

# Notes on the book: *Atiyah and Macdonald, Introduction to Commutative Algebra*

Meng-Gen Tsai  
plover@gmail.com

August 16, 2021

## Contents

<b>Chapter 1: Rings and Ideals</b>	<b>3</b>
Exercise 1.1. . . . .	3
Exercise 1.2. . . . .	3
Exercise 1.3. . . . .	6
Exercise 1.4. . . . .	7
Exercise 1.5. . . . .	7
Supplement 1.5.1. . . . .	9
Exercise 1.6. . . . .	10
Exercise 1.7. . . . .	11
Exercise 1.8. . . . .	11
Exercise 1.9. . . . .	12
Exercise 1.10. . . . .	12
Exercise 1.11. (Boolean ring) . . . . .	13
Exercise 1.12. . . . .	13
Construction of an algebraic closure of a field (E. Artin) . . . . .	14
Exercise 1.13. . . . .	14
Exercise 1.14. . . . .	15
The prime spectrum of a ring . . . . .	15
Lemma 1.15.1. . . . .	15
Exercise 1.15. . . . .	16
Exercise 1.16. . . . .	17
Exercise 1.17. . . . .	19
Exercise 1.18. . . . .	23
Exercise 1.19. . . . .	24
Exercise 1.20. . . . .	25
Exercise 1.21. . . . .	26
Exercise 1.22. . . . .	29

Exercise 1.23. . . . .	30
Exercise 1.24. (Boolean lattice) . . . . .	32
Exercise 1.25. (Stone's theorem) . . . . .	36
Exercise 1.26. (Maximal spectrum) . . . . .	36
Affine algebraic varieties . . . . .	38
Exercise 1.27. (Hilbert's Nullstellensatz) . . . . .	38
Exercise 1.28. . . . .	39
<b>Chapter 2: Modules</b>	<b>41</b>
Exercise 2.1. . . . .	41
Exercise 2.2. . . . .	43
Exercise 2.3. . . . .	44
Exercise 2.4. . . . .	45
Exercise 2.5. . . . .	46
Exercise 2.8. . . . .	47
Exercise 2.9. . . . .	47

## Chapter 1: Rings and Ideals

### 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  $g = b_0 + b_1x + \cdots + b_mx^m$  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  $g = b_0 + b_1x + \cdots + b_mx^m$  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  $x^{n+m-r}$ ,

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

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

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

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  $0 = f^N = a_0^N + \cdots + a_n^N x^{nN}$ . Compare the coefficient in the lowest term to get  $a_0^N = 0$ , or  $a_0$  is a nilpotent.
- (3) Note that  $f - a_0 = a_1 x + \cdots + a_n x^n \in A[x]$  is nilpotent since  $f$  and  $a_0$  are nilpotent.  $f - a_0$  is a nilpotent too. Continue the same argument in (2), the result is established.

□

*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 1.3.

Generalize the results of Exercise 1.2 to a polynomial ring  $A[x_1, \dots, x_r]$  in several indeterminates.

*Generalization.* Let

$$f = \sum_{(i)} a_{(i)} x^{(i)} \in A[x_1, \dots, x_r]$$

where  $\sum_{(i)}$  is the summation over  $(i) = (i_1, \dots, i_r)$  with  $i_1 + \dots + i_r = n$ . Then

- (i)  $f$  is a unit in  $A[x_1, \dots, x_r]$  if and only if  $a_{(0)}$  is a unit in  $A$  and all other  $a_{(i)}$  are nilpotent.
- (ii)  $f$  is nilpotent if and only if all  $a_{(i)}$  are nilpotent.
- (iii)  $f$  is a zero-divisor if and only if there exists  $a \neq 0$  such that  $af = 0$ .
- (iv) If  $f, g \in A[x_1, \dots, x_r]$ , then  $fg$  is primitive if and only if  $f$  and  $g$  are primitive.

