$ can be generated by finitely many elements (namely, the images of the finitely many generators of its corresponding ideal I' in A), the localized ring $S^{-1}A$ is Noetherian. □

Theorem 3.1 (Hilbert basis theorem)**.** If A is a Noetherian ring, then $A[X]$ is also Noetherian.

Proof. See my MA4273 notes. □

We will see in Example 3.5 that the converse of the Hilbert basis theorem (Theorem 3.1) also holds.

Corollary 3.1. If A is Noetherian, then $A[X_1, \ldots, X_n]$ is also Noetherian.

Example 3.5 (Atiyah and Macdonald p. 85 Question 8)**.** If $A[x]$ is Noetherian, is A necessarily Noetherian?

Solution. We claim that A is also Noetherian. Let

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \ldots \subseteq \mathfrak{a}_n \subseteq \ldots \quad \text{be} \quad \text{any ascending chain of ideals in } A.$$

This induces an ascending chain

$$\mathfrak{a}_1[x] \subseteq \mathfrak{a}_2[x] \subseteq \ldots \mathfrak{a}_n[x] \subseteq \ldots \quad \text{in } A[x].$$

Since $A[x]$ is Noetherian, then this chain stabilises, i.e. there exists $n \in \mathbb{N}$ sufficiently large such that $\mathfrak{a}_n[x] = \mathfrak{a}_{n+1}[x] = \ldots$. Now, assume for the sake of contradiction that the chain in A does not stabilize at n, i.e. there exists $y \in \mathfrak{a}_{n+1}$ such that $y \notin \mathfrak{a}_n$. Since $y \in A$, we can view it as a constant polynomial in $A[x]$. Thus, $y \in \mathfrak{a}_{n+1}[x]$. However, because the chain of polynomial ideals has stabilised, we have $\mathfrak{a}_{n+1}[x] = \mathfrak{a}_n[x]$, so $y \in \mathfrak{a}_n[x]$.

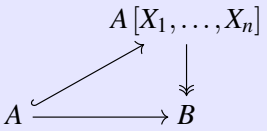
However, any polynomial in $\mathfrak{a}_n[x]$ is of the form

$$f(x) = a_0 + a_1 x + \ldots + a_m x^m \quad \text{where each coefficient } a_i \in \mathfrak{a}_n.$$

In particular, since y is a constant polynomial, it can only be represented as $y = a_0$, so $y \in \mathfrak{a}_n$, which is a contradiction because we assumed $y \notin \mathfrak{a}_n$. So, A is Noetherian. □

Definition 3.2 (finitely generated and finitely presented algebras)**.** Fix a ring A. Let B be an A-algebra. Then, B is *finitely generated* (or of *finite type*) as an A-algebra if and only if there exist ring homomorphisms such that the following diagram commutes, i.e. there exists

$$\text{an isomorphism } B \cong A[X_1, \ldots, X_n]/I \quad \text{for some ideal } I \text{ of } A[X_1, \ldots, X_n].$$



Moreover, if there exists such a diagram where I is finitely generated as a $A[X_1, \cdots, X_n]$-module, then we say that B is a *finitely presented* A-algebra.

Proposition 3.3. If A is Noetherian, then any finitely generated A-algebra B is Noetherian and finitely presented.

3.2 Dimension Theory

Definition 3.3 (height of prime ideal)**.** Given a prime ideal of a ring $\mathfrak{p} \subseteq A$, define

$$\operatorname{ht}(\mathfrak{p}) = \sup\{n : \text{there exists a chain } \mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n = \mathfrak{p}\}$$

to be the height of $\mathfrak{p}$.

Definition 3.4 (Krull dimension)**.** Given a prime ideal of a ring $\mathfrak{p} \subseteq A$, define

$$\dim(A) = \sup_{\mathfrak{p}} \operatorname{ht}(\mathfrak{p}) = \sup\{n : \text{there exists a chain } \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_n\}.$$

Example 3.6 (Krull dimension of a field)**.** For any field k, we have $\dim(k) = 0$. This is easy to see — the only prime ideals of k are itself and the zero ideal (0). However, k is not a proper ideal of itself. As the longest possible chain of prime ideals is (0), and there are no prime ideals strictly contained in (0) and no proper prime ideals strictly containing (0), the longest chain of prime ideals has length 0.

Example 3.7 (Krull dimension of $\mathbb{Z}$)**.** In $\mathbb{Z}$, the prime ideals are exactly (0) and (p) for each prime p. As such, $(0) \subset (p)$ is a non-trivial chain of prime ideal, which is of length 1. So, $\dim(\mathbb{Z}) = 1$.

Also, recall that the height of a prime ideal $\mathfrak{p}$ is the supremum of the lengths of all chains of prime ideals ending at $\mathfrak{p}$. For any prime p, the only chain is $(0) \subset (p)$, so $\operatorname{ht}((p)) = 1$.

Example 3.8 (Krull dimension of polynomial ring)**.** For any field k, we have $\dim(k[X_1,\ldots,X_n]) \geq n$. To see why, consider the chain

$$0 \subseteq (X_1) \subseteq (X_1,X_2) \subseteq \ldots \subseteq (X_1,X_2,\ldots,X_n).$$

The zero ideal 0 is prime because $k[X_1,\ldots,X_n]$ is an integral domain. Also, for each $1 \leq i \leq n$, the ideal $(X_1,\ldots,X_i)$ is prime because

$$k[X_1,\ldots,X_n]/(X_1,\ldots,X_i) \cong k[X_{i+1},\ldots,X_n] \quad \text{which is an integral domain.}$$

Each inclusion in the chain is proper. For example, (X_1) is strictly contained in (X_1,X_2) because X_2 is not an element of (X_1). This continues for the successive ideals, ensuring that the chain is strictly increasing. As the chain consists of $n+1$ ideals (starting at 0 and ending at $(X_1,X_2,\ldots,X_n)$), the length of a chain is the number of strict inclusions, which here is n. The result follows.

Theorem 3.2. If A is Noetherian, then $\dim(A[X]) = \dim(A)+1$.

Even if A is a Noetherian ring, its Krull dimension can still be infinite. An example of a Noetherian ring with infinite Krull dimension was constructed by Nagata in the 1950s. For the interested reader, please refer to Exercise 9.6 of 'Commutative Algebra' by D. Eisenbud.

Proposition 3.4. $\operatorname{ht}(\mathfrak{p}) = \dim(A_{\mathfrak{p}})$

Theorem 3.3. $\dim(A_{\mathfrak{p}})$ is finite for any Noetherian ring.

Remark 3.1. $\operatorname{ht}(\mathfrak{p}) = \dim(A_{\mathfrak{p}})$.

Theorem 3.4. $\dim(A_{\mathfrak{p}})$ is finite for any Noetherian ring.

Here is a fun fact: suppose that A is not Noetherian but $\dim A$ is finite. Then $\dim(A)+1 \leq \dim(A[X]) \leq 2\dim(A)$, and there exist examples exhibiting every possibility in this range.

3.3 Integral Dependence and Integral Rings

Definition 3.5. Suppose $A \subseteq B$. An element $x \in B$ is said to be *integral* over A if x satisfies some monic polynomial with coefficients in A, i.e. if

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 = 0 \quad \text{for some } a_0,\ldots,a_{n-1} \in A.$$

Example 3.9. If $A = \mathbb{Z}$ and $B = \mathbb{Q}$, then the set of elements in $\mathbb{Q}$ integral over $\mathbb{Z}$ is just $\mathbb{Z}$.

Example 3.10 (Atiyah and Macdonald p. 67 Question 5)**.** Let $A \subseteq B$ be rings, B integral over A.

(i) If $x \in A$ is a unit in B, then it is a unit in A.

(ii) The Jacobson radical of A is the contraction of the Jacobson radical of B.

Solution.

(i) Assume $x \in A$ is a unit in B. Then, there exists $u \in B$ such that $xu = 1$. Since B is integral over A, every element of B satisfies a monic polynomial with coefficients in A. In particular, the inverse u satisfies an equation of the form

$$u^n + a_{n-1}u^{n-1} + \ldots + a_1 u + a_0 = 0 \quad \text{where } a_i \in A.$$

We multiply the entire equation by x^{n-1}. As $x \in A$ and the coefficients $a_i \in A$, then the product stays within A. Also, note that because $xu = 1$, then $u = x^{-1}$ so $u^k x^k = \left(x^{-1}\right)^k x^k = \left(x^k\right)^{-1} x^k = 1$ for any exponent k. In particular,

$$u = -\left(a_{n-1} + a_{n-2}x + \ldots + a_0 x^{n-1}\right).$$

The RHS is in A because it is a sum of product of elements from A. So, $u \in A$ so x has an inverse in A. We conclude that x is a unit in A.

(ii) Recall that for any ring, the Jacobson radical is defined to be the intersection of the maximal ideals of the ring. Equivalently, by Proposition 1.18, for any ring R,

$$J(R) \quad \text{consists of} \quad \text{elements } r \in R \text{ for which } 1 - ry \text{ is a unit for every } y \in R.$$

Let $x \in A$. We claim that

$$x \in J(A) \quad \text{if and only if} \quad \begin{array}{l}\text{for every maximal ideal } \mathfrak{m}' \text{ of } B \text{ whose contraction} \\ \text{is a maximal ideal of } A \text{ we have } x \in \mathfrak{m}'\end{array}$$

By contraction, we mean that for any maximal ideal $\mathfrak{a} \in A$, we have $\mathfrak{m}' \cap A = \mathfrak{m}$. To see why, there exists a maximal ideal $\mathfrak{m}' \in B$ with $\mathfrak{m}' \cap A = \mathfrak{m}$. If x is in every maximal ideal fo B, i.e. $x \in J(B)$, then $x \in \mathfrak{m}'$ so $x \in \mathfrak{m}$. Hence,

$$J(B) \cap A \subseteq J(A).$$

Conversely, if $x \in J(A)$, then for every maximal ideal $\mathfrak{m}$ of A, we have $x \in \mathfrak{m}$. Since every maximal ideal $\mathfrak{m}'$ of B contracts to some maximal ideal $\mathfrak{m}$ of A, then x must belong to every maximal ideal $\mathfrak{m}'$ of B. Hence, $x \in J(B)$, so

$$J(A) \subseteq J(B) \cap A.$$

Thereafter, combining both facts yields the desired result. □

Definition 3.6. A module M is *faithful* if and only if $\operatorname{Ann}(M) = 0$, i.e. $R \to \operatorname{Hom}_R(M, M)$ is injective.

Example 3.11. $\mathbb{Z}$ is a faithful $\mathbb{Z}$-module. To see why, note that

$$\operatorname{Ann}(\mathbb{Z}) = \{n \in \mathbb{Z} : n\mathbb{Z} = 0\},$$

which forces $n = 0$, so $\operatorname{Ann}(\mathbb{Z}) = 0$.

Example 3.12 (Atiyah and Macdonald p. 85 Question 12)**.** Let A be a ring and B a faithfully flat A-algebra. If B is Noetherian, show that A is Noetherian.
Hint: Use the ascending chain condition.

Solution. Let

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots \quad \text{be} \quad \text{an ascending chain of ideals in } A.$$

We wish to show that this chain stabilises, which is equivalent to A being Noetherian. Since B is a flat A-algebra, tensoring preserves injections and exact sequences. Thus, when we tensor the chain with B, we obtain

an ascending chain of ideals in B, i.e.

$$I_1B \subseteq I_2B \subseteq I_3B \subseteq \dots.$$

Because B is Noetherian, every ascending chain of ideals in B must eventually stabilise. That is, there exists $N \in \mathbb{N}$ such that

$$I_NB = I_{N+1}B = I_{N+2}B = \dots.$$

Recall that a module M over A is zero if and only if $M \otimes_A B$ is zero when B is faithfully flat over A. Now, consider the quotient I_{N+1}/I_N. Tensoring with B gives

$$(I_{N+1}/I_N) \otimes_A B \cong I_{N+1}B/I_NB.$$

Since $I_{N+1}B = I_NB$, it follows that

$$I_{N+1}B/I_NB = 0.$$

Faithful flatness implies that

$$(I_{N+1}/I_N) \otimes_A B = 0 \quad \text{so} \quad I_{N+1}/I_N = 0.$$

This means that $I_{N+1} = I_N$. Since the chain of ideals in A stabilises at I_N, A satisfies the ascending chain condition. Therefore, A is Noetherian. □

Note that $A[x]$ is not a polynomial ring, but rather the submodule of B generated by A-multiples of powers of x. Thus $A[x]$ consists of elements of B of the form

$$\sum_i a_i x^i.$$

Proposition 3.5. Fix $A \subseteq B$. Then, fix $x \in B$. The following are equivalent:

- **(i)** x is integral over A
- **(ii)** $A[x]$ is a finitely generated A-module
- **(iii)** There exists a finitely generated B-module C such that $A[x] \subseteq C \subseteq B$
- **(iv)** There exists a faithful $A[x]$-module M which is finitely generated as an A-module

Proof. **(i)** implies **(ii)** is trivial. To see why, if x satisfies $x^n + a_{n-1}x^{n-1} + \dots + a_0 = 0$, then $A[x]$ is generated by $1, x, x^2, \dots, x^{n-1}$ since all combinations of powers of x greater than $n-1$ can be reduced to lower terms by the relation.

(ii) implies **(iii)** by taking $C = A[x]$; **(iii)** implies **(iv)** by taking $M = C$.

