

## Chapter 1: Rings and Ideals

*Author: Meng-Gen Tsai*

*Email: plover@gmail.com*

**Exercise 1.1.** *Let  $x$  be a nilpotent element of  $A$ . Show that  $1 + x$  is a unit of  $A$ . Deduce that the sum of a nilpotent element and a unit is a unit.*

*Proof.*

- (1) Suppose  $x^m = 0$  for some odd integer  $m \geq 0$ . Then

$$1 = 1 + x^m = (1 + x)(1 - x + x^2 - \cdots + (-1)^{m-1}x^{m-1}),$$

or  $1 + x$  is a unit.

- (2) If  $u$  is any unit and  $x$  is any nilpotent,  $u + x = u \cdot (1 + u^{-1}x)$  is a product of two units (using that  $u^{-1}x$  is nilpotent and applying (1)) and hence a unit again.

□

*Proof (Proposition 1.9).*

- (1) *The nilradical is a subset of the Jacobson radical.*

(a) The nilradical  $\mathfrak{N}$  of  $A$  is the intersection of all the prime ideals of  $A$  by Proposition 1.8.

(b) The Jacobson radical  $\mathfrak{J}$  of  $A$  is the intersection of all the maximal ideals of  $A$  by definition.

- (2) By Proposition 1.9,  $x \in \mathfrak{J}$  if and only if  $1 - xy$  is a unit in  $A$  for all  $y \in A$ . So  $1 + x = 1 - (-x) \cdot 1$  is a unit in  $A$  since  $x$  is a nilpotent and  $\mathfrak{J}$  is an ideal.

□

**Exercise 1.2.** *Let  $A$  be a ring and let  $A[x]$  be the ring of polynomials in an indeterminate  $x$ , with coefficients in  $A$ . Let  $f = a_0 + a_1x + \cdots + a_nx^n \in A[x]$ . Prove that*

- (i)  *$f$  is a unit in  $A[x]$  if and only if  $a_0$  is a unit in  $A$  and  $a_1, \dots, a_n$  are nilpotent. (Hint: If  $b_0 + b_1x + \cdots + b_mx^m$  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 Exercise 1.1.)*

- (ii)  $f$  is nilpotent if and only if  $a_0, a_1, \dots, a_n$  are nilpotent.
- (iii)  $f$  is a zero-divisor if and only if there exists  $a \neq 0$  such that  $af = 0$ . (Hint: Choose a polynomial  $g = b_0 + b_1x + \dots + b_mx^m$  of least degree  $m$  such that  $fg = 0$ . Then  $a_nb_m = 0$ , hence  $a_ng = 0$  (because  $a_ng$  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  $(a_0, a_1, \dots, a_n) = (1)$ . Prove that if  $f, g \in A[x]$ , then  $fg$  is primitive if and only if  $f$  and  $g$  are primitive.

*Proof of (i).*

- (1) ( $\Leftarrow$ ) holds by Exercise 1.1.
- (2) ( $\Rightarrow$ ) There exists the inverse  $g$  of  $f$ , say  $g = b_0 + b_1x + \dots + b_mx^m$  satisfying  $1 = fg$ . Clearly,  $1 = a_0b_0$ , or  $a_0$  is a unit in  $A$ . Also,

$$\begin{aligned} 0 &= a_nb_m, \\ 0 &= a_nb_{m-1} + a_{n-1}b_m, \\ 0 &= a_nb_{m-2} + a_{n-1}b_{m-1} + a_{n-2}b_m, \\ &\dots \end{aligned}$$

A direct computing shows that

$$\begin{aligned} 0 &= a_n^1b_m, \\ 0 &= a_n(a_nb_{m-1} + a_{n-1}b_m) \\ &= a_n^2b_{m-1} + a_{n-1}a_nb_m \\ &= a_n^2b_{m-1}, \\ 0 &= a_n^2(a_nb_{m-2} + a_{n-1}b_{m-1} + a_{n-2}b_m) \\ &= a_n^3b_{m-2} + a_{n-1}a_n^2b_{m-1} + a_{n-2}a_n^2b_m \\ &= a_n^3b_{m-2}, \\ &\dots \end{aligned}$$

So we might have  $a_n^{r+1}b_{m-r} = 0$  for  $r = 0, 1, 2, \dots, m$ .