*Proof.* Use the mathematical induction to prove (i)(ii)(iii) and apply the same argument in Exercise 1.2 (iv) to prove (iv).  $\square$

**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)

$$\begin{aligned}
 & f \in \mathfrak{J} \\
 \iff & 1 - fy \text{ is a unit in } A[x] \text{ for all } y \in A[x] && \text{(Proposition 1.9)} \\
 \implies & 1 - xf \text{ is a unit in } A[x] && (y = x) \\
 \implies & \text{All coefficients of } f \text{ are nilpotent} && \text{(Exercise 1.2 (i))} \\
 \implies & f \text{ is nilpotent} && \text{(Exercise 1.2 (ii))} \\
 \implies & f \in \mathfrak{N}.
 \end{aligned}$$

$\square$

**Exercise 1.5.**

*Let  $A$  be a ring and let  $A[[x]]$  be the ring of formal power series  $f = \sum_{n=0}^{\infty} a_n x^n$  with coefficients in  $A$ . Show that*

- (i)  *$f$  is a unit in  $A[[x]]$  if and only if  $a_0$  is a unit in  $A$ .*
- (ii) *If  $f$  is nilpotent, then  $a_n$  is nilpotent for all  $n \geq 0$ . Is converse true? (See Exercise 7.2.)*
- (iii)  *$f$  belongs to the Jacobson radical of  $A[[x]]$  if and only if  $a_0$  belongs to the Jacobson radical of  $A$ .*
- (iv) *The contraction of a maximal ideal  $\mathfrak{m}$  of  $A[[x]]$  is a maximal ideal of  $A$ , and  $\mathfrak{m}$  is generated by  $\mathfrak{m}^c$  and  $x$ .*
- (v) *Every prime ideal of  $A$  is the contraction of a prime ideal of  $A[[x]]$ .*

*Proof of (i).*

- (1) ( $\implies$ ) If  $g = \sum_{n=0}^{\infty} b_n x^n$  is an inverse of  $f$ , then  $fg = 1$  implies that  $a_0 b_0 = 1$  so that  $a_0$  is a unit in  $A$ .
- (2) ( $\impliedby$ ) Our goal is to find  $g = \sum_{n=0}^{\infty} b_n x^n$  such that the Cauchy product  $fg = \sum_{n=0}^{\infty} c_n x^n$  is equal to  $1 \in A[x]$ . Here  $c_n = \sum_{r=0}^n a_r b_{n-r}$ . By the assumption we have that  $c_0 = 1$  and  $c_1 = c_2 = \dots = 0$ . Hence

$$\begin{aligned} b_0 &= a_0^{-1} \\ b_1 &= -a_0^{-1} a_1 b_0 \\ &\dots \\ b_n &= a_0^{-1} \sum_{r=1}^n a_r b_{n-r} \\ &\dots \end{aligned}$$

by induction.

□

*Proof of (ii).*

- (1) The proof is the same as Exercise 1.2 (ii).
- (2) The converse is true if  $A$  is Noetherian (by Exercise 7.2).
- (3) The converse is not always true. Take

$$A = \mathbb{F}_2[t, t^{-2}, t^{-2^2}, \dots]/(t)$$

and

$$f(x) = \sum_{n=1}^{\infty} a_n x^n = \sum_{n=1}^{\infty} t^{-2^n} x^n \in A[x].$$

Note that  $A$  is not Noetherian and all  $a_n$  are nilpotent in  $A$ . To show  $f$  is not nilpotent in  $A[x]$ , it suffices to show that  $f^{2^r}$  is not equal to zero for all positive integers  $r$ .

- (4) Note that  $\mathbb{F}_2$  is a field of characteristic 2. So

$$f^{2^r} = \sum_{n=1}^{\infty} a_n^{2^r} x^n = \sum_{n=1}^{\infty} t^{2^{r-n}} x^n = \sum_{n=r+1}^{\infty} t^{2^{r-n}} x^n \neq 0$$

for all  $r$ .