Lastly, to prove **(iv)** implies **(i)**, suppose we are given a finitely generated A-module M equipped with a faithful action by the elements of $A[x]$. Consider the A-module endomorphism $\phi : M \to M$ where $m \mapsto xm$. By applying the useless version of Nakayama's lemma (Proposition 2.2) to the whole ring $R = J = A$ and $M = N$, and ϕ as defined previously, we then get, as an A-module endomorphism on M,

$$x^n + a_{n-1}x^{n-1} + \dots + a_0 = 0$$

Since M is a faithful $A[x]$-module, then $A[x] \hookrightarrow \mathrm{Hom}_A(M, M)$ is injective, so that $x^n + a^{n-1}x^{n-1} + \dots + a_0 = 0$ in $A[x]$. The result follows. □

Corollary 3.2. Given $A \subseteq B$ and $x_1, \ldots, x_n \in B$ each integral over A, then $A[x_1, \ldots, x_n] \subseteq B$ is a finitely generated A-module.

Definition 3.7. Let $f : A \to B$ be a ring homomorphism. We say that it is *integral* if and only if $f(A) \subseteq B$ is an integral ring extension, i.e. B is an integral ring extension of $f(A)$.

Proposition 3.6 (transitivty of integral ring extension)**.** Given $A \subseteq B \subseteq C$ are ring extensions, and $A \subseteq B$ and $B \subseteq C$ are integral ring extensions, then $A \subseteq C$ is an integral ring extension.

Proof. Pick $x \in C$. Then, there exists an equation

$$x^n + b_1 x^{n-1} + \cdots + b_n = 0 \quad \text{where } b_i \in B.$$

Since B is integral over A, then $B' = A[b_1, \ldots, b_n] \subseteq C$ is a finitely generated A-module. So, $B'[x]$ is also a finitely generated B'-module, so it is finitely generated as an A-module. Thus $A[x] \subseteq B'[x] \subseteq C$ with $B'[x]$ finitely generated as an A-module. To complete the proof, recall that **(iii)** implies **(i)** in Proposition 3.5. □

Corollary 3.3. Let $A \subseteq B$ be a ring extension and C be the integral closure of A in B. Then, C is also intgerally closed in B.

Proof. If $x \in B$ is integral over C, then $A \subseteq C \subseteq C[x]$ are integral ring extensions. So, $A \subseteq C[x]$ is an integral ring extension. So, x is integral over A. We conclude that $x \in C$. □

Proposition 3.7. Let $A \subseteq B$ be an integral ring extension. Then, the following hold:

(i) Let $J \subseteq B$ be an ideal. Then,

$$A/(J \cap A) = B/J \quad \text{is} \quad \text{an integral ring extension.}$$

(ii) Let $S \subseteq A$ be a multiplicatively closed subset. Then,

$$S^{-1}A \subseteq S^{-1}B \quad \text{is} \quad \text{an integral ring extension.}$$

Proof. For **(i)**, suppose we are given $b \in B/J$ and a lift $\widetilde{b} \in B$. Note that $\widetilde{b}$ satisfies

$$\widetilde{b}^n + a_1 \widetilde{b}^{n-1} + \ldots + a_n = 0 \quad \text{where } a_i \in A.$$

Then, modulo $J \cap A$, we obtain

$$b^n + \overline{a_1} b^{n-1} + \ldots + \overline{a_n} = 0 \quad \text{where } \overline{a_i} \in A/(J \cap A).$$

This proves **(i)**. As for **(ii)**, pick any $\frac{x}{s} \in S^{-1}B$. Then, we can pick

$$x^n + a_1 x^{n-1} + \ldots + a_n = 0 \quad \text{in } B.$$

As such, we obtain

$$\frac{x^n}{s^n} + \frac{a_1}{s} \cdot \frac{x^{n-1}}{s^{n-1}} + \ldots + \frac{a_n}{s^n} = 0 \quad \text{in } S^{-1}B.$$

Thus, $t = \frac{x}{s}$ is a root of the polynomial equation

$$t^n + \frac{a_1}{s} t^{n-1} + \ldots + \frac{a_n}{s^n} = 0,$$

which proves **(ii)**. □

Proposition 3.8. Let $A \subseteq B$ be an integral ring extension with both rings being integral domains. Then,

$$A \text{ is a field} \quad \text{if and only if} \quad B \text{ is a field.}$$

Proof. We first prove the forward direction. Suppose A is a field. Let $0 \neq x \in B$ be an element. Then, there exists an equation

$$x^n + a_1 x^{n-1} + \ldots + a_{n-1}x + a_n = 0 \quad \text{where } a_i \in A.$$

Note that $a_n \neq 0$ since A is an integral domain. Then,

$$y = -a_n^{-1}\left(x^{n-1} + a_1 x^{n-2} + \ldots + a_{n-1}\right) \text{ in } B \quad \text{satisfies the equation } xy = 1.$$

As such, B is a field.

For the reverse direction, suppose B is a field. Choose $0 \neq x \in A$. Then, $x^{-1} \in B$ is integral over A so we obtain the equation

$$x^{-n} + a_1 x^{-n+1} + \ldots + a_n = 0 \quad \text{where } a_i \in A.$$

Then,

$$x^{-1} = -\left(a_1 + a_2 x + a_3 x^2 + \ldots + a_n x^{n-1}\right) \in A.$$

This implies that $x^{-1} \in A$, so A is a field. □

Corollary 3.4. Let $A \subseteq B$ be an integral ring extension and $\mathfrak{q} \subseteq B$ be a prime ideal. Let $\mathfrak{p} = A \cap \mathfrak{q}$ be its contraction. Then,

$$\mathfrak{q} \text{ is maximal} \quad \text{if and only if} \quad \mathfrak{p} \text{ is a field.}$$

Proof. Note that $A/\mathfrak{p} \subseteq B/\mathfrak{q}$ is an integral ring extension, where A and B are integral domains. Recall that

$$\mathfrak{p} \text{ is a maximal ideal} \quad \text{if and only if} \quad A/\mathfrak{p} \text{ is a field.}$$

Hence, this is equivalent to saying that $B/\mathfrak{q}$ is a field and $\mathfrak{q}$ is a maximal ideal. □

Proposition 3.9. Let $A \subseteq B$ be an integral ring extension. Suppose we are given

$$\mathfrak{q} \subseteq \mathfrak{q}' \subseteq B \text{ as prime ideals} \quad \text{such that} \quad \mathfrak{q} \cap A = \mathfrak{q}' \cap A = \mathfrak{p}.$$

Then, $\mathfrak{q} = \mathfrak{q}'$.

Proof. It is clear that $\mathfrak{q}$ and $\mathfrak{q}'$ both contain the extension of $\mathfrak{p}$. Set $A_\mathfrak{p}$ as usual and $B_\mathfrak{p} = (A \setminus \mathfrak{p})^{-1} B$. So, $A_\mathfrak{p} \subseteq B_\mathfrak{p}$ is an integral ring extension. Let $\mathfrak{m} = \mathfrak{p}A_\mathfrak{p}$, and $\mathfrak{n} = \mathfrak{q}B_\mathfrak{p}$, $\mathfrak{n}' = \mathfrak{q}'B_\mathfrak{p}$.

By construction, $\mathfrak{n}$ and $\mathfrak{n}'$ contract to $\mathfrak{q}$ and $\mathfrak{q}'$ respectively in B. But contracting $\mathfrak{n}$ and $\mathfrak{n}'$ in $A_\mathfrak{p}$ yields $\mathfrak{m}$, and $A_\mathfrak{p} \subseteq B_\mathfrak{p}$ is integral, so $\mathfrak{n} \subseteq \mathfrak{n}'$ are both maximal. □

Theorem 3.5. Let $A \subset B$ be an integral ring extension and let $\mathfrak{p} \subseteq A$ be a prime ideal. Then there exists a prime ideal $\mathfrak{q} \subseteq B$ with $A \cap \mathfrak{q} = \mathfrak{p}$. In other words, there exists a surjective map $\operatorname{Spec}(B) \to \operatorname{Spec}(A)$ (given by contraction).

Proof. Consider the following diagram of ring homomorphisms:

$$\begin{array}{ccc} A & \hookrightarrow & B \\ \downarrow & & \downarrow \\ A_{\mathfrak{p}} & \hookrightarrow & B_{\mathfrak{p}} \end{array}$$

Here, the horizontal arrows are integral extensions. Pick any maximal ideal $\mathfrak{n}$ in $B_{\mathfrak{p}}$. Then $\mathfrak{n} \cap A_{\mathfrak{p}}$ is maximal in the local ring $A_{\mathfrak{p}}$, so $n \cap A_{\mathfrak{p}} = \mathfrak{p}A_{\mathfrak{p}}$. Thus, $\mathfrak{n} \cap A = \mathfrak{p}$ (this is contracted into A). Then $\mathfrak{q} := \mathfrak{n} \cap B$ is prime and $\mathfrak{q} \cap A = \mathfrak{p}$, as desired. □

We then discuss a *funny theorem* known as the *going up theorem*. This is also known as the Cohen–Seidenberg theorem.

Theorem 3.6 (Cohen–Seidenberg theorem, going up)**.** Let $A \subseteq B$ be an integral ring extension and

$$\begin{aligned} \mathfrak{p}_1 \subseteq \mathfrak{p}_2 \subseteq \ldots \mathfrak{p}_n \quad &\text{be} \quad \text{a chain of prime ideals in } A \\ \mathfrak{q}_1 \subseteq \mathfrak{q}_2 \subseteq \ldots \subseteq \mathfrak{q}_m \quad &\text{be} \quad \text{a chain of prime ideals in } B \end{aligned}$$

where $m \leq n$ such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ for all $1 \leq i \leq m$. Then, we can extend the chain to $\mathfrak{q}_1 \subseteq \ldots \subseteq \mathfrak{q}_n$ such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ for all $1 \leq i \leq n$.

Proof. It suffices to consider where we can lengthen the chain of $\mathfrak{q}$'s one step at a time. This reduces to the case $n = 2$ and $m = 1$.

Set $\overline{A} = A/\mathfrak{p}_1 \subseteq \overline{B} = B/\mathfrak{q}$. This is an integral ring extension. Since $\mathfrak{p}_2$ contains $\mathfrak{p}_1$, $\overline{\mathfrak{p}}_2 = \mathfrak{p}_2/\mathfrak{p}_1 \subseteq \overline{A}$ is a prime ideal, and thus there exists $\mathfrak{q}' \subseteq \overline{B}$ with $\mathfrak{p}' \cap \overline{A} = \overline{\mathfrak{p}}_2$. Then, $\mathfrak{q}_2$, defined as the preimage of $\mathfrak{q}'$ along $B \twoheadrightarrow \overline{B}$, has the desired property. □

Corollary 3.5. If $A \subseteq B$ is an integral ring extension, then $\dim A \leq \dim B$.

Proof. This is immediate from the going up theorem (Theorem 3.6) since given any chain of prime ideals in A, we can find a corresponding chain of prime ideals in B that is at least as long. □

Theorem 3.7 (Cohen–Seidenberg theorem, going down)**.** Let $A \subseteq B$ be an integral ring extension and

$$\begin{aligned} \mathfrak{p}_1 \supseteq \mathfrak{p}_2 \supseteq \ldots \mathfrak{p}_n \quad &\text{be} \quad \text{a chain of prime ideals in } A \\ \mathfrak{q}_1 \supseteq \mathfrak{q}_2 \supseteq \ldots \supseteq \mathfrak{q}_m \quad &\text{be} \quad \text{a chain of prime ideals in } B \end{aligned}$$

where $m \leq n$ such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ for all $1 \leq i \leq m$. Then, we can extend the chain to $\mathfrak{q}_1 \supseteq \ldots \supseteq \mathfrak{q}_n$ such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ for all $1 \leq i \leq n$.

Proposition 3.10. Suppose we are given a ring extension $A \subseteq B$ (not necessarily integral), and C is the integral closure of A in B. Let $S \subseteq A$ be any multiplicatively closed subset. Then,

$$S^{-1}C \quad \text{is} \quad \text{the integral closure of } S^{-1}A \text{ in } S^{-1}B.$$

Proof. We already know that $S^{-1}C$ is integral over $S^{-1}A$. Now, suppose $\frac{b}{s} \in S^{-1}B$ is integral over $S^{-1}A$, i.e. there exists an equation:

$$\left(\frac{b}{s}\right)^n + \frac{a_1}{s_1}\left(\frac{b}{s}\right)^{n-1} + \ldots + \frac{a_n}{s_n} = 0$$

with $\frac{a_i}{s_i} \in S^{-1}A$. Set $t = s_1 \dots s_n$ and multiply the previous equation by $(st)^n$. After some rearrangement, we see that $bt \in B$ is integral over A, so $\frac{b}{s} = \frac{bt}{st} \in S^{-1}C$. □

Definition 3.8 (field of fractions). Let A be an integral domain. Then,

$$\mathrm{Frac}\,(A) = (A \setminus \{0\})^{-1} A \quad \text{is a field.}$$

We call this the field of fractions of A.

Definition 3.9 (integrally closed domain). A domain A is said to be an integrally closed domain if A is integrally closed in $\mathrm{Frac}\,(A)$.

Example 3.13. $\mathbb{Z}$ is an integrally closed domain. Note that the field of fractions of $\mathbb{Z}$ is $\mathbb{Q}$. To see why $\mathbb{Z}$ is integrally closed, we must prove that if every $x \in \mathbb{Q}$ satisfies a monic polynomial with integer coefficients, then $x \in \mathbb{Z}$. The proof is simple so we shall omit it.