- (3) Show that  $a_n^{r+1}b_{m-r} = 0$  for  $r = 0, 1, 2, \dots, m$  by induction on  $r$ .
  - (a) As  $r = 0$ ,  $a_nb_m = 0$  by comparing the coefficient of  $fg = 1$  at  $x^{n+m}$ .
  - (b) For any  $r > 0$ , comparing the coefficient of  $fg = 1$  at  $x^{n+m-r}$ ,

$$0 = a_nb_{m-r} + a_{n-1}b_{m-r+1} + \dots + a_{n-r}b_m.$$

Multiplying by  $a_n^r$  on the both sides,

$$\begin{aligned} 0 &= a_n^{r+1}b_{m-r} + a_{n-1}a_n^rb_{m-r+1} + \dots + a_{n-r}a_n^rb_m \\ &= a_n^{r+1}b_{m-r}. \end{aligned}$$

by the induction hypothesis.

- (4)  $a_n$  is a nilpotent. Putting  $r = m$  in  $a_n^{r+1}b_{m-r} = 0$  and get  $a_n^{m+1}b_0 = 0$ . Notice that  $b_0$  is a unit,  $a_n^{m+1} = 0$ , or  $a_n$  is a nilpotent.
- (5) Consider  $f - a_n x^n = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$ , a polynomial  $\in A[x]$  of degree  $n-1$ . Note that  $f$  is a unit and  $a_n x^n$  is a nilpotent. By Exercise 1.1,  $f - a_n x^n$  is a unit too. Applying the (2)(3)(4) again,  $a_{n-1}$  is a nilpotent as  $n-1 > 0$ , that is, applying descending induction on  $n$  then yields the desired property.

□

*Proof of (ii).*

- (1)  $(\Leftarrow)$  holds since the nilradical of any ring is an ideal.
- (2)  $(\Rightarrow)$   $f^N = 0$  for some  $N > 0$ . So  $0 = f^N = a_n^N x^{nN} + \cdots + a_0^N$ . Comparing the coefficient in the leading term  $x^{nN}$  leads to  $a_n^N = 0$ , or  $a_n$  is a nilpotent.
- (3) Consider  $f - a_n x^n = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$ , a polynomial  $\in A[x]$  of degree  $n-1$ . Note that  $f$  and  $a_n x^n$  are nilpotent.  $f - a_n x^n$  is a nilpotent too. Similar to step (5) in the proof of (i), applying descending induction on  $n$  then yields the desired property.

□

*Proof of (iii).*

- (1)  $(\Leftarrow)$  holds trivially.
- (2)  $(\Rightarrow)$  Pick a polynomial  $g = b_0 + b_1 x + \cdots + b_m x^m$  of least degree  $m$  such that  $fg = 0$ . Especially,  $a_n b_m = 0$ .
- (3) Consider

$$\begin{aligned} a_n g &= a_n b_0 + \cdots + a_n b_{m-1} x^{m-1} + a_n b_m x^m \\ &= a_n b_0 + \cdots + a_n b_{m-1} x^{m-1} \end{aligned}$$

(since  $a_n b_m = 0$ ).  $a_n g$  is a polynomial over  $A$  of having degree strictly less than  $m$ . Notice that  $f \cdot (a_n g) = a_n \cdot (fg) = 0$ . By minimality of  $m$ ,  $a_n g = 0$ .

- (4) Induction on the degree  $n$  of  $f$ .
- (a) As  $n = 0$ ,  $f = a_0$ . There exists  $b_m \neq 0$  such that  $b_m f = b_m a_0 = 0$  by (2).
- (b) For any zero-divisor  $f$  of degree  $n$ , there is a polynomial  $g = b_0 + b_1 x + \cdots + b_m x^m$  of least degree  $m$  such that  $fg = 0$ . By (2)(3),

$$\begin{aligned} (f - a_n x^n) \cdot g &= fg - a_n x^n g \\ &= 0 - 0 \\ &= 0. \end{aligned}$$

That is,  $f - a_n x^n$  is a zero-divisor of degree  $n - 1$ . By the induction hypothesis, there exists  $b_m \neq 0$  such that  $b_m(f - a_n x^n) = 0$ . So  $b_m f = b_m(f - a_n x^n) + b_m a_n x^n = 0 + 0 = 0$ .

