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

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 $S \cong R/I$. $\square$

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

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

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 $a_0b_0 = 1$, so a_0 is a unit in A. Recall the convolution formula that

$$fg = c_0 + c_1x + \ldots + c_kx^k,$$

where $c_0 = a_0b_0$ (discussed earlier),

$$c_1 = a_0b_1 + a_1b_0 = 0$$
$$c_2 = a_0b_2 + a_1b_1 + a_2b_0 = 0$$

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

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

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 $g = b_0 + b_1x + \ldots + b_mx^m$ such that $\deg g > 0$. Then, $a_nb_m = 0$, i.e. a_ng annihilates f but $\deg(a_ng) < m$, 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

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

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,

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

Multiplying both elements, we obtain

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

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 **??**, the set of prime ideals of A in Example 1.8 is actually called the prime spectrum of A or $\operatorname{Spec}(A)$.

1.2. *Module Theory*

2. **Basic Commutative Algebra**

3.