Example 3.14. We claim that $\mathbb{Z}\left(\sqrt{5}\right)$ not an integrally closed domain. First, note that the field of fractions of $\mathbb{Z}\left(\sqrt{5}\right)$ is $\mathbb{Q}\left(\sqrt{5}\right)$, which consists of all numbers of the form

$$\frac{a+b\sqrt{5}}{c} \quad \text{with } a,b,c \in \mathbb{Z} \text{ and } c \neq 0.$$

Consider the element

$$\alpha = \frac{1+\sqrt{5}}{2} \quad \text{which lies in } \mathbb{Q}\left(\sqrt{5}\right).$$

α satisfies the monic polynomial $x^2 - x - 1 = 0$. Since the coefficients of x and the constant term, which are -1 and -1 respectively, are in $\mathbb{Z}$ (and hence in $\mathbb{Z}\left(\sqrt{5}\right)$), then α is integral over $\mathbb{Z}\left(\sqrt{5}\right)$. However, α is not in $\mathbb{Z}\left(\sqrt{5}\right)$. Note that $\mathbb{Z}\left(\sqrt{5}\right)$ consists of all numbers of the form

$$a+b\sqrt{5} \quad \text{where } a,b \in \mathbb{Z}.$$

If $\alpha \in \mathbb{Z}\left(\sqrt{5}\right)$, then we would be able to write

$$\frac{1+\sqrt{5}}{2} = a+b\sqrt{5} \quad \text{for some } a,b \in \mathbb{Z}.$$

However, this gives a contradiction as $a = b = 1/2$ which are not integers. In fact, the full set of elements in $\mathbb{Q}\left(\sqrt{5}\right)$ that are integral over $\mathbb{Z}\left(\sqrt{5}\right)$ is exactly

$$\mathbb{Z}\left(\frac{1+\sqrt{5}}{2}\right)$$

which is the integral closure of $\mathbb{Z}\left(\sqrt{5}\right)$ in $\mathbb{Q}\left(\sqrt{5}\right)$.

Theorem 3.8. Let A be an integral domain. Then, the following are equivalent:

(i) A is integrally closed

(ii) $A_{\mathfrak{p}}$ is integrally closed for all prime ideals $\mathfrak{p}$

(iii) $A_{\mathfrak{m}}$ is integrally closed for all maximal ideals $\mathfrak{m}$

Definition 3.10 (normal ring)**.** A ring A is normal if $A_{\mathfrak{p}}$ is an integrally closed domain for all prime ideals $\mathfrak{p}$.

3.4 Completions

Definition 3.11 (directed set)**.** A directed set is a set Λ with a relation R which is reflexive and transitive and such that

$$\text{for all } a,b \in \Lambda \quad \text{we have} \quad a \leq c \text{ and } b \leq c.$$

We have the following chain of inclusions:

$$\text{totally ordered sets} \subseteq \text{directed sets} \subseteq \text{partially ordered sets}$$

Now, fix a ring A and let M be an A-module. Suppose we are given a collection $\{M_\lambda\}_{\lambda\in\Lambda}$ of submodules $M_\lambda \subseteq M$, where Λ is a directed set with M_λ's ordered by inclusion. Given this data, we can put a topology on M.

We declare that the open sets of M are arbitrary unions of the cosets of the M_λ's. In other words,

$$\{x+M_\lambda : x \in M, \lambda \in \Lambda\} \quad \text{forms} \quad \text{a base for this topology.}$$

Note that this makes M into a topological Abelian group under addition because $M \times M \xrightarrow{+} M$ has the property that the preimage of any $x+M_\lambda \supseteq (x+M_\lambda)\times M_\lambda$. Moreover, A-multiplication is continuous because $a : M \times M$ has the property that the pre-image of $ax+M_\lambda \supseteq x+M_\lambda$. M is what we call a linearly topologized A-module.

Example 3.15. If $M = A$, then all M_λ's are ideals, and one can check that the multiplication map $\cdot$ is continuous because

$$(x+M_\lambda)(y+M_\lambda) = xy+M_\lambda.$$

In particular, A is a topological ring.

Example 3.16 (I-adic topology on M)**.** Let our directed set $\Lambda = \mathbb{N}$, and let $I \subset A$ be some fixed ideal. For any A-module M, define $M_n = I^n M$ for any A-module M.

The I-adic topology need not be Hausdorff — in fact, it can be quite nasty in general. For example, in Example 3.16, let $I = (0)$, then our topology becomes the one-point set topology. One can check that the topology induced on M induced by $\{M_\lambda\}_{\lambda\in\Lambda}$ is Hausdorff if and only if

$$\bigcap_{\lambda\in\Lambda} M_\lambda = \{0\}.$$

Consider M/M_λ with its quotient topology. As M_λ is open and closed (since its complement is just a union of cosets of it), it follows that the preimage of any $S \subset M/M_\lambda$ is

$$\bigcup_{s\in\widetilde{S}} s+M_\lambda \quad \text{where} \quad s+M_\lambda \in \widetilde{S} \text{ refers to the lift of } s \in S$$

is open and closed. In other words, the inherited quotient topology of M/M_λ is discrete.

Definition 3.12 (separation quotient). Define

$$M^{\text{sep}} = M/\bigcap_{\lambda\in\Lambda} M_\lambda.$$

This set inherits an inherent linear topology coming from

$$\left\{\left(M_\lambda + \bigcap_{\mu\in\Lambda} M_\mu\right)/\bigcap_{\mu\in\Lambda} M_\mu\right\}_{\lambda\in\Lambda} \quad \text{is Hausdorff.}$$

Definition 3.13 (completion of module). We define

$$\widehat{M} = \varprojlim M/M_\lambda \quad \text{to be} \quad \text{the completion of } M.$$

Observe that for all $\lambda \le \mu$, we have canonical maps $\varphi_{\lambda\mu} : M/M_\mu \to M/M_\lambda$ (since we can quotient the larger submodule by the smaller submodule) such that $\varphi_{\lambda\mu}\circ\varphi_{\mu\gamma} = \varphi_{\lambda\gamma}$ for all $\lambda \le \mu \le \gamma$. By definition,

$$\widehat{M} = \left\{\{x_\lambda\}_{\lambda\in\Lambda} \in \prod_\lambda M/M_\lambda \mid \varphi_{\lambda_\mu}(x_\mu) = x_\lambda \text{ for all } \lambda \le \mu\right\} \subseteq \prod_{\lambda\in\Lambda} M/M_\lambda.$$

Equip $\widehat{M}$ the subspace topology for

$$\subseteq \prod_{\lambda\in\Lambda} M/M_\lambda,$$

where M/M_λ is in the discrete topology and the product of M/M_λ over all $\lambda\in\Lambda$ is in the product topology. A crucial observation here is that the following diagram commutes:

$$\begin{array}{ccc} M & \xrightarrow{\psi} & \hat{M} \\ & \searrow & \downarrow p_\lambda \\ & & M/M_\lambda \end{array}$$

Here, $\psi(x) = \{x\}_{\lambda\in\Lambda}$ and p_λ is the obvious projection of $\widehat{M}$ to the corresponding coordinate $\lambda\in\Lambda$. By the commutativity of the diagram and the obvious surjectivity of taking quotients (since p_λ is a projection map), we deduce that p_λ is also surjective.

We also note that

$$\ker\psi = \bigcap_{\lambda\in\Lambda} M_\lambda \quad \text{and} \quad \operatorname{im}\psi = \psi(M) \subseteq \widehat{M} \text{ is dense in } M.$$

This is seen from the following proposition (Proposition 3.11).

Proposition 3.11. $\widehat{M}$ is linearly topologized by the submodules $M_\lambda^* = \ker p_\lambda$, and $\ker p_\lambda$ is equal to the closure of $\psi(M_\lambda)$ in $\widehat{M}$. Moreover, $\widehat{M}$ is complete, in the sense that $\widehat{\widehat{M}} \cong \widehat{M}$ as topological A-modules.

Example 3.17. Let A be a ring $x_1,\dots,x_n \in A$, $I = (x_1,\dots,x_n)$, then $\{I^jM\}_{j\in\mathbb{N}}$ gives the I-adic topology. We could also consider the directed system of ideals $J_n = (x_1^n,\dots,x_n^n)$. We claim that the two directed sets of ideals induce the same topology. Indeed, it is clear that $J_m \subseteq I^m$. Also $I^{mn} \subseteq J_m$. Therefore these two systems define the same topology on any A-module.

Now suppose that M is topologized by $\{M_\lambda\}_{\lambda\in\Lambda}$ and let $N \subseteq M$ be a submodule. Observe that the closure of N in M is $\overline{N} = \bigcap_{\lambda\in\Lambda}(N+M_\lambda)$. Indeed, we have the following chain of equivalent statements:

$$\begin{aligned} x \in \overline{N} \quad &\text{if and only if} \quad (x+M_\lambda)\cap N \neq \emptyset \text{ for all } \lambda \in \Lambda \\ &\text{if and only if} \quad x \in \bigcap_{\lambda\in\Lambda}(N-M_\lambda) = \bigcap_{\lambda\in\Lambda}(N+M_\lambda) \end{aligned}$$

Proposition 3.12. Let $N \subset M$ be a submodule, and let M'_λ be the image of $M_\lambda \to M \to M/N$. Then the quotient topology on M/N is the same as the linear topology induced by $\{M'_\lambda\}_{\lambda\in\Lambda}$.

Proof. Note that $\overline{U} \subseteq M/N$ is open is the quotient topology if and only if its preimage U is open on M, i.e. for all $x \in U$, there exists $\lambda \in \Lambda$ satisfying the following chain of equivalent statements:

$$\begin{aligned} \overline{U} \subseteq M/N \text{ is open} \quad &\text{if and only if} \quad U \subseteq M \text{ is open} \\ &\text{if and only if} \quad \text{for all } x \in U \text{ there exists } \lambda, x+M_\lambda \subseteq U \\ &\text{if and only if} \quad \text{for all } x \in \overline{U} \text{ there exists } \lambda \text{ with } \overline{x}+M'_\lambda \subseteq \overline{U} \\ &\text{if and only if} \quad \overline{U} \text{ is open in the linear topology} \end{aligned}$$

□

One can check that M/N is separated (i.e. the intersection of M_λ's is 0) if and only if $N \subseteq M$ is closed. Also check that the subspace topology on N coincides with the linear topology generated by $\{N\cap M_\lambda\}_{\lambda\in\Lambda}$.

Now, for every $\lambda \in \Lambda$, we have an exact sequence

$$0 \to N/N\cap M_\lambda \to M/M_\lambda \to (M/N)/M' = M/(N+M_\lambda) \to 0$$

which is compatible with varying λ. Hence, we obtain the maps $\widehat{N} \to \widehat{M} \to \widehat{M/N}$. In fact, we get an exact sequence

$$0 \to \widehat{N} \to \widehat{M} \to \widehat{(M/N)}.$$

Note that if M is an A-module, then $\widehat{M}$ is naturally an $\widehat{A}$-module where the ring action is defined componentwise. In other words, the I-adic completion is a functor from A-modules to $\widehat{A}$-modules.

Example 3.18. Let $A = \mathbb{Z}$, $I = (p)$, where p prime. Then

$$\widehat{A} \subseteq \prod_{n\geq 1} \mathbb{Z}/p^n\mathbb{Z},$$

so $a_n \pmod{p^n} = a_m$ for all $m \leq n$.

Note that $1+p$ is not a unit for p prime, but $1+p$ is a unit in $\mathbb{Z}/p\mathbb{Z}$: the element $a \in \mathbb{Z}/p\mathbb{Z}$ with

$$a_m = \sum_{k=0}^{m-1}(-p)^k \quad \text{satisfies } a(1+p) = 1.$$

Furthermore, $\mathbb{Z}/p\mathbb{Z}$ has only two prime ideals, which are the ideal generated by p and the zero ideal.

Definition 3.14 (complete local ring). If $(A,\mathfrak{m})$ is a local ring such that A is $\mathfrak{m}$-adically complete, we say that A is a complete local ring.

Example 3.19. $\mathbb{Z}/p\mathbb{Z}$ is a complete local ring.

Proposition 3.13. For any local ring $(A,\mathfrak{m})$, $\left(\widehat{A},\mathfrak{m}\widehat{A}\right)$ is a complete local ring.

Theorem 3.9 (Hensel's lemma). Suppose $(A,\mathfrak{m})$ is a complete local ring with residue field k. Let $F \in A[X]$ be a monic polynomial. Suppose in $k[X]$, there exists a factorisation $\overline{F} = GH$ for some coprime monic polynomials $G,H \in k[X]$. Then,

$$\text{there exist } \widetilde{G},\widetilde{H} \in A[X] \quad \text{such that } \widetilde{G} \equiv G \pmod{\mathfrak{m}} \text{ and } \widetilde{H} \equiv H \pmod{\mathfrak{m}}.$$

Example 3.20. Let $A = \mathbb{Z}/5\mathbb{Z}$ and $F = X^2+1$. Then, $k = \mathbb{F}_5$ (the field consisting of five elements). Notice that $X^2+1 \in \mathbb{F}_5[X]$ has roots 2 and 3, so $X^2+1 = (X-2)(X-3)$. Since $X-2$ and $X-3$ are monic and coprime in $\mathbb{F}_5[X]$, they meet the conditions of Hensel's lemma.

Theorem 3.10. For a ring A, fix an ideal $I \subseteq A$ and M an A-module. Assume A is I-adically complete and M is I-adically separated, i.e.

$$\bigcap_{n\in\mathbb{N}} I^n M = \{0\}.$$

If $\overline{w}_1 \ldots, \overline{w}_n \in M/IM$ generate as an A/I-module, then any lifts $w_1,\ldots,w_n \in M$ generate as an A-module.