(c) By (a)(b),  $(\implies)$  holds by mathematical induction.

□

*Proof of (iv).* Note that

- (1)  $f \notin \mathfrak{m}[x]$  for any maximal ideal  $\mathfrak{m}$  of  $A$  if and only if  $f$  is primitive.
- (2) For any maximal ideal  $\mathfrak{m}$  of  $A$ ,  $A/\mathfrak{m}$  is a field (or an integral domain).
- (3)  $A[x]$  is an integral domain if  $A$  is an integral domain.
- (4)  $A[x]/\mathfrak{m}[x] \cong (A/\mathfrak{m})[x]$  as a ring isomorphism.

Hence,

$$\begin{aligned}
 f, g : \text{primitive} &\iff f, g \notin \mathfrak{m}[x] \text{ for any maximal ideal } \mathfrak{m} \\
 &\iff f, g \neq 0 \text{ in } (A/\mathfrak{m})[x] \text{ for any maximal ideal } \mathfrak{m} \\
 &\iff fg \neq 0 \text{ in } (A/\mathfrak{m})[x] \text{ for any maximal ideal } \mathfrak{m} \\
 &\iff fg \notin \mathfrak{m}[x] \text{ for any maximal ideal } \mathfrak{m} \\
 &\iff fg : \text{primitive}.
 \end{aligned}$$

□

**Exercise 1.4.** *In the ring  $A[x]$ , the Jacobson radical is equal to the nilradical.*

*Proof.*

- (1) The nilradical  $\mathfrak{N}$  is a subset of the Jacobson radical  $\mathfrak{J}$ . It suffices to show that  $\mathfrak{J} \subseteq \mathfrak{N}$ .
- (2) Given any  $f \in \mathfrak{J}$ . By Proposition 1.9,  $f \in \mathfrak{J}$  if and only if  $1 - fy$  is a unit in  $A[x]$  for all  $y \in A[x]$ . Especially, pick  $y = x \in A[x]$  and then  $1 - xf$  is a unit in  $A[x]$ .
- (3) By Exercise 1.2 (i), all coefficients of  $f$  are nilpotent. By Exercise 1.2 (ii),  $f$  is nilpotent, or  $f \in \mathfrak{N}$ .

□

## The prime spectrum of a ring

**Exercise 1.15.** *Let  $A$  be a ring and let  $X$  be the set of all prime ideals of  $A$ . For each subset  $E$  of  $A$ , let  $V(E)$  denote the set of all prime ideals of  $A$  which contain  $E$ . Prove that*

- (i) if  $\mathfrak{a}$  is the ideal generated by  $E$ , then  $V(E) = V(\mathfrak{a}) = V(r(\mathfrak{a}))$ .
- (ii)  $V(0) = X$ ,  $V(1) = \emptyset$ .
- (iii) if  $(E_i)_{i \in I}$  is any family of subsets of  $A$ , then

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

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

The results 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  $\text{Spec}(A)$ .

Note that if  $E_1 \subseteq E_2$ , then  $V(E_1) \supseteq V(E_2)$ .

*Proof of (i).*

- (1) Show that  $V(E) = V(\mathfrak{a})$ .
  - (a) Show that  $V(E) \subseteq V(\mathfrak{a})$ . Given any  $\mathfrak{p} \in V(E)$ ,  $\mathfrak{p} \supseteq E$ . For any  $a \in \mathfrak{a}$ , since  $\mathfrak{a}$  is generated by  $E$ , we can write  $a$  as a finite sum  $a = \sum \alpha\beta$  where  $\alpha \in A$  and  $\beta \in E$ . Since  $E \subseteq \mathfrak{p}$ , all  $\beta \in \mathfrak{p}$ . Since  $\mathfrak{p}$  is an ideal,  $a = \sum \alpha\beta \in \mathfrak{p}$ . That is,  $\mathfrak{p} \supseteq \mathfrak{a}$ , or  $\mathfrak{p} \in V(\mathfrak{a})$ .
  - (b)  $V(E) \supseteq V(\mathfrak{a})$  since  $\mathfrak{a} \supseteq E$ .
- (2) Show that  $V(\mathfrak{a}) = V(r(\mathfrak{a}))$ .
  - (a) Show that  $V(\mathfrak{a}) \subseteq V(r(\mathfrak{a}))$ . Given any  $\mathfrak{p} \in V(\mathfrak{a})$ ,