□



*Proof of (iii).*

$$\begin{aligned}
& f \text{ in the Jacobson radical of } A[[x]] \\
& \iff 1 - fg \in A[[x]] \text{ is unit for all } g = \sum_{n=0}^{\infty} b_n x^n \in A[[x]] \quad (\text{Proposition 1.9}) \\
& \iff 1 - a_0 b_0 \in A \text{ is unit for all } b_0 \in A \quad ((i)) \\
& \iff a_0 \text{ belongs to the Jacobson radical of } A. \quad (\text{Proposition 1.9})
\end{aligned}$$

□

*Proof of (iv).*

- (1) Note that  $x = 0 + x$  belongs to the Jacobson radical of  $A[[x]]$  since 0 obviously belongs to the Jacobson radical of  $A$  (by (iii)).
- (2) So  $x \in \mathfrak{m}$  or  $(x) \subseteq \mathfrak{m}$  for any maximal ideal in  $A[[x]]$ . So it is clear that  $\mathfrak{m} = \mathfrak{m}^c + (x)$ .
- (3) Moreover,  $\mathfrak{m}^c$  is a maximal ideal since  $A/\mathfrak{m}^c \cong A[[x]]/\mathfrak{m}$  is a field.

□

*Proof of (v).*

- (1) Similar to (iv). Suppose  $\mathfrak{p}$  is a prime ideal of  $A$ . Let  $\mathfrak{q} = \mathfrak{p} + (x)$  be an ideal of  $A[[x]]$ .
- (2)  $\mathfrak{q}^c = \mathfrak{p}$  clearly. Besides,  $\mathfrak{q}^c$  is a prime ideal since

$$A[[x]]/\mathfrak{q}^c \cong A/\mathfrak{p}$$

is an integral domain.

□

### Supplement 1.5.1.

(Exercise II.1.2 in the textbook: Jrgen Neukirch, *Algebraic Number Theory*.) A  $p$ -adic integer  $a = a_0 + a_1 p + a_2 p^2 + \cdots$  is a unit in the ring  $\mathbb{Z}_p$  if and only if  $a_0 \neq 0$ .

*Proof.*

- (1) ( $\implies$ ) If  $b = b_0 + b_1 p + b_2 p^2 + \cdots$  is an inverse of  $a$ , then  $ab = 1$  implies that  $a_0 b_0 = 1$  so that  $a_0$  is a unit in  $\mathbb{Z}/p\mathbb{Z}$  or  $a_0 \neq 0$ .

(2) ( $\Leftarrow$ ) Our goal is to find

$$b = b_0 + b_1p + b_2p^2 + \cdots \in \mathbb{Z}_p$$

such that the Cauchy product

$$ab = c_0 + c_1p + c_2p^2 + \cdots$$

is equal to  $1 \in \mathbb{Z}_p$ . Here  $c_n = \sum_{\nu=0}^n a_\nu b_{n-\nu}$ . By the assumption we have that  $c_0 = 1$  and  $c_1 = c_2 = \cdots = 0$ . Hence

$$b_0 = a_0^{-1}$$

$$b_1 = -a_0^{-1}a_1b_0$$

$$\dots$$

$$b_n = a_0^{-1} \sum_{\nu=1}^n a_\nu b_{n-\nu}$$

$$\dots$$

by induction.

□

### Exercise 1.6.

*A ring  $A$  is such that every ideal not contained in the nilradical contains a nonzero idempotent (that is, an element  $e$  such that  $e^2 = e \neq 0$ ). Prove that the nilradical and Jacobson radical of  $A$  are equal.*

*Proof.*

(1)  $\mathfrak{N} \subseteq \mathfrak{J}$  clearly.

(2) Since

$$\begin{aligned} a \notin \mathfrak{N} &\implies (a) \not\subseteq \mathfrak{N} \\ &\implies \text{there exists a nonzero idempotent } e \in (a) \\ &\implies e = ar \text{ for some } r \in A \\ &\implies 0 = e - e^2 = e(1 - e) = ar(1 - ar) \\ &\implies 1 - ar \text{ is a zero-divisor, not a unit} \\ &\implies a \notin \mathfrak{J}, \end{aligned} \tag{Proposition 1.9}$$

we have  $\mathfrak{J} \subseteq \mathfrak{N}$ .