Proof. Pick w_i. We know that

$$M = \sum_i Aw_i + IM.$$

We can iterate this to obtain

$$M = \sum Aw_i + I\left(\sum Aw_i + IM\right) = \sum Aw_i + I^2M.$$

As such, for sufficiently large n, we have

$$M = \sum Aw_i + I^nM.$$

For $\xi \in M$, choose expressions:

$$\begin{aligned}
\xi &= \sum_i a_i w_i + \xi_1, \quad \text{where } \xi_1 \in IM,\\
\xi_1 &= \sum_i a_{i,1} w_i + \xi_2 \quad \text{where } \xi_2 \in I^2M \text{ and } a_{i,1} \in I,\\
\xi_2 &= \sum_i a_{i,2} w_i + \xi_3 \quad \text{where } \xi_3 \in I^3M \text{ and } a_{i,2} \in I^2
\end{aligned}$$

and the process continues. Set $b_i = a_i + a_{i,1} + a_{1,2} + \ldots \in A$, which is well-defined as A is I-adically complete. Then,

$$\xi - \sum_i b_i w_i \subseteq \bigcap_{n\geq 1} I^nM = \{0\} \quad \text{which implies} \quad \xi = \sum b_i w_i$$

and the w_i's generate M. □

Suppose we are given that $A \supseteq I$. In general, it is not true that for A-modules $N \subseteq M$, the I-adic topology on N is equal to the subspace topology coincides with the subspace topology from the I-adic topology on M.

Example 3.21. Let $A = \mathbb{Z}$, $I = (p)$, $N = \mathbb{Z}$, and $M = \mathbb{Q}$. Then, $I^NM = \mathbb{Q}$ but $I^nN = p^n\mathbb{Z}$[†].

[†]However, if A is Noetherian or M is finitely generated, this problem disappears.

Theorem 3.11 (Artin-Rees lemma). Fix $I \subseteq A$ with A Noetherian, $N \subseteq M$ being A-modules with M finitely generated. Then there exists $c > 0$ such that for all $n \geq c$,

$$I^n M \cap N = I^{n-c}\left(I^c M \cap N\right).$$

In particular, one has $I^n N \subseteq I^n M \cap N \subseteq I^{n-c} N$.

The proof of Theorem 3.11 is too long.

Corollary 3.6. Let $A \supseteq I$ with A Noetherian and $0 \to N \to M \to Q \to 0$ be a short exact sequence of A-modules with M finitely generated. Then the induced sequence on I-adic completions $0 \to \widehat{N} \to \widehat{M} \to \widehat{Q} \to 0$ is still exact.

Corollary 3.7. Let $I \subseteq A$ with A Noetherian, and M a finitely generated A-module. Then, $M \otimes_A \widehat{A} \cong \widehat{M}$.

Proof. Pick a presentation $A^n \to A^m \to M \to 0$. Then the sequence $\widehat{A}^n \to \widehat{A}^m \to \widehat{M} \to 0$ is still exact. Taking the tensor with $\widehat{A}$, we also have the following commutative diagram, where the rows are exact:

$$\begin{array}{ccccccc}
\hat{A}^n & \longrightarrow & \hat{A}^m & \longrightarrow & \hat{M} & \longrightarrow & 0 \\
\uparrow & & \uparrow & & \uparrow{\scriptstyle f} & & \| \\
A^n \otimes \hat{A} & \longrightarrow & A^m \otimes_A \hat{A} & \longrightarrow & M \otimes_A \hat{A} & \longrightarrow & 0
\end{array}$$

Then, f is an isomorphism by the four lemma. □

Proposition 3.14. An A-module M is flat if and only if for all ideals $J \subseteq A$, the natural map $J \otimes_A M \to M$ is injective.

Theorem 3.12. If A is Noetherian and $I \subseteq A$, then $\widehat{A}$ is a flat A-module.

Proof. Apply Proposition 3.14 with $M = \widehat{A}$. For all $J \subseteq A$, $J \otimes_A \widehat{A} \cong \widehat{J}$ by Corollary 3.7. Then

$$J \otimes_A \hat{A} \to \hat{A} = J \otimes_A \hat{A} \cong \hat{J} \hookrightarrow \hat{A} \quad \text{is injective.}$$

□

3.5 Artinian Rings

Definition 3.15 (Artinian ring). A ring A is Artinian if it satisfies the descending chain condition (DCC), i.e.

$$I_1 \supseteq I_2 \supseteq \ldots \quad \text{implies} \quad I_n = I_{n+1} \text{ for } n \text{ sufficiently large.}$$

Remark 3.2. In practice, it is not easy to make an ascending chain of ideals. (i.e. if A is a local ring, it is not possible to make a non-trivial ascending chain starting from its maximal ideal. The DCC says that the sequence of ideals $I \supseteq I^2 \supseteq I^3 \supseteq \ldots$ eventually stabilises for any ideal $I \subseteq A$.

Example 3.22. Let k be a field and let $A = [x,y] / \left(x^3, xy, y^3\right)$, then A is a finite dimensional vector space (in fact, it is 8-dimensional).

Each chain of descending ideals is also a chain of descending vector spaces over k so the dimension can only strictly decrease finitely many times.

Example 3.23. Let $A = \mathbb{Z}/n\mathbb{Z}$. Then, A cannot have a decreasing chain that does not stabilise as A is finite cardinality. So, $\mathbb{Z}/n\mathbb{Z}$ is Artinian.

Example 3.24. $A = \mathbb{Z}$ is a non-example of an Artinian ring because we can consider

$$(4) \supseteq \left(4^2\right) \supseteq \left(4^3\right) \supseteq \ldots.$$

Proposition 3.15. If A is an integral domain and Artinian, then A is a field.

Proof. Let $x \in A$ be non-zero and consider the descending chain of ideals $(x) \supseteq \left(x^2\right) \supseteq \left(x^3\right) \supseteq \ldots$. By the descending chain condition, $(x^n) = \left(x^{n+1}\right)$, hence there exists $y \in A$ such that $x^{n+1} \cdot y = x^n$. So, $xy = 1$ and we conclude that A is a field. □

Corollary 3.8. If A is Artinian and $\mathfrak{p} \subseteq A$ is a prime ideal, then $\mathfrak{p}$ is a maximal ideal.

Proof. It is clear that a quotient of an Artinian ring is Artinian, so $A/\mathfrak{p}$ is an integral domain. By Proposition 3.15, A is a field, so $\mathfrak{p}$ is a maximal ideal. □

Proposition 3.16. If A is Artinian, then A only has finitely many maximal ideals.

Proof. Suppose we have maximal ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$, then we get a descending chain

$$\mathfrak{m}_1 \supseteq \mathfrak{m}_1\mathfrak{m}_2 \supseteq \mathfrak{m}_1\mathfrak{m}_2\mathfrak{m}_3 \supseteq \ldots$$

By the Chinese remainder theorem, since maximal ideals are pairwise comaximal, we have

$$A/\mathfrak{m}_1\mathfrak{m}_2 \ldots \mathfrak{m}_i \cong A/\mathfrak{m}_1 \times \ldots \times A/\mathfrak{m}_i$$

so the inclusion $\mathfrak{m}_1 \supsetneq \mathfrak{m}_1\mathfrak{m}_2$ is strict. By the DCC, the chain cannot descend infinitely. Hence, the number of distinct maximal ideals is finite. □

Corollary 3.9. For an Artinian ring

$$\mathfrak{N}_A = J(A) = \bigcap_{i=1}^{l} \mathfrak{m}_i = \prod_{i=1}^{l} \mathfrak{m}_i,$$

where $\mathfrak{m}_1, \ldots, \mathfrak{m}_l$ is an enumeration of all the maximal ideals of A.

Proof. This is immediate from Proposition 3.16 since

$$J(A) \text{ is the intersection of all maximal ideals} \quad \text{and} \quad \mathfrak{N}_A \text{ is the intersection of all prime ideals,}$$

and prime ideals and maximal ideals are the same. □

Proposition 3.17. If A is an Artinian ring, then $\mathfrak{N}_A^k = 0$ for all k sufficiently large.

Proof. Since A is an Artinian ring, then by the descending chain condition, $\mathfrak{N}_A^k$ must stabilise at some ideal $\mathfrak{a}$. Suppose $\mathfrak{a} \neq 0$. We observe that

$$\mathfrak{a}^2 = \left(\mathfrak{N}_A^k\right)^2 = \mathfrak{N}_A^{2k} = \mathfrak{a}.$$

Hence,

$$\emptyset \neq \Sigma = \{\mathfrak{b} \subseteq A; \mathfrak{b}\mathfrak{a} \neq 0\}.$$

Note that every descending chain stabilises so by Zorn's lemma, there exists a minimal element $\mathfrak{c}$. Pick $x \in \mathfrak{c}$ such that $x\mathfrak{a} \neq 0$, which exists as $\mathfrak{c}\mathfrak{a} \neq 0$. However,

$$(x\mathfrak{a})\,\mathfrak{a} = x\,(\mathfrak{a} \cdot \mathfrak{a}) = x\mathfrak{a} \neq 0.$$

This implies that $x\mathfrak{a} \in \Sigma$. Since $x\mathfrak{a} \subseteq \mathfrak{c}$, we see that $x\mathfrak{a} = \mathfrak{c}$. Together, this implies that $(x) = x\mathfrak{a} = \mathfrak{c}$, so $x = xy$ for some $y \in \mathfrak{a} \subseteq \mathfrak{N}_A$. In fact, replacing x with xy, we have

$$x = xy = (xy)\,y = \ldots = xy^n \quad \text{for all } n \in \mathbb{N}$$

However, by the definition of the nilradical, we must have $xy^n = 0$ for sufficiently large n. THUS, $x = xy^n = 0$ so that $\mathfrak{c} = 0$, which contradicts out assumption that $\mathfrak{c}$ is non-zero. □

Corollary 3.10. Let A be an Artinian ring. For all k sufficiently large, we have

$$\mathfrak{m}_1^k \ldots \mathfrak{m}_l^k = 0 \quad \text{where } \mathfrak{m}_1, \ldots, \mathfrak{m}_l \text{ are maximal ideals of } A.$$

Corollary 3.11. If A is an Artinian ring, then

$$A \cong A_1 \times \ldots \times A_l \quad \text{where} \quad \text{each } A_i \text{ is an Artinian and a local ring.}$$

Proof. Observe that $A \cong A/(0) \cong A/\left(\mathfrak{m}_1^k \ldots \mathfrak{m}_l^k\right)$ for some sufficiently large k. One can check that $\mathfrak{m}_i^k$ and $\mathfrak{m}_j^k$ are coprime for $i \neq j$, thus by the Chinese remainder theorem, we have

$$A \cong A/\mathfrak{m}_1^k \times \ldots \times A/\mathfrak{m}_l^k.$$

A maximal ideal $\mathfrak{n}$ of $A/\mathfrak{m}_i^k$ is a maximal ideal of A such that $\mathfrak{n} \supseteq \mathfrak{m}_i^k$, which implies $\mathfrak{n} \supseteq \mathfrak{m}_i$. Hence, $\mathfrak{n} = \mathfrak{m}_i$. Thus, the maximal ideal of $A/\mathfrak{m}_i^k$ is unique, so this ring is Artinian and local. □

Definition 3.16. The *length function* is a function from the class of A-modules of $N \cup \{\infty\}$ defined by

$$\ell = \sup\{n : M = M_n \supsetneq \ldots \supsetneq M_0 = 0\}.$$

Example 3.25. We have $\ell_{\mathbb{Z}}(\mathbb{Z})$ because $\mathbb{Z}$ does not satisfy the descending chain condition.

Example 3.26. $\ell_{\mathbb{Z}}(\mathbb{Z}/6) = 2$, i.e. there are exactly 2 chains of length 2. They are as follows:

$$\mathbb{Z}/6\mathbb{Z} \supseteq 3\mathbb{Z}/6\mathbb{Z} \supseteq (0) \quad \text{and} \quad \mathbb{Z}/6\mathbb{Z} \supseteq 2\mathbb{Z}/6\mathbb{Z} \supseteq (0)$$

We note that for an Artinian ring A, ℓ_A is uniquely characterised by the following. Firstly, $\ell_A(A/\mathfrak{m}) = 1$, where $\mathfrak{m}$ is a maximal ideal of A. Also, for a short exact sequence of modules

$$0 \to K \to M \to Q \to 0 \quad \text{we have} \quad \ell_A(M) = \ell_A(K) + \ell_A(Q).$$

Moreover,

$$\ell_A(M) = n \quad \text{if and only if} \quad M = M_n \supseteq M_{n-1} \supseteq \ldots M_0 = 0$$

such that each $M_i/M_{i-1} \cong A/\mathfrak{m}$ for some maximal ideal $\mathfrak{m} \subseteq A$.

Theorem 3.13. The following are equivalent:

(i) A is Noetherian and $0 = \mathfrak{n}_1 \dots \mathfrak{n}_l$, where each $\mathfrak{n}_i$ is a maximal ideal

(ii) A is Noetherian and all prime ideals are maximal, i.e. A is Noetherian and $\dim(A) = 0$

(iii) $\ell_A(A) < \infty$

(iv) A is Artinian

Proof. We first prove **(i)** implies **(ii)**. Suppose A is Noetherian and there exists a factorisation $\mathfrak{n}_1, \dots, \mathfrak{n}_l$, where each $\mathfrak{n}_i$ is a maximal ideal. We wish to show that A is Noetherian of Krull dimension 0. More concretely, we wish to show that every prime ideal of A is maximal. Suppose $\mathfrak{p} \subseteq A$ is a prime ideal. As $0 = \mathfrak{n}_1 \dots \mathfrak{n}_l$, then every element in the product $\mathfrak{n}_1 \dots \mathfrak{n}_l$ is 0. For this product to lie in $\mathfrak{p}$, at least one of the factors must be contained in $\mathfrak{p}$[†]. Hence,

$$\mathfrak{n}_i \subseteq \mathfrak{p} \quad \text{for some } 1 \leq i \leq l.$$

However, as $\mathfrak{n}_i$ is maximal, then $\mathfrak{p} = \mathfrak{n}_i$. This shows that every prime ideal is maximal, so $\dim(A) = 0$. Thus, **(ii)** follows.