$$\begin{aligned} \mathfrak{p} \in V(\mathfrak{a}) &\implies \mathfrak{p} \supseteq \mathfrak{a} \\ &\implies \mathfrak{p} \supseteq \text{the intersection of the prime ideals } \mathfrak{p} \supseteq \mathfrak{a} \\ &\implies \mathfrak{p} \supseteq r(\mathfrak{a}) \text{ (by Proposition 1.14)} \\ &\implies \mathfrak{p} \in V(r(\mathfrak{a})). \end{aligned}$$

- (b)  $V(\mathfrak{a}) \supseteq V(r(\mathfrak{a}))$  since  $r(\mathfrak{a}) \supseteq \mathfrak{a}$ .

□

*Proof of (ii).*

- (1)  $V(1) = \emptyset$  since no prime ideal contains 1 by definition.
- (2)  $V(0) = X$  since 0 is in every ideal (especially in every prime ideal).

□

*Proof of (iii).*

$$\begin{aligned}
\mathfrak{p} \in V\left(\bigcup_{i \in I} E_i\right) &\iff \mathfrak{p} \supseteq \bigcup_{i \in I} E_i \\
&\iff \mathfrak{p} \supseteq E_i \text{ for all } i \in I \\
&\iff \mathfrak{p} \in V(E_i) \text{ for all } i \in I \\
&\iff \mathfrak{p} \in \bigcap_{i \in I} V(E_i).
\end{aligned}$$

□

**Lemma.** *For any  $\mathfrak{p} \supseteq \mathfrak{a}\mathfrak{b}$ ,  $\mathfrak{p} \supseteq \mathfrak{a}$  or  $\mathfrak{p} \supseteq \mathfrak{b}$ .*

*Proof of Lemma.*

- (1) If  $\mathfrak{p} \supseteq \mathfrak{a}$ . We are done.
- (2) If  $\mathfrak{p} \not\supseteq \mathfrak{a}$ , there exists  $a \in \mathfrak{a} - \mathfrak{p}$ . So for any  $b \in \mathfrak{b}$ ,  $b \in \mathfrak{p}$  since  $ab \in \mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p}$  and  $\mathfrak{p}$  is a prime ideal, that is,  $\mathfrak{p} \supseteq \mathfrak{b}$ .

By (1)(2),  $\mathfrak{p} \supseteq \mathfrak{a}$  or  $\mathfrak{p} \supseteq \mathfrak{b}$ . □