□

**Exercise 1.7.**

Let  $A$  be a ring in which every element satisfies  $x^n = x$  for some  $n > 1$  (depending on  $x$ ). Show that every prime ideal in  $A$  is maximal.

*Proof.* It suffices to show that for any prime ideal  $\mathfrak{p}$  in  $A$ ,  $A/\mathfrak{p}$  is a field.

- (1) Take any  $0 \neq \bar{x} \in A/\mathfrak{p}$ , which is represented by  $x \in A - \mathfrak{p}$ . By assumption there exists  $n \geq 2$  such that  $x^n = x$ . So  $\bar{x}^n = \bar{x}$  or  $\bar{x}(\bar{x}^{n-1} - 1) = 0$ .
- (2) Since  $\mathfrak{p}$  is prime,  $A/\mathfrak{p}$  is an integral domain. That is,  $\bar{x} = 0$  (impossible) or  $\bar{x}^{n-1} - 1 = 0$ . Write  $\bar{x} \cdot \bar{x}^{n-2} = 1$  in  $A/\mathfrak{p}$ . So  $\bar{x}^{n-2}$  is an inverse of  $\bar{x} \neq 0$  in  $A/\mathfrak{p}$ , which implies that  $A/\mathfrak{p}$  is a field (since  $\bar{x}$  is arbitrary).
- (3)  $A/\mathfrak{p}$  is a field if and only if  $\mathfrak{p}$  is maximal.

□

**Exercise 1.8.**

Let  $A$  be a ring  $\neq 0$ . Show that the set of prime ideals of  $A$  has minimal elements with respect to inclusion.

Similar to Theorem 1.3.

*Proof (Zorn's Lemma).*

- (1) Let  $\Sigma$  be the set of all prime ideals of  $A$ .
- (2) Order  $\Sigma$  by  $\supseteq$ , that is,  $\mathfrak{p} \leq \mathfrak{q}$  if  $\mathfrak{p} \supseteq \mathfrak{q}$ .
- (3)  $\Sigma$  is not empty, since every ring  $A \neq 0$  has at least one maximal ideal (or prime ideal) (Theorem 1.3).
- (4) To apply Zorn's lemma we must show that every chain in  $\Sigma$  has a lower bound in  $\Sigma$ ; let then  $(\mathfrak{p}_\alpha)$  be a chain of prime ideals in  $\Sigma$ , so that for each pair of indices  $\alpha, \beta$  we have either  $\mathfrak{p}_\alpha \subseteq \mathfrak{p}_\beta$  or  $\mathfrak{p}_\beta \subseteq \mathfrak{p}_\alpha$ . Let  $\mathfrak{p} = \bigcap_\alpha \mathfrak{p}_\alpha$ .
- (5) Show that  $\mathfrak{p}$  is a prime ideal. Clearly  $\mathfrak{p}$  is an ideal. Given any  $xy \in \mathfrak{p}$  and  $x \notin \mathfrak{p}$ . So  $xy$  is in all prime ideals  $\mathfrak{p}_\alpha$ . By assumption  $x \notin \mathfrak{p}$ , there is some  $\beta$  such that  $x \notin \mathfrak{p}_\beta$ , or  $x \notin \mathfrak{p}_\alpha$  whenever  $\alpha \geq \beta$ . So  $y \in \mathfrak{p}_\alpha$  whenever  $\alpha \geq \beta$ . Since  $y \in \mathfrak{p}_\beta$ ,  $y \in \mathfrak{p}_\gamma$  whenever  $\beta \geq \gamma$ . Therefore,  $y \in \mathfrak{p}_\alpha$  for all  $\alpha$ , or  $y \in \mathfrak{p}$ , or  $\mathfrak{p}$  is prime.

□

**Exercise 1.9.**

Let  $\mathfrak{a}$  be an ideal  $\neq (1)$  in a ring  $A$ . Show that  $\mathfrak{a} = r(\mathfrak{a}) \iff \mathfrak{a}$  is an intersection of prime ideals.