We then prove **(ii)** implies **(iii)**. There is a standard fact which states that if A is Noetherian ring such that $\dim(A) = 0$, then it is said to be Artinian on the punctured spectrum, or it can be shown to be the finite product of local rings, each with nilpotent Jacobson radical. Concretely, dimension 0 forces the prime ideals and maximal ideals to coincide. Noetherian plus dimension 0 then implies that the Jacobson radical is nilpotent and that A has only finitely many maximal ideals.

One can show A is the finite direct product of local Artinian rings, each of which has finite length over itself. Finite direct sums of finite-length modules also have finite length. Hence, A as an A-module has a composition series, so **(iii)** follows.

We then prove that **(iii)** implies **(iv)**. If A has finite length as a module over itself, it cannot admit any infinite chain of submodules. But an ideal $I \subseteq A$ is precisely a submodule of A. Hence, there can be no infinite descending chain of ideals in A. By Definition 3.15, A is Artinian.

Lastly, we prove **(iv)** implies **(i)**. By Definition 3.15 again, Artinian rings satisfy the descending chain condition on ideals. This implies the ascending chain condition (ACC) on ideals as well, making the ring Noetherian.

In an Artinian ring, the nilradical is nilpotent. Also, the prime ideals coincide with the maximal ideals (the dimension is 0). So, the intersection of all maximal ideals is nilpotent. Equivalently, some product of all the maximal ideals is the zero ideal. So we can label these maximal ideals

$$\mathfrak{n}_1, \dots, \mathfrak{n}_l \quad \text{and obtain} \quad 0 = \mathfrak{n}_1 \cdot \ldots \cdot \mathfrak{n}_l.$$

Hence, **(i)** holds. □

[†]Recall that this essentially follows from the definition of $\mathfrak{p}$ being a prime ideal, i.e. if $xy \in \mathfrak{p}$, then either $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$.

3.6 Euclidean Domains, Principal Ideal Domains and Unique Factorisation Domains

Definition 3.17 (Euclidean domain)**.** A ring A is said to be a Euclidean domain (ED) if there exists $f : A \setminus \{0\} \to \mathbb{N}$ such that for all $a, b \in A$, there exist $q, r \in A$ such that

$$a = qb + r \text{ with } r = 0 \quad \text{or} \quad f(r) < f(b).$$

Example 3.27. For any field k, we have $k[x]$ is an ED, where f can be the map $p(x) \mapsto \deg(p)$.

Definition 3.18 (prinicpal ideal domain)**.** A ring A is said to be a principal ideal domain (PID) if all ideals of A are principal, i.e. $I = (a)$.

One should recall from MA3201 that a principal ideal is an ideal that is generated by a single element.

Definition 3.19 (unique factorisation domain)**.** A ring A is said to be a unique factorisation domain if every element $a \in A$ can be written as

$$a = a_1 \dots a_n,$$

with each a_i being irreducible. By irreducible, we mean that if there exist $b, c \in A$ such that $a_i = bc$, then either b or c is a unit, and this is unique up to units.

Proposition 3.18. One has

$$\{\text{euclidean domains}\} \subsetneq \{\text{principal ideal domains}\} \subsetneq \{\text{unique factorization domains}\}$$

and these inclusions are strict.

Example 3.28. Given a field k, the ring $k[x, y]$ is a UFD but not a PID.

Example 3.29. The ring $\mathbb{Z}\left[\sqrt{-19}\right]$[†] is a PID but not a ED.

Example 3.30 (Gaussian integers)**.** The ring of Gaussian integers $\mathbb{Z}[i]$ is an ED with

$$f : \mathbb{Z}[i] \setminus \{0\} \to \mathbb{N} \quad \text{given by} \quad a + bi \mapsto a^2 + b^2$$

Example 3.31. $\mathbb{Z}\left[\sqrt{-5}\right]$ is a non-example of a UFD. To see why, we have

$$2 \cdot 3 = \left(1 + \sqrt{-5}\right)\left(1 - \sqrt{-5}\right) \quad \text{where} \quad 2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5} \text{ are all irreducible.}$$

Define a norm

$$N : \mathbb{Z}[\sqrt{-5}] \to \mathbb{Z} \quad \text{where} \quad N\left(a + b\sqrt{-5}\right) = \left(a + b\sqrt{-5}\right)\left(a - b\sqrt{-5}\right) = a^2 + 5b^2.$$

by: Notice that $N(x) = 1$ if and only if x is a unit since the norm function N is multiplicative. To see that, for instance, 2 is irreducible. Suppose otherwise. Then we have

$$4 = N(2) = N(x)N(y)$$

and $N(x) = 2$ implies there exists an integer solution to $2 = a^2 + 5b^2$, which there clearly isn't. Then, we see that 2 is not associate to $1 + \sqrt{-5}$. So, $\mathbb{Z}\left[\sqrt{-5}\right]$ is not a UFD.

[†] -19 is a Heegner number.

Example 3.32 (cyclotomic field). Consider $\mathbb{Z}[\mathbb{Z}eta_n]$ where $\mathbb{Z}eta_n = \exp(2\pi i/n)$, this is a UFD for many $n \leq 90$ and no $n > 90$. Observe that for $x, y, z \in \mathbb{Z}$, we have

$$z^n = x^n + y^n = (x+y)(x+\mathbb{Z}eta_n y)\dots\left(x+\mathbb{Z}eta_n^{n-1}y\right) \in \mathbb{Z}[\mathbb{Z}eta_n].$$

A known result is that Fermat's Last Theorem for a given exponent $n \in \mathbb{N}$ holds if and only if the ring $\mathbb{Z}[\mathbb{Z}eta_n]$ is a UFD. Unfortunately, this unique factorization property likely fails for most values of n.

3.7 Primary Decomposition

Definition 3.20 (primary ideal). An ideal $I \subseteq A$ is primary if

$$xy \in I \quad \text{implies} \quad x \in I \text{ or } y \in \sqrt{I}.$$

Proposition 3.19. $I \subseteq A$ is primary if and only if every zero-divisor in A/I is nilpotent.

Example 3.33. A prime ideal $\mathfrak{p}$ is primary. In fact $\mathfrak{p}$ is primary and radical.

Example 3.34. $\left(x^2, xy\right) \subseteq k[x,y]$ is primary.

Example 3.35. Here is a non-example. Let

$$A = \left\{p(T) \in \mathbb{Z}[T] : 3 \mid p'(0)\right\}.$$

Then $\mathfrak{p} = \left(3T, T^2, T^3\right)$ is prime but $\mathfrak{p}^2$ is not primary.

Proposition 3.20. If I is primary, then $\sqrt{I}$ is prime.

Note that the converse of Proposition 3.20 does not hold in general as shown in Example 3.35.

Definition 3.21. If $I \subseteq A$ is primary and $\mathfrak{p} = \sqrt{I}$, then I is $\mathfrak{p}$-primary.

Proposition 3.21. If $\sqrt{I} = \mathfrak{m}$ is maximal, then I is primary.

Proof. $\mathfrak{m}/I \subseteq A/I$ is the unique prime of A/I because every prime ideal of A/I corresponds to a prime ideal in A containing I; such an ideal must contain $\sqrt{I} = \mathfrak{m}$, so this is just $\mathfrak{m}$.

Hence, all non-units of A/I are in $\mathfrak{m}/I$. In particular, every zero-divisor of A/I is in $\mathfrak{m}/I$. But then all elements in $\mathfrak{m}/I$ nilpotent, so I is primary. □

The main theorems of the section are the following:

Lemma 3.1. Let A be a Noetherian ring. Then, the following hold:

(i) If I is a $\mathfrak{p}$-primary ideal, there exists N such that $\mathfrak{p}^N \subseteq I$

(ii) I is $\mathfrak{m}$-primary for some maximal ideal $\mathfrak{m}$ if and only if A/I is Artinian and local

(iii) I is $\mathfrak{m}$-primary and $IA_{\mathfrak{m}} = \mathfrak{m}^n A_{\mathfrak{m}}$ implies $I = \mathfrak{m}^n$

Theorem 3.14. Let A be a 1-dimensional Noetherian domain, i.e. every non-zero prime ideal is maximal. Then every $0 \neq I \subseteq A$ admits a unique factorisation

$$I = \prod_{i=1}^{l} I_i \quad \text{where} \quad I_i \text{ is primary and } \sqrt{I_i} \neq \sqrt{I_j} \text{ for } i \neq j.$$

Proposition 3.22. Let A be a Noetherian local ring with dimension 1. Set $k = A/\mathfrak{m}$. Then, the following are equivalent:

(i) A is a discrete valuation ring
(ii) A is normal
(iii) $\mathfrak{m}$ is principal
(iv) $\dim_k\left(\mathfrak{m}/\mathfrak{m}^2\right) = 1$
(v) All ideals are of the form $\left(x^l\right)$ for some x

Lemma 3.2. Let $(A, \mathfrak{m})$ be an Artinian local ring. Then, the following are equivalent:

(i) Every ideal is principal
(ii) $\mathfrak{m}$ is principal
(iii) $\dim_k\left(\mathfrak{m}/\mathfrak{m}^2\right) \leq 1$

3.8 Discrete Valuation Rings

Definition 3.22 (discrete valuation ring). A discrete valuation on a field k is a map $v : k^\times \to \mathbb{Z}$ such that the following hold:

(i) $v(xy) = v(x) + v(y)$
(ii) $v(x+y) \geq \min\{v(x), v(y)\}$, and equality holds if $v(x) \neq v(y)$

Define

$$\mathcal{O}_v = \{x \in k : v(x) \geq 0\} \quad \text{which is} \quad \text{a subring of } k.$$

A ring that is of the form $\mathcal{O}_v$ is a discrete valuation ring.

Remark 3.3. As a convention, we usually set $v(0) = \infty$.

Example 3.36. Let

$$v_p : \mathbb{Q}^\times \to \mathbb{Z} \quad \text{be defined by} \quad p^n \frac{a}{b} \mapsto n \text{ for } p \text{ that does not divide } ab.$$

Then $\mathcal{O}_v = \mathbb{Z}_{(p)}$.

Example 3.37. Let

$$v : k(t) \to \mathbb{Z} \quad \text{where} \quad t^n \frac{f(t)}{g(t)} \mapsto n \text{ for } t \text{ which does not divide } f(t)\, g(t).$$

Then $\mathcal{O}_v = k[t]_{(t)}$.

Here are some nice facts about the structure of ideals in discrete valuation rings (DVR). Let A be a DVR with valuation v. Then, the following properties hold:

(i) We have

$$x \in A^\times \quad \text{if and only if} \quad v(x) = 0$$

since $x \in A^\times$ implies $x^{-1} \in A$ and $v(x) \geq 0$ and $v\left(x^{-1}\right) = -v(x) \geq 0$ forces $v(x) = 0$

(ii) For $x, y \in A$, we have

$$(x) = (y) \quad \text{if and only if} \quad v(x) = v(y)$$

(iii) Given $0 \neq I$, let $x \in I$ have minimal valuation. Then given $y \in I$, we have

$$v\left(x^{-1}y\right) = v(y) - v(x) \geq 0,$$

which implies that $\frac{y}{x} \in A$, or $x \mid y$, or $y \in (x)$. In fact, we have $(x) \subseteq I \subseteq (x)$, so $I = (x)$.

(iv) The ideals of A are

$$I_i = \{x \in A : v(x) \geq i \text{ where } i \geq 0\}$$

(v) Moreover, if $v(x) = 1$, then $I_i = \left(x^i\right)$. We say that x is a uniformizer of the DVR.

Lemma 3.3. Let $(A, \mathfrak{m})$ be an Artinian local ring. Then, the following are equivalent:

(i) Every ideal is principal

(ii) $\mathfrak{m}$ is principal

(iii) $\dim_k(\mathfrak{m}/\mathfrak{m}^2) \leq 1$

Proof. **(i)** implies **(ii)** is obvious. We then prove **(ii)** implies **(iii)**. Suppose $\mathfrak{m} = (x)$. Then, there exists a surjection

$$A/\mathfrak{m} \twoheadrightarrow \mathfrak{m}/\mathfrak{m}^2 = (x)/\left(x^2\right) \quad \text{defined by} \quad a \mapsto ax + \left(x^2\right)$$

This implies $\dim_k\left(\mathfrak{m}/\mathfrak{m}^2\right) \leq 1$.

