MA5204 Commutative and Homological Algebra

Thang Pang Ern

Reference books:

(1) Atiyah, M. and Macdonald, I. (1994). '*Introduction to Commutative Algebra*'. CRC Press.

(2) Matsumura, H. (1986). '*Commutative Ring Theory*'. Cambridge University Press.

Contents

1. Recap of 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 $R^\times = R \backslash \{0\}$.

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 $\overline{x} \cdot \overline{y} = 0$. This holds if and only if $xy \in I$. Equivalently, $x \in I$ or $y \in I$, i.e. $\overline{x} = 0$ or $\overline{y} = 0$. 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

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

The map is given by $J \mapsto J/I = \overline{J}$ such that $\overline{J} \mapsto \varphi^{-1}(\overline{J})$ 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

$$\mathfrak{p} \not\ni x^{n+m} = p_1p_2 + p_1zr_2 + p_2yr_1 + yzr_1r_2 \in yzr_1r_2 + \mathfrak{p}.$$

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,

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

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 $\varphi : \mathbb{Z} \hookrightarrow \mathbb{Q}$, the zero ideal is maximal in $\mathbb{Q}$, 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:

$$\begin{tikzcd} R \arrow[r, "\varphi"] \arrow[d] & S \arrow[d] \\ R/\varphi^{-1}(\mathfrak{p}) \arrow[r] & S/\mathfrak{p} \end{tikzcd}$$

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. $\square$

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 R to be the sets of the form $V(I) = \{\mathfrak{p} : I \subseteq \mathfrak{p}\}$. This defines a topology because

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

Definition 1.13 (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 1.13 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 $\mathfrak{a}\mathfrak{b}$ by **(i)** of Proposition 1.10 since $\mathfrak{a}\mathfrak{b}\subseteq\mathfrak{a}\cap\mathfrak{b}$ and both ideals generate the same radical in this case. So, $V(\mathfrak{a}\cap\mathfrak{b})=V(\mathfrak{a}\mathfrak{b})$.

Next, we note that a prime ideal $\mathfrak{p}$ contains $\mathfrak{a}\mathfrak{b}$ 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 $\mathcal{S} = \left\{X_{f_i} : i \in I\right\}$ 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 1.14 (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 1.15 (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 1.16 (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 1.15 can be generalised to multiple indeterminates.

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

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

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

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

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 1.17 (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. □

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

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

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 1.17, 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 1.18 (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 1.19 (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

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

Definition 1.20 (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 $i_1 m_1 + \cdots + i_j m_j$.

Example 1.25. If $M = R$ then we have $IR = I$.

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

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

(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 $\operatorname{im} f_i = \ker f_i$

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

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

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:

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

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 $f / \operatorname{im} f$.

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

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

[†]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.

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

$$\begin{aligned} R^n &\to M \to 0 \\ e_i &\mapsto x_i \end{aligned}$$

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 $1 \leq i \leq m$. 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

$$\begin{aligned} x - (b_1 y_1 + \ldots + b_m y_m) &= a_1 u(x_1) + a_n u(x_n) \\ x &= b_1 y_1 + \ldots + b_m y_m + a_1 u(x_1) + a_n u(x_n) \end{aligned}$$

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 $1 \leq i \leq n$. 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

$$\varphi(m) = a_1 e_1 + \ldots + a_n e_n \quad \text{where } a_1, \ldots, a_n \in A.$$

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

$$\begin{aligned} u &= a_1 u_1 + \ldots + a_n u_n \\ \varphi(u) &= a_1 \varphi(u_1) + a_n \varphi(u_n) \\ &= a_1 e_1 + \ldots + a_n e_n \end{aligned}$$

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

$$m = a_1 u_1 + \ldots + a_n u_n \quad \text{where } a_1, \ldots, a_n \in A.$$

Applying φ to both sides, we obtain $0 = a_1 e_1 + \ldots + a_n e_n$. 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. $\square$

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

$$\begin{tikzcd} 0 \arrow[r] & M' \arrow[r, "a"] \arrow[d, "f'"] & M \arrow[r, "b"] \arrow[d, "f"] & M'' \arrow[r] \arrow[d, "f''"] & 0 \\ 0 \arrow[r] & N' \arrow[r, "c"] & N \arrow[r, "d"] & N'' \arrow[r] & 0 \end{tikzcd}$$

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 $f(y) - f(y') \in \operatorname{im} c$. $\square$

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

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

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

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

Recall from MA2001 that

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

Hence,

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

As such, $\det\left(\mathbf{A}\right)x_i=0$ for all $1\le i\le n$. So, $\det\left(\mathbf{A}\right)=0$ in $\operatorname{Hom}_A\left(M,M\right)$. We conclude that $\det\left(\mathbf{A}\right)=\varphi^n+a_1\varphi^{n-1}+\ldots+a_n$, 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 $\operatorname{Hom}_A\left(M,M\right)$, 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 $I\subseteq J\left(A\right)$ be an ideal (recall that $J\left(A\right)$ 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, $I\subseteq J\left(A\right)$, which implies $a\in A^{\star}$. So, $M=a^{-1}\left(aM\right)=0$. □

Example 2.9. Let $A=\mathbb{Z}/4\mathbb{Z}$ and M be a finitely-generated A-module. Recall that the Jacobson radical $J\left(A\right)$ is the intersection of all maximal ideals $\mathfrak{m}$ of A, for which there is only one $\left(2\right)$. As such, $J\left(A\right)=2A$. Setting $I=J\left(A\right)$, we have $J\left(A\right)M=M$ 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 $J\left(A\right)$; 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 $L=N/u\left(M\right)$. We shall prove that $L=0$, i.e. $N=u\left(M\right)$,, 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. □

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 2.11. 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 $M = A/\left(x^2\right)$ as an A-module. The residue field is $k = A/\mathfrak{m}$. The module $M/\mathfrak{m}M = \left(A/\left(x^2\right)\right)/(x) = k$, 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 $A/\left(x^2\right)$ 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 2.12. For any ring A, the set of non-zero divisors is multiplicatively closed.

Example 2.13. For any $f \in A$, $\left\{1, f, f^2, \ldots\right\}$ is multiplicatively closed.

Example 2.14. 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:

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

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

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

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:

$$\begin{tikzcd}
A \arrow[r, "\varphi_S"] \arrow[dr, "\varphi_T"'] & S^{-1}A \arrow[d, dashed] \arrow[dr, "\varphi_{\varphi_S(T)}"] & \\
& T^{-1}A \arrow[r, dashed, "\sim"'] & \left(\varphi_S(T)\right)^{-1}S^{-1}A
\end{tikzcd}$$

Example 2.15. Choose $f \in A$ and take $S = \left\{1, f, f^2, \ldots\right\}$ 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 2.16. 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.