*Proof.*

- (1)  $(\implies)$ . By Proposition 1.14,  $\mathfrak{a} = r(\mathfrak{a})$  is the intersection of the prime ideals which contain  $\mathfrak{a}$ .
- (2)  $(\impliedby)$ .

$$\begin{aligned}
 \mathfrak{a} &= \bigcap \{\mathfrak{p} \in \text{some subset of } \text{Spec}(A)\} \\
 &= \bigcap \{\mathfrak{p} \in \text{some subset of } \text{Spec}(A) : \mathfrak{p} \supseteq \mathfrak{a}\} \\
 &\supseteq \bigcap \{\mathfrak{p} \in \text{Spec}(A) : \mathfrak{p} \supseteq \mathfrak{a}\} \\
 &= r(\mathfrak{a}) \\
 &\supseteq \mathfrak{a}.
 \end{aligned}$$

□

**Exercise 1.10.**

Let  $A$  be a ring,  $\mathfrak{N}$  its nilradical. Show 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.

*Proof.*

$$\begin{aligned}
 &A/\mathfrak{N} \text{ is a field} \\
 \implies &\mathfrak{N} \text{ is a maximal ideal} \\
 \implies &\mathfrak{p} = \mathfrak{N} \text{ for every prime ideal } \mathfrak{p} && (\text{Proposition 1.8}) \\
 \implies &A \text{ has exactly one prime ideal } \mathfrak{p} \\
 \implies &\mathfrak{p} = \mathfrak{N} \\
 \implies &A \text{ has exactly one maximal ideal } \mathfrak{p} \\
 \implies &\text{Given any } a \in A, a \text{ is a unit or } a \in \mathfrak{p} = \mathfrak{N}. && (\text{Corollary 1.5}) \\
 \implies &A/\mathfrak{N} \text{ is a field.}
 \end{aligned}$$

□

**Exercise 1.11. (Boolean ring)**

A ring  $A$  is **Boolean** if  $x^2 = x$  for all  $x \in A$ . In a Boolean ring  $A$ , show that

- (i)  $2x = 0$  for all  $x \in A$ ;
- (ii) every prime ideal  $\mathfrak{p}$  is maximal, and  $A/\mathfrak{p}$  is a field with two elements;
- (iii) every finitely generated ideal in  $A$  is principal.

*Proof of (i).* Note that  $2x = x + x = (x + x)^2 = (2x)^2 = 4x^2 = 4x$ . So  $2x = 0$ .  $\square$

*Proof of (ii).* Same as Exercise 1.7 with  $n = 2$ .  $\square$

*Proof of (iii).*

- (1) By induction, it suffices to show that if  $\mathfrak{a} = (x, y)$  is an ideal in  $A$ , then  $\mathfrak{a} = (z)$  for some  $z \in A$ .
- (2) Take  $z = x + y + xy$ .  $(z) \subseteq \mathfrak{a}$  obviously.
- (3) Conversely, note that

$$x = x^2 = x(z - y - xy) = xz - \overbrace{xy}^{=2xy=0} - \underbrace{x^2y}_{=xy} = xz \in (z).$$

Also  $y \in (z)$  similarly. So  $\mathfrak{a} \subseteq (z)$  and thus  $\mathfrak{a} = (z)$  is principal.

$\square$

**Exercise 1.12.**

A local ring contains no idempotent  $\neq 0, 1$ .

*Proof.*

- (1) If  $e$  is an idempotent  $\neq 0, 1$  in a local ring  $A$  with the maximal ideal  $\mathfrak{m}$ , then by definition  $0 = e(1 - e)$  shows that both  $e \neq 0$  and  $1 - e \neq 0$  are not unit.
- (2) Thus  $e \in \mathfrak{m}$  and  $1 - e \in \mathfrak{m}$ . So  $1 = (1 - e) + e$  is a unit in  $\mathfrak{m}$ , which is absurd.