To prove **(iii)** implies **(i)**, if $\dim\left(\mathfrak{m}/\mathfrak{m}^2\right) = 0$, then $\mathfrak{m}/\mathfrak{m}^2 = 0$. By Nakayama's lemma, $\mathfrak{m} = (0)$, so A is a field. On the other hand, if $\mathfrak{m}/\mathfrak{m}^2$ is 1-dimensional, then there exists $x \in \mathfrak{m}$ whose image generates $\mathfrak{m}/\mathfrak{m}^2$. By Nakayama's lemma, if $\bar{x}$ generates $\mathfrak{m}/\mathfrak{m}^2$, then $\mathfrak{m} = (x)$ in A. Let $0 \neq I \subseteq A$, then there exists $N \in \mathbb{N}$ such that $I \subseteq \mathfrak{m}^N = \left(x^N\right)$ but $I \subseteq \mathfrak{m}^{N+1}$. Then, there exists $y \in I$ such that $y = x^n t$, $t \notin (x)$. Since $(x) = \mathfrak{m}$ is maximal and $t \notin (x)$, this implies that t is a unit, therefore $I = \left(x^N\right)$. □

Proposition 3.23. Let A be a Noetherian local domain (by local, it means that A has a unique maximal ideal) with dimension 1. Set $k = A/\mathfrak{m}$. Then, the following are equivalent:

(i) A is a DVR

(ii) A is normal (integrally closed in its field of fractions)

(iii) $\mathfrak{m}$ is principal

(iv) $\dim_k\left(\mathfrak{m}/\mathfrak{m}^2\right) = 1$

(v) All ideals are of the form $\left(x^l\right)$ for some x

Proposition 3.24. Let A be a 1-dimensional Noetherian domain. Then, the following are equivalent:

(i) A is normal.

(ii) $A_\mathfrak{m}$ is normal for all maximal ideals $\mathfrak{m}$

(iii) $A_\mathfrak{m}$ is a DVR for every maximal ideal $\mathfrak{m}$

3.9 Dedekind Domains

It feels as if we are venturing into MA5202 territory now.

Definition 3.23 (Dedekind domain)**.** A ring A is a Dedekind domain if it is a 1-dimensional Noetherian normal domain.

Example 3.38. $\mathbb{Z}[\zeta_n]$ is a Dedekind domain for every $n \in \mathbb{N}$.

Proposition 3.25. Let A be a Dedekind domain. Then any non-zero primary ideal is a power of a prime.

Proof. Let $0 \neq I$ be primary, then I is $\mathfrak{m}$-primary for some $\mathfrak{m}$, since every non-zero prime is maximal. But $A_\mathfrak{m}$ is a DVR, and $IA_\mathfrak{m} = \mathfrak{m}^n A_\mathfrak{m}$, so I is a power of $\mathfrak{m}$. □

Together with the primary decomposition theorem we obtain Theorem 3.15 on the unique factorisation of ideals in a Dedekind domain.

Theorem 3.15 (unique factorisation of ideals in a Dedekind domain)**.** Let A is a Dedekind domain and $I \neq 0$ be an ideal of A. Then, I factorises into a product of powers of prime ideals uniquely, i.e. there exist unique $\mathfrak{p}_i$, e_i up to ordering such that

$$I = \prod_{i=1}^{l} \mathfrak{p}_i^{e_i}.$$

Here is a fun fact — Kummer's theorem on Fermat's last theorem for regular primes states that if $\mathbb{Z}[\zeta_p]$ is such that p is a regular prime, then Fermat's last theorem holds for $n = p$.

Example 3.39. $\mathbb{Z}\left[\sqrt{-5}\right]$ is not a UFD but it is a Dedekind domain. We have

$$(6) = (2)(3) = \left(1+\sqrt{5}\right)\left(1-\sqrt{5}\right).$$

However, $(2), (3)$ $\left(1 \pm \sqrt{-5}\right)$ are not prime! To see why, for (2), we have

$$\mathbb{Z}\left[\sqrt{-5}\right]/(2) = \mathbb{Z}[x]/\left(x^2+5, 2\right) = \mathbb{F}_2[x]/\left(x^2+5\right) = \mathbb{F}_2[x]/(x+1)^2$$

is not an integral domain because $x+1$ is nilpotent. Hence, $(2) = \left(2, 1+\sqrt{-5}\right)^2$. We also have

$$\begin{aligned}(3) &= \left(3, 1+\sqrt{-5}\right)\left(3, 1-\sqrt{-5}\right)\\ \left(1+\sqrt{5}\right) &= \left(3, 1+\sqrt{-5}\right)\left(2, 1+\sqrt{-5}\right)\\ \left(1-\sqrt{5}\right) &= \left(3, 1-\sqrt{-5}\right)\left(2, 1+\sqrt{-5}\right)\end{aligned}$$

3.10 Fractional Ideals

Recall that a PID is precisely a UFD that is also a Dedekind domain. At this juncture, we shall try to quantify the difference between a Dedekind domain and a PID. The answer turns to be that if A is a Dedekind domain, then we can define canonically the ideal class group of A, written $\mathrm{Cl}(A)$.

In fact, we will see that $|\mathrm{Cl}(A)| = 1$ if and only if A is a PID.

Example 3.40. We have $\mathrm{Cl}\left(\mathbb{Z}\left[\sqrt{-5}\right]\right) \cong \mathbb{Z}/2\mathbb{Z}$ because

$$6 = \left(1+\sqrt{-5}\right)\left(1-\sqrt{-5}\right) = 2\cdot 3.$$

Definition 3.24 (fractional ideal)**.** Let A be an integral domain, and $K = \mathrm{Frac}(A)$. Let $M \subseteq K$ be an A-submodule such that

$$\text{there exists } x \in A\setminus\{0\} \quad \text{such that} \quad xM \subseteq A.$$

Then, M is said to be a *fractional ideal* of A. Informally, we sy that $M \subseteq x^{-1}A$ so $M = x^{-1}J$ for some ideal $J \subseteq A$.

Example 3.41. Every ideal of A is a fractional ideal.

Example 3.42. Any $x \in K$ generates a fractional ideal $xA \subseteq K$.

For a submodule $M \subseteq K$, we write

$$(A : M) = \{x \in K \mid xM \subseteq A\}.$$

We sometimes use the symbol A/M to denote this.

Proposition 3.26. Every finitely generated A-module of K is a fractional ideal. Conversely, if A is Noetherian, then every fractional ideal is finitely generated.

In Proposition 3.26, the converse holds because $xM \subseteq A$ is a regular ideal of A.

Definition 3.25 (invertible module)**.** Given a A-submodule $M \subseteq K$, M is said to be *invertible* if there exists a submodule $N \subseteq K$ such that

$$MN = A \quad \text{where } MN \text{ is the } A\text{-submodule generated by } \{mn : m \in M, n \in N\}.$$

In a Dedekind domain, the set of all invertible ideals form a group, which contains the subgroup of principal invertible ideals. The *class group* is defined to be the group of invertible ideals quotient by the subgroup of principal invertible ideals. We will see this in due course.

Proposition 3.27. Let $M \subseteq K$ be an A-submodule. If there exists $N \subseteq K$ such that $MN = A$, then N is in fact unique and equal to $(A : M)$.

Proof. For any such N we have $N \subseteq (A : M) = (A : M)MN \subseteq N$. □

Proposition 3.28. Any invertible ideal is a finitely generated A-module and hence, fractional.

Proof. By Proposition 3.27, we can write $A = M \cdot (A : M)$. This implies that

$$1 = \sum_i x_i y_i \quad \text{for some } x_i \in M \text{ and } y_i \in (A : M).$$

Hence, if $x \in M$, then

$$x = \sum_i x_i (y_i x) \quad \text{implies} \quad \text{the set } \{x_i\}_i \text{ generate } M \text{ as an } A\text{-module}$$

since $y_i x \in A$ for all i. □

Proposition 3.29. Let $M \subseteq K$ be a fractional ideal. Then, the following are equivalent:

(i) M is invertible;

(ii) M is finitely generated and $M_\mathfrak{p}$ is invertible for every prime ideal $\mathfrak{p} \subseteq A$;

(iii) M is finitely generated and $M_\mathfrak{m}$ is invertible for every maximal ideal $\mathfrak{m} \subseteq A$

Proof. We first prove **(i)** implies **(ii)**. Note that $A = M \cdot (A : M)$ so for any prime ideal $\mathfrak{p}$ of A, we have

$$A_\mathfrak{p} = M_\mathfrak{p} \cdot (A : M)_\mathfrak{p} = M_\mathfrak{p} \cdot (A_\mathfrak{p} : M_\mathfrak{p}).$$

This shows that $M_\mathfrak{p}$ is invertible.

(ii) implies **(iii)** is obvious. Lastly, we prove **(iii)** implies **(i)**. Note the obvious inclusion $I = M \cdot (A : M) \subseteq A$. Since $\mathfrak{m}$ is a maximal ideal, then

$$I_\mathfrak{m} = M_\mathfrak{m} \cdot (A_\mathfrak{m} : M_\mathfrak{m}) = A_\mathfrak{m} \quad \text{so} \quad I = A.$$

□

Proposition 3.30. If A is a local domain (i.e. unique maximal ideal), then

$$A \text{ is a DVR} \quad \text{if and only if} \quad \text{every non-zero fractional ideal is invertible.}$$

Proof. For the forward direction, suppose A is a DVR. Let $\mathfrak{m} = (x)$ denote the maximal ideal. Recall that every ideal is principal and is of the form (x^n). Hence, $x^n M \subseteq A$ for some $n \in \mathbb{N}$, which implies that $x^n M = (x^t)$ for some t. As such,

$$M = x^{t-n} A \subseteq K \quad \text{is invertible with } (A : M) = x^{n-t} a.$$

For the reverse direction, suppose every non-zero fractional ideal is invertible. Hence, each fractional ideal is finitely generated. By **(ii)** of Definition 3.1, we infer that A is Noetherian.

To prove that A is a DVR, it suffices to show that all ideals $I = \mathfrak{m}^n$ for some n. Suppose otherwise. Let Σ denote the set of all proper ideals of A such that $I \neq \mathfrak{m}^r$ for all r. Let $\Omega \in \Sigma$ be a maximal element, which exists since A is Noetherian. Then, $\Omega \neq \mathfrak{m}$. So,

$$\mathfrak{m}^{-1} \cdot \Omega \subsetneq A \quad \text{since} \quad 1 \notin \{x \in A : x\mathfrak{m} \subseteq \Omega\} \quad \text{implies} \quad \mathfrak{m} \subseteq \Omega \quad \text{implies} \quad \mathfrak{m} = \Omega.$$

Now $\Omega \subseteq \mathfrak{m}^{-1}\Omega$. If $\Omega = \mathfrak{m}^{-1}\Omega$, then $\mathfrak{m}\Omega = \Omega$. By Nakayama's lemma, we have $\Omega = 0$. Thus, $\Omega \subsetneq \mathfrak{m}^{-1}\Omega$, so $\mathfrak{m}^{-1}\Omega = \mathfrak{m}^r$, and thus $\Omega = \mathfrak{m}^{r+1}$. The result follows. □

Theorem 3.16. Let A be an integral domain. Then,

$$A \text{ is a Dedekind domain} \quad \text{if and only if} \quad \text{all non-zero fractional ideals are invertible.}$$

Proof. For the forward direction, suppose A is a Dedekind domain. If $0 \neq M$ is a fractional ideal, then M is finitely-generated. Also, for all prime ideals $\mathfrak{p}$, $M_\mathfrak{p}$ is a fractional ideal of $A_\mathfrak{p}$, so for all $\mathfrak{p}$, $M_\mathfrak{p}$ is invertible. We conclude that M is invertible.

For the reverse direction, suppose every non-zero fractional ideal is invertible. Then, each of these ideals is finitely generated. By **(ii)** of Definition 3.1, A is Noetherian. Hence, for all $(0) \neq \mathfrak{p}$, $A_\mathfrak{p}$ is a DVR. One can

show that all $I \subseteq A_{\mathfrak{p}}$ are invertible. Let $J = I \cap A$. Then, J is invertible so $I = JA_{\mathfrak{p}} = J_{\mathfrak{p}}$. We conclude that A is a Dedekind domain. □

Corollary 3.12. If A is a Dedekind domain, the non-zero fractional ideal form an Abelian group, denoted by I_A, under multiplication.

If $I \subseteq K$ is a fractional ideal, then for all $(0) \neq \mathfrak{p}$, $IA_{\mathfrak{p}}$ is a fractional ideal of $A_{\mathfrak{p}}$ implies that there exists $n \in \mathbb{Z}$ such that $\mathfrak{p}^n A\mathfrak{p}$.

Actually,

$$I_A \cong \bigoplus_{0 \neq \mathfrak{p}} \mathbb{Z} \quad \text{where} \quad I \mapsto (v_{\mathfrak{p}}(I)).$$

In fact, given a short exact sequence

$$1 \to A^{\times} \to K^{\times} \to I_A \to \mathrm{Cl}(A) \to 1,$$

we infer that $\mathrm{Cl}(A) = \{1\}$ if and only if A is a PID.

Theorem 3.17. If $K/\mathbb{Q}$ is a finite extension, then $\mathcal{O}_K$ (ring of integers) is Dedekind, so

$$\mathcal{O}_K^{\times} \quad \text{is} \quad \text{a finitely generated Abelian group and } \mathrm{Cl}(\mathcal{O}_K) \text{ is a finite Abelian group.}$$

There is a nice conjecture which asks if there exists infinitely many square-free $d > 0$ such that

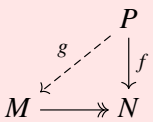
$$\left|\mathrm{Cl}\left(\mathbb{Q}\left(\sqrt{d}\right)\right)\right| = 1.$$

Theorem 3.18 (Stark-Heegner theorem). We have $\left|\mathrm{Cl}\left(\sqrt{-d}\right)\right| = 1$ for finitely many $d > 0$.

3.11 Projective Modules

Theorem 3.19 (projective module). Let A be a ring and P be an A-module. Then, the following are equivalent:

- **(i)** P is a summand of a free A-module
- **(ii)** $\mathrm{Hom}_A(P, -)$ is exact
- **(iii)** For all commutative diagrams:

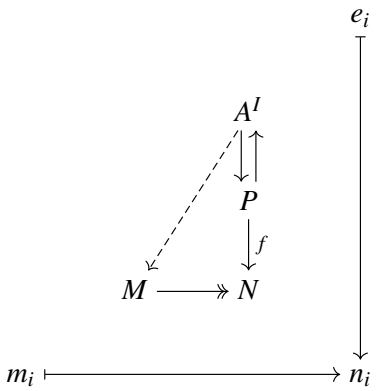


there exists a map g making the diagram commute.