*Proof of (iv).*

- (1) *Show that  $V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}\mathfrak{b})$ .*
  - (a)  $V(\mathfrak{a} \cap \mathfrak{b}) \subseteq V(\mathfrak{a}\mathfrak{b})$  since  $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$ .
  - (b) *Show that  $V(\mathfrak{a} \cap \mathfrak{b}) \supseteq V(\mathfrak{a}\mathfrak{b})$ .* Given any  $\mathfrak{p} \in V(\mathfrak{a}\mathfrak{b})$ ,  $\mathfrak{p} \supseteq \mathfrak{a}\mathfrak{b}$ . By Lemma,  $\mathfrak{p} \supseteq \mathfrak{a}$  or  $\mathfrak{p} \supseteq \mathfrak{b}$ . Notice that  $\mathfrak{a} \supseteq \mathfrak{a} \cap \mathfrak{b}$  and  $\mathfrak{b} \supseteq \mathfrak{a} \cap \mathfrak{b}$ . In any case,  $\mathfrak{p} \supseteq \mathfrak{a} \cap \mathfrak{b}$ ,  $\mathfrak{p} \in V(\mathfrak{a} \cap \mathfrak{b})$ .
- (2) *Show that  $V(\mathfrak{a}\mathfrak{b}) = V(\mathfrak{a}) \cup V(\mathfrak{b})$ .*
  - (a) *Show that  $V(\mathfrak{a}\mathfrak{b}) \subseteq V(\mathfrak{a}) \cup V(\mathfrak{b})$ .* Given any  $\mathfrak{p} \in V(\mathfrak{a}\mathfrak{b})$ ,  $\mathfrak{p} \supseteq \mathfrak{a}\mathfrak{b}$ . By Lemma,  $\mathfrak{p} \supseteq \mathfrak{a}$  or  $\mathfrak{p} \supseteq \mathfrak{b}$ ,  $\mathfrak{p} \in V(\mathfrak{a})$  or  $\mathfrak{p} \in V(\mathfrak{b})$ ,  $\mathfrak{p} \in V(\mathfrak{a}) \cup V(\mathfrak{b})$ .
  - (b) *Show that  $V(\mathfrak{a}\mathfrak{b}) \supseteq V(\mathfrak{a}) \cup V(\mathfrak{b})$ .* Given any  $\mathfrak{p} \in V(\mathfrak{a}) \cup V(\mathfrak{b})$ ,  $\mathfrak{p} \in V(\mathfrak{a})$  or  $\mathfrak{p} \in V(\mathfrak{b})$ ,  $\mathfrak{p} \supseteq \mathfrak{a}$  or  $\mathfrak{p} \supseteq \mathfrak{b}$ . Notice that  $\mathfrak{a} \supseteq \mathfrak{a}\mathfrak{b}$  and  $\mathfrak{b} \supseteq \mathfrak{a}\mathfrak{b}$ . In any cases,  $\mathfrak{p} \supseteq \mathfrak{a}\mathfrak{b}$ , or  $\mathfrak{p} \in V(\mathfrak{a}\mathfrak{b})$ .

□

**Exercise 1.17.** *For each  $f \in A$ , let  $X_f$  denote the complement of  $V(f)$  in  $X = \text{Spec}(A)$ . 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)  $X_f = \emptyset \iff f$  is nilpotent.
- (iii)  $X_f = X \iff f$  is a unit.
- (iv)  $X_f = X_g \iff r((f)) = r((g))$ .
- (v)  $X$  is quasi-compact (compact), that is, 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  $X = \text{Spec}(A)$ .

(Hint: To prove (v), remark that it is enough to consider a covering of  $X$  by basic open sets  $X_{f_i}$  ( $i \in I$ ). 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  $X_{f_i}$  ( $i \in J$ ) cover  $X$ .)

*Proof of basis.* It is equivalent to Exercise 1.15 (iii). Given any open set  $O$  in  $X$ . Write  $O = X - V(\mathfrak{a})$  for some ideal  $\mathfrak{a}$  of  $A$ . Since

$$V(\mathfrak{a}) = V\left(\bigcup_{f \in \mathfrak{a}} (f)\right) = \bigcap_{f \in \mathfrak{a}} V(f),$$

we have

$$O = X - V(\mathfrak{a}) = X - \bigcap_{f \in \mathfrak{a}} V(f) = \bigcup_{f \in \mathfrak{a}} (X - V(f)) = \bigcup_{f \in \mathfrak{a}} X_f,$$

or any open set is a union of basic open sets.  $\square$

*Proof of (i).*  $X_f \cap X_g = X_{fg} \iff V(f) \cup V(g) = V(fg)$  holds by Exercise 1.15 (iv).  $\square$

*Proof of (ii).*

$$\begin{aligned} X_f = \emptyset &\iff V(f) = X \\ &\iff f \in \mathfrak{p} \text{ for all prime ideal } \mathfrak{p} \text{ of } A \\ &\iff f \in \mathfrak{N}, \text{ the nilradical of } A \text{ (Proposition 1.8)} \\ &\iff f \text{ is nilpotent (Proposition 1.7)} \end{aligned}$$

□

*Proof of (iii).*

$$\begin{aligned} X_f = X &\iff V(f) = \emptyset \\ &\iff f \notin \mathfrak{p} \text{ for all prime ideal } \mathfrak{p} \text{ of } A \\ &\iff f \text{ is unit (Corollary 1.5)} \end{aligned}$$

□

*Proof of (v).* By (iii), it is a special case of (vi) as  $X_f = X_1 = X$ . □