$\square$

## Construction of an algebraic closure of a field (E. Artin)

### Exercise 1.13.

Let  $K$  be a field and let  $\Sigma$  be the set of all irreducible monic polynomials  $f$  in one indeterminate with coefficients in  $K$ . Let  $A$  be the polynomial ring over  $K$  generated by indeterminates  $x_f$ , one for each  $f \in \Sigma$ . Let  $\mathfrak{a}$  be the ideal of  $A$  generated by the polynomials  $f(x_f)$  for all  $f \in \Sigma$ . Show that  $\mathfrak{a} \neq (1)$ .

Let  $\mathfrak{m}$  be a maximal ideal of  $A$  containing  $\mathfrak{a}$  and let  $K_1 = A/\mathfrak{m}$ . Then  $K_1$  is an extension field of  $K$  in which each  $f \in \Sigma$  has a root. Repeat the construction with  $K_1$  in place of  $K$ , obtaining a field  $K_2$ , and so on. Let  $L = \bigcup_{n=1}^{\infty} K_n$ . Then  $L$  is a field in which each  $f \in \Sigma$  splits completely into linear factors. Let  $\overline{K}$  be the set of all elements of  $L$  which are algebraic over  $K$ . Then  $\overline{K}$  is an algebraic closure of  $K$ .

*Proof.*

- (1) Show that  $\mathfrak{a} \neq (1)$ . (Reductio ad absurdum) If  $\mathfrak{a} = (1)$ , then we can write

$$1 = \sum_{i=1}^n g_i(x) f_i(x_{f_i}) \in A$$

where  $x = (x_{f_1}, \dots, x_{f_n}, x_{g_1}, \dots, x_{g_r})$  is a tuple with finitely many indeterminates. It is possible since it is a finite sum.

- (2) Let  $L$  be an algebraic extension of  $K$  such that each  $f_i$  has a root  $a_i \in L$  ( $i = 1, \dots, n$ ).
- (3) Take  $x = (a_1, \dots, a_n, 0, \dots, 0)$  in the equation  $1 = \sum_{i=1}^n g_i(x) f_i(x_{f_i})$  to get

$$\begin{aligned} 1 &= \sum_{i=1}^n g_i(a_1, \dots, a_n, 0, \dots, 0) f_i(a_i) \\ &= \sum_{i=1}^n g_i(a_1, \dots, a_n, 0, \dots, 0) \cdot 0 \\ &= 0, \end{aligned}$$

which is absurd.

□

**Exercise 1.14.**

In a ring  $A$ , let  $\Sigma$  be the set of all ideals in which every element is a zero-divisor. Show that the set  $\Sigma$  has maximal elements and that every maximal element of  $\Sigma$  is a prime ideal. Hence the set of zero-divisors in  $A$  is a union of prime ideals.

*Proof.*

- (1) Suppose  $1 \neq 0$ .
- (2) Show that the set  $\Sigma$  has maximal elements. Order  $\Sigma$  by inclusion.  $\Sigma$  is not empty, since  $0 \in \Sigma$ . To apply Zorn's lemma we must show that every chain in  $\Sigma$  has an upper bound in  $\Sigma$ ; let then  $(\mathfrak{a}_\alpha)$  be a chain of ideals in  $\Sigma$ , so that for each pair of indices  $\alpha, \beta$  we have either  $\mathfrak{a}_\alpha \subseteq \mathfrak{a}_\beta$  or  $\mathfrak{a}_\beta \subseteq \mathfrak{a}_\alpha$ .
- (3) Let  $\mathfrak{a} = \bigcup_\alpha \mathfrak{a}_\alpha$ . Then  $\mathfrak{a}$  is an ideal and every element of  $\mathfrak{a}$  is a zero-divisor. Hence  $\mathfrak{a} \in \Sigma$ , and  $\mathfrak{a}$  is an upper bound of the chain. Hence by Zorn's lemma,  $\Sigma$  has maximal elements.
- (4) Show that every maximal element of  $\Sigma$  is a prime ideal. Let  $\mathfrak{p}$  be a maximal element in  