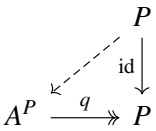
Such P are called projective modules.

Proof. We note that **(ii)** if and only if **(iii)** by definition. We then prove **(i)** implies **(iii)**. Let $A^I = P \oplus Q$. Then, we consider the following diagram. Here, we define a map $A^I \to M$ by choosing one element in the fiber of the

n_i's, then the result follows by considering $P \to A^I \to M$.



Lastly, we prove **(iii)** implies **(i)**. It is clear that we have a surjection $A^P \twoheadrightarrow P$ which yields the commutative diagram



We conclude then that $A^P \cong P \oplus \ker(q)$. □

We give some common examples of projective modules.

Example 3.43. Let A be a ring. Then, for any $n \in \mathbb{N}$, the module A^n (or even A itself) is free and hence, projective. To see why, every free module has a basis (recall from MA3201). Since every free module is isomorphic to a direct sum of copies of A, it is a direct summand of itself. This satisfies **(i)** of Theorem 3.19.

Example 3.44. If P is a direct summand of a free module F, then P is projective. For example, let Q be a module and $F = P \oplus Q$. Then, P is projective. Equivalently, this means that any module P that can be *split off* from a free module is projective, even if it is not free itself.

Example 3.45. Let $e \in A$ be idempotent, i.e. $e^2 = e$. Then, the left ideal eA is a projective A-module. To see why, the multiplication map

$$A \to eA \quad \text{where} \quad a \mapsto ea$$

admits a *splitting*[†] via the inclusion map, making eA a direct summand of A. This fulfils **(i)** of Theorem 3.19.

Proposition 3.31. Let A be a local Noetherian ring, and M a finitely generated projective A-module. Then $M \cong A^n$ for some n.

Proposition 3.32. Let A be Noetherian and M be a finitely generated A-module. Then,

$$M \text{ is projective} \quad \text{if and only if} \quad M_\mathfrak{p} \text{ is free for all } \mathfrak{p} \subseteq A.$$

It is a fact that for any domain that is integrally closed in its field of fractions, any fractional ideal is a projective module of rank 1. For Dedekind domains, this is easy to see because

$$I_\mathfrak{p} = \mathfrak{p}^n A\mathfrak{p} \cong A_\mathfrak{p}.$$

[†]By the term 'split', we mean that there exists another A-module homomorphism $\psi : eA \to A$ such that the composition $\varphi(\psi(x)) = x$ for all $x \in eA$, where $\varphi : A \to eA$. The splitting implies that $A = eA \oplus \ker\varphi$.

Proposition 3.33. If P and P' are projective modules, then $P \otimes P'$ is also projective. Moreover, if A is an integral domain and P and P' are finitely generated of rank n, then

$$\operatorname{rank}\left(P \otimes P'\right) = n \cdot n'.$$

Corollary 3.13. The collection of rank 1 projective modules form a monoid under $\otimes$. In fact, it is a group as the inverse of any projective module P is $\operatorname{Hom}_A(P,A)$. We denote this group by $\operatorname{Pic}(A)$, which is known as the Picard group.

In Corollary 3.13, a monoid is a set equipped with an associative binary operation and an identity element.

Theorem 3.20. For a Dedekind domain, A we have an isomorphism

$$\operatorname{Cl}(A) \cong \operatorname{Pic}(A) \quad \text{where} \quad I \mapsto [I].$$

3.12 Links with Algebraic Geometry

Now, we will draw some connections with Algebraic Geometry.

Definition 3.26 (finite type k-algebra)**.** Let k be a field. A k-algebra is of finite type if there exists

$$\text{a surjection} \quad k[x_1,\dots,x_n] \twoheadrightarrow A.$$

Proposition 3.34. If K is a field and a finite type k-algebra, then K is a finite field extension of k.

Proof. Suppose $x_1,\dots,x_n \in K$ generate K over k. We prove the statement by induction. For the base case, we have a surjection

$$k[X_1] \twoheadrightarrow K \quad \text{where} \quad X_1 \mapsto x.$$

As such, the kernel is non-empty. This implies that $K \cong k[X_1]/(f)$. Since f has finite degree, the corresponding field extension must also have finite degree.

Now suppose $n > 1$ and let $A = k[x_1] \subseteq K$, i.e. a subalgebra of K. Let $L = \operatorname{Frac}(A) \subseteq K$. Then we know that K is finitely generated by $x_2,\dots,x_n$ over L. By the induction hypothesis, K/L is a finite field extension. It remains to show that L/k is a finite field extension.

Since K/L is a finite extension, then there exist

$$\text{monic polynomials } f_2,\dots,f_n \in L[t] \quad \text{such that} \quad f_2(x_2) = 0,\dots,f_n(x_n) = 0.$$

Let $f \in A$ be the product of all the denominators (L is a field of fractions) of the coefficients of the f_i. Then $x_2,\dots,x_n$ are integral over A_f, which tells us that K is integral over A_f. As such, L is integral over A_f.

The goal now is to show that x_1 is algebraic over k. Assume on contrary that it is not, then $A \cong k[X_1]$ (as x_1 would be transcendental) but A is integrally closed so A_f is integrally closed. This forces $L = A_f$. However, this is impossible. Indeed, if $g \in A$ is irreducible and $g \nmid f$, then g is not invertible in A_f. However, $k[X_1]$ has

infinitely many irreducibles so one can always find such a g[†].

Therefore, x_1 is algebraic over k, so L/k is finite. By the tower theorem (recall this from MA4203), we conclude that K/k is finite. □

Theorem 3.21 (weak Nullstellensatz). Suppose $k = \bar{k}$, i.e. k is an algebraically closed field. Then, every maximal ideal of $k[x_1,\dots,x_n]$ is of the form

$$(x_1 - a_1,\dots,x_n - a_n) \quad \text{for some } (a_1,\dots,a_n) \in k^n.$$

Also, if $f_1,\dots,f_k \in k[x_1,\dots,x_n]$ are elements such that

$$V(f_1,\dots,f_k) = \emptyset \quad \text{then} \quad (f_1,\dots,f_k) = (1).$$

Example 3.46 (weak Nullstellensatz application). We work with the familiar polynomial ring $\mathbb{C}[x,y]$. In this ring, every maximal ideal is of the form $(x-a,y-b)$ for some $(a,b) \in \mathbb{C}^2$. Consider the maximal ideal

$$\mathfrak{m} = (x-1,y+2).$$

We briefly justify that the ideal is maximal. Consider the evaluation homomorphism

$$\mathrm{ev}_{(1,-2)} : \mathbb{C}[x,y] \to \mathbb{C} \quad \text{where} \quad f(x,y) \mapsto f(1,-2).$$

The kernel of this map is the set of all polynomials that vanish at $(1,-2)$, which is $(x-1,y+2)$. Recall from MA3201 that

$$\mathbb{C}[x,y]/(x-1,y+2) \cong \mathbb{C} \quad \text{where} \quad \mathbb{C} \text{ is a field.}$$

It follows that $(x-1,y+2)$ is a maximal ideal.

In an algebraically closed field, every maximal ideal *picks out* a single point in the space $\mathbb{C}^2$. Here, the maximal ideal corresponds to the point $(1,-2)$. Consider the polynomials $f(x,y) = x$ and $g(x,y) = 1-x$. Then, a point $(a,b) \in \mathbb{C}^2$ is a common zero if and only if $a = 0$ and $1-a = 0$. Clearly, no such a exists so theredoes not exist any point in $\mathbb{C}^2$ where both f and g vanish simultaneously.

Since $V(x,1-x) = \emptyset$, by the weak Nullstellensatz (Theorem 3.21), we have $(x,1-x) = (1)$, meaning to say that we can write the constant polynomial 1 as a linear combination of x and $1-x$, which holds trivially.

Theorem 3.22 (strong Nullstellensatz). Let k be an algebraically closed field.

(i) Algebraic version: If $f, f_1,\dots,f_k \in k[x_1,\dots,x_n]$ and

$$V(f) \supseteq V(f_1,\dots,f_k),$$

then there exists $d \in \mathbb{N}$ such that $f^d \in (f,f_1,\dots,f_k)$

(ii) Geometric version: There is a bijective correspondence between

$$\{\text{algebraic sets in } k^n\} \quad \text{and} \quad \{\text{radical ideals of } k[x_1,\dots,x_n]\}.$$

Here,

$$V(I) \leftarrow I \quad \text{and} \quad X \to I(X) = \{f : f(x) = 0 \text{ for } x \in X\}.$$

[†]Similar to Euclid's proof of the infinitude of primes.

Also, every radical ideal of I can be written as $\operatorname{rad}(I) = \{f \in R : f^d \in I\}$.

Proof. We use Rabinowitsch's trick. Consider $k[x_0, x_1, \ldots, x_n]$. Suppose

$$V(1 - x_0 \cdot f, f_1, \ldots, f_k) = \emptyset.$$

Then, by the weak Nullstellensatz (Theorem 3.21), there exist $g_0, g_1, \ldots, g_k \in k[x_0, x_1, \ldots, x_n]$ such that

$$1 = g_0(1 - x_0 f) \sum_{i=1}^{n} g_i f_i.$$

Consider

$$\varphi : k[x_0, x_1, \ldots, x_n] \to k[x_1, \ldots, x_n] \quad \text{where} \quad x_0 \mapsto 1/f \text{ and } x_i \mapsto x_i \text{ for all } 1 \leq i \leq n.$$

Then,

$$1 = \sum_{i=1}^{n} g_i\left(\frac{1}{f}, x_1, \ldots, x_n\right) f(x_1, \ldots, x_n) \quad \text{so} \quad f^d = \sum_{i=1}^{n} \widetilde{g}_i(x_1, \ldots, x_n) f_i(x_1, \ldots, x_n) \in (f_1, \ldots, f_n).$$

Here we multiplied by sufficiently large $d \in \mathbb{N}$ to clear denominators, so $f^d \in (f_1, \ldots, f_n)$. □

Theorem 3.23 (Noether normalisation theorem). Let k be a field and A be a finite k-algebra. Then, we can choose $n \in \mathbb{Z}_{\geq 0}$ and $x_1, \ldots, x_n \in A$ such that

$$k[X_1, \ldots, X_n] \hookrightarrow A \quad \text{where} \quad X_i \mapsto x_i$$

and A is finitely generated as a module over the image. In particular, A is integral over $k[x_1, \ldots, x_n]$.

Example 3.47 (application of Noether normalisation to a parabola). Consider the parabola defined by the equation $x = y^2$ and its coordinate ring $A = k[x, y] / (x - y^2)$. Because the relation $x = y^2$ holds in A, then every element can be expressed solely in terms of y. In fact,

$$\varphi : k[y] \cong k[x, y] / (x - y^2) \quad \text{where} \quad y \mapsto y$$

Hence, $A \cong k[y]$, which tells us that the parabola is isomorphic, as an algebraic variety, to the affine line. By Noether's normalisation theorem, we can choose the subalgebra $k[x]$ with $x = y^2$. Noether's normalisation theorem (Theorem 3.23) states that for any finitely generated k-algebra A, there exists a subalgebra isomorphic to a polynomial ring $k[t_1, \ldots, t_n]$ such that A is a finite module over this subalgebra. In our example, one natural choice is the subalgebra

$$k[x] \quad \text{with} \quad x = y^2.$$

The inclusion

$$k[x] \hookrightarrow A \quad \text{induces a morphism of spectra} \quad \pi : \operatorname{Spec}(A) \to \operatorname{Spec}(k[x]) \cong k.$$

Geometrically, this map corresponds to the projection of the parabola onto the x-axis. To see how this works, over a general point $x \neq 0$, the equation $x = y^2$ has two solutions $y = \sqrt{x}$ and $y = -\sqrt{x}$ (assuming we work over an algebraically closed field of characteristic not 2). So, for most x, there are two points on the parabola lying above x.

At the branch point $x = 0$, the equation becomes $0 = y^2$, which has a unique solution $y = 0$. Here the two sheets of the cover meet, and the map is not locally a homeomorphism. This is the branching behaviour described in the theorem.

Chapter 4
Introduction to Homology

4.1
Chain Complexes

Definition 4.1 (chain complex). A chain complex is a sequence of A-modules such that

$$C_\bullet : \ldots \to C_{n+1} \xrightarrow{d_{n+1}} C_n \xrightarrow{d_n} C_{n-1} \xrightarrow{d_{n-1}} \ldots \quad \text{such that} \quad d_n \circ d_{n+1} = 0 \text{ for all } n.$$

Note that the above condition is equivalent to saying that $\operatorname{im}(d_{n+1}) \subseteq \ker(d_n)$.

