MA5204 Commutative and Homological Algebra

Thang Pang Ern

Reference books:

Contents

1. Recap

1.1. *Ring Theory and Module 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 $S \cong R/I$. $\square$

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 $\bar{x} \cdot \bar{y} = 0$. 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. $\square$

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

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

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

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. $\qquad \square$

> **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. $\qquad \square$

> **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.

> **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

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

which is 0 (*not surprising anyway*). $\qquad \square$

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

Example 1.6. 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, $\bar{x} \in A/\mathfrak{p}$ is nilpotent, so $\bar{x} = 0$ 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

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

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