Definition 4.2 (cochain complex). A cochain complex is a sequence of A-modules such that

$$C^\bullet : \ldots \to C^n \xrightarrow{d^n} C^{n+1} \xrightarrow{d^{n+1}} C^{n+2} \xrightarrow{d^{n+2}} \ldots \quad \text{such that} \quad d^{n+1} \circ d^n = 0 \text{ for all } n.$$

Remark 4.1. If $C_\bullet$ is a chain complex, then

$$C^i = C_{-i} \quad \text{where} \quad d^i = d_{-i} \quad \text{is a chain complex.}$$

Definition 4.3 (morphism of chain complexes). We define a morphism of chain complexes to be as follows:

$$f_\bullet : C_\bullet \to D_\bullet \text{ is a collection of maps} \quad \text{and} \quad f_i : C_i \to D_i$$

such that the following diagram commutes for all i:

$$\begin{array}{ccc} C_i & \xrightarrow{d_i} & C_{i-1} \\ {\scriptstyle f_i}\downarrow & & \downarrow{\scriptstyle f_{i-1}} \\ D_i & \xrightarrow{d'_i} & D_{i-1} \end{array}$$

Definition 4.4 (homology and cohomology groups). Given a chain complex $C_\bullet$, its homology groups are the A-modules

$$H_n(C_\bullet) = \ker(d_n) / \operatorname{im}(d_{n+1}) \quad \text{which is indexed by } n \in \mathbb{Z}.$$

Similarly, given a cochain complex $C^\bullet$, its cohomology groups are the A-modules

$$H^n(C^\bullet) = \ker(d^n) / \operatorname{im}\left(d^{n-1}\right).$$

Note that if $f_\bullet : C_\bullet \to D_\bullet$ is a map of chain complexes, it induces maps

$$H_n(f_\bullet) : H_n(C_\bullet) \to H_n(D_\bullet)$$

by observing that $f_\bullet$ induces compatible maps

$$\begin{array}{ccc} \operatorname{im}\left(d_n^C\right) & \longrightarrow & \operatorname{im}\left(d_n^D\right) \\ \uparrow & & \uparrow \\ \operatorname{im}\left(d_{n+1}^C\right) & \longrightarrow & \operatorname{im}\left(d_{n+1}^D\right) \end{array}$$

A similar result holds for cochain complexes.

At this juncture, we will only discuss cochain complexes, but keep in mind that everything has an analogue for chain complexes.

Definition 4.5 (SES of chain complexes). A short exact sequence of chain complexes is a pair of maps of cochain complexes

$$L^\bullet \xrightarrow{f^\bullet} M^\bullet \xrightarrow{g^\bullet} N^\bullet$$

such that for all $n \in \mathbb{N}$, the sequence

$$0 \to L^n \xrightarrow{f^n} M^n \xrightarrow{g^n} N^n \to 0 \quad \text{is} \quad \text{a short exact sequence.}$$

Lemma 4.1 (Fundamental Lemma of Homological Algebra). Given a short exact sequence of cochain complexes

$$0 \to L^\bullet \xrightarrow{f^\bullet} M^\bullet \xrightarrow{g^\bullet} N^\bullet \to 0,$$

there exists a long exact sequence

$$\ldots \to H^{n-1}\left(N^\bullet\right) \xrightarrow{\delta} H^n\left(L^\bullet\right) \to H^n\left(M^\bullet\right) \to H^n\left(N^\bullet\right) \xrightarrow{\delta} H^{n+1}\left(L^\bullet\right) \to \ldots \quad \text{of } A\text{-modules.}$$

Proof. We start with a short exact sequence of cochain complexes, i.e.

$$0 \to L^\bullet \xrightarrow{f^\bullet} M^\bullet \xrightarrow{g^\bullet} N^\bullet \to 0,$$

meaning that for every n, the sequence

$$0 \to L^n \xrightarrow{f^n} M^n \xrightarrow{g^n} N^n \to 0$$

is exact, and the differentials d_L^n, d_M^n, and d_N^n commute with $f^\bullet$ and $g^\bullet$. That is,

$$f^{n+1} \circ d_L^n = d_M^n \circ f^n \quad \text{and} \quad g^{n+1} \circ d_M^n = d_N^n \circ g^n.$$

For each n, consider the following commutative diagram whose rows are short exact sequences:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & L^n & \xrightarrow{f^n} & M^n & \xrightarrow{g^n} & N^n & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle d_L^n} & & \downarrow{\scriptstyle d_M^n} & & \downarrow{\scriptstyle d_N^n} & & \\ 0 & \longrightarrow & L^{n+1} & \xrightarrow{f^{n+1}} & M^{n+1} & \xrightarrow{g^{n+1}} & N^{n+1} & \longrightarrow & 0 \end{array}$$

The vertical maps are the differentials of the complexes, and the horizontal maps are given by the inclusion f^n and the projection g^n. Because each row is exact and the diagram commutes, we can apply the snake lemma

(Lemma 2.1) to this diagram. The Snake Lemma yields a connecting homomorphism

$$\delta : \ker\left(d_N^n\right) / \operatorname{im}(g^{n-1}) \to \ker\left(d_L^{n+1}\right) / \operatorname{im}\left(d_L^n\right)$$

which, when interpreted in the language of cohomology, becomes

$$\delta : H^n\left(N^\bullet\right) \to H^{n+1}\left(L^\bullet\right).$$

More precisely, for an element $c \in H^n\left(N^\bullet\right)$ represented by $x \in N^n$ with $d_N^n(x) = 0$, we lift x to an element $y \in M^n$ (possible because g^n is surjective). Then, $d_M^n(y)$ maps to zero in N^{n+1} (by commutativity of the diagram) and hence, lies in the image of f^{n+1}. That is, there exists a unique $z \in L^{n+1}$ such that $f^{n+1}(z) = d_M^n(y)$. The class $[z] \in H^{n+1}(L^\bullet)$ is defined to be $\delta([x])$. One checks that this is well defined and independent of the choices made.

Collecting these connecting homomorphisms together with the induced maps on cohomology from $f^\bullet$ and $g^\bullet$, we obtain the long exact sequence

$$\cdots \to H^{n-1}\left(N^\bullet\right) \xrightarrow{\delta} H^n\left(L^\bullet\right) \longrightarrow H^n\left(M^\bullet\right) \longrightarrow H^n\left(N^\bullet\right) \xrightarrow{\delta} H^{n+1}\left(L^\bullet\right) \to \cdots.$$

The result follows. □

Definition 4.6 (homotopy). Suppose we are given

$$\text{maps } f^\bullet, g^\bullet : C^\bullet \to D^\bullet \quad \text{of} \quad \text{cochain complexes.}$$

A homotopy between $f^\bullet$ and $g^\bullet$ is

$$\text{a collection of } A\text{-module maps } k^n : C^n \to D^{n-1} \quad \text{such that} \quad f^n - g^n = d_D^{n-1} \circ h^n + h^{n+1} d_C^n.$$

Pictorally, the following diagram commutes:

$$\begin{array}{ccccccccc}
\cdots & \longrightarrow & C^n & \longrightarrow & C^{n+1} & \longrightarrow & \cdots \\
 & & \overset{h^n}{\swarrow} \downarrow & & \downarrow & & \\
\cdots & \longrightarrow & D^{n-1} & \longrightarrow & D^n & \longrightarrow & D^{n+1} & \longrightarrow & \cdots
\end{array}$$

Say

$$f^n \text{ and } g^n \text{ are homotopic} \quad \text{if} \quad \text{there exists a homotopy } h^\bullet \text{ between } f^\bullet \text{ and } g^\bullet.$$

Symbolically, we write $f^\bullet \sim g^\bullet$.

Remark 4.2. Being homotopic is an equivalence relation.

Proposition 4.1. If $f^\bullet, g^\bullet : C^\bullet \to D^\bullet$ are homotopic, then

$$H^n\left(f^\bullet\right) = H^n\left(g^\bullet\right) : H^n\left(C^\bullet\right) \to H^n\left(D^\bullet\right) \quad \text{are} \quad \text{equal as maps.}$$

Proof. We note that $H^n\left(f^\bullet\right)$ sits in the following diagram:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \operatorname{im}\left(d_C^{n-1}\right) & \longrightarrow & \ker\left(d_C^n\right) & \longrightarrow & H^n\left(C^\bullet\right) & \longrightarrow & 0 \\
 & & \text{induced by } f^{n-1} \downarrow & & f^n \downarrow & & \downarrow & & \\
0 & \longrightarrow & \operatorname{im}\left(d_D^{n-1}\right) & \longrightarrow & \ker\left(d_D^n\right) & \longrightarrow & H^n\left(D^\bullet\right) & \longrightarrow & 0
\end{array}$$

Pick $x \in H(C^\bullet)$ and a lift $\widetilde{x} \in \ker\left(d_C^n\right)$. Then,

$$H^n(f^\bullet)(\widetilde{x}) = \text{class of } f^n(\widetilde{x}) \quad \text{and} \quad H^n(g^\bullet)(\widetilde{x}) = \text{class of } g^n(\widetilde{x}).$$

However,

$$(f^n - g^n)(\widetilde{x}) = d_D^{n-1} \circ h^n(\widetilde{x}) + h^{n+1} \circ d_C^n(\widetilde{x}).$$

We know that $d_C^n(\widetilde{x}) = 0$, so $(f^n - g^n)(\widetilde{x}) \in d_D^{n-1}$. Thus, the class of $(f^n - g^n)(\widetilde{x})$ in $H^n(D^\bullet)$ is 0. □

Definition 4.7 (homotopy equivalence). Let $C^\bullet$ and $D^\bullet$ be chain complexes. We say that $C^\bullet$ and $D^\bullet$ are *homotopy-equivalent* if

$$\text{there exist maps of cochain complexes} \quad f^\bullet : C^\bullet \to D^\bullet \quad \text{and} \quad g^\bullet : D^\bullet \to C^\bullet$$

such that $f^\bullet \circ g^\bullet \sim \mathrm{id}_{D^\bullet}$ and $g^\bullet \circ f^\bullet \sim \mathrm{id}_{C^\bullet}$.

Given that $C^\bullet$ and $D^\bullet$ are homotopy equivalent via $f^\bullet : C^\bullet \leftrightarrows D^\bullet : g^\bullet$, we get induced isomorphisms

$$H^n(C^\bullet) \underset{H^n(g^\bullet)}{\overset{H^n(f^\bullet)}{\rightleftarrows}} H^n(D^\bullet)$$

Recall Theorem 3.19 where we defined projective modules.

Now, let M be an A-module. We claim that there exists an exact sequence

$$\ldots \to P_{i+1} \xrightarrow{d_{i+1}} P_i \xrightarrow{d_i} P_{i-1} \to \ldots \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\varepsilon} M \to 0$$

(possibly infinite on the left) where all the P_i's are projective A-modules. To prove this, we can pick $\varepsilon : P_0 \to M$ to be any surjection from a free A-module. Then we can pick $d_1 : P_1 \twoheadrightarrow \ker \varepsilon \subseteq P_0$ to be any surjection from a free A-module P_1. We can keep going inductively to obtain the desired sequence.

From this construction, we obtain a chain complex

$$P_\bullet : \ldots \to P_{i+1} \to P_i \to \ldots \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{0} 0 \quad \text{with} \quad \text{homology groups } H_i(P_\bullet) = \begin{cases} 0 & \text{if } i \neq 0; \\ M & \text{if } i = 0. \end{cases}$$

$P_\bullet$ is called a *projective resolution* of M.

Proposition 4.2. Suppose we are given an A-module map $f : M \to N$. Given projective resolutions

$$\begin{array}{ccccccccccccc}
\ldots & \longrightarrow & P_2 & \xrightarrow{d_2} & P_1 & \xrightarrow{d_1} & P_0 & \xrightarrow{\varepsilon} & M & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \varphi_2} & & \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_0} & & \downarrow{\scriptstyle f} & & \\
\ldots & \longrightarrow & Q_2 & \xrightarrow{d_2'} & \bullet & \xrightarrow{d_1'} & \bullet & \xrightarrow{\varepsilon'} & N & \longrightarrow & 0
\end{array}$$

there exist maps $\varphi_i : P_i \to Q_i$ such that $\varphi_\bullet : P_\bullet \to Q_\bullet$ is a map of chain complexes. Moreover, $\varphi_\bullet$ is unique up to homotopy.

Proof. We will only prove the existence of $\varphi_\bullet$ — the uniqueness claim is left as an exercise. For φ_0, we have the diagram

$$\begin{array}{ccc}
 & & P_0 \\
 & \overset{\varphi_0}{\swarrow} & \downarrow{\scriptstyle f \circ \varepsilon} \\
Q_0 & \xrightarrow{\varepsilon'} & N
\end{array}$$

Then φ_0 comes out by the definition of a projective modules.

Likewise for φ_i, consider the digram

$$\begin{array}{ccc} & & P_i \\ & \overset{\varphi_i}{\swarrow} & \downarrow{\scriptstyle \varphi_{i-1}\circ d_i} \\ Q_i & \xrightarrow[d_i']{} & \operatorname{im}(d_i') = \ker\left(d_{i-1}'\right) \end{array}$$

where φ_{i-1} is defined inductively. □

Proposition 4.3. Any two projective resolutions $P_\bullet$, $Q_\bullet$ of M are homotopy-equivalent.

Proposition 4.4. When A is Noetherian and M is a finitely generated A-module, there exists a projective resolution $P_\bullet$ of M with P_i a finitely generated free A-module for all i.

Definition 4.8 (torsion functor). Fix A-modules M and N. Define a sequence of A-modules $\operatorname{Tor}_i^A(M,N)$ indexed by $i \geq 0$ as follows:

(i) Pick $P_\bullet$ to be a projective resolution of M

(ii) Define

$$P_\bullet \otimes_A N : \ldots \to P_{i+1} \otimes_A N \xrightarrow{d_{i+1}\otimes \mathrm{id}_N} P_i \otimes_A N \xrightarrow{d_i \otimes \mathrm{id}_N} \to \ldots \quad \text{to be a chain complex}$$

(iii) Finally set $\operatorname{Tor}_i^A(M,N) = H_i(P_\bullet \otimes_A N)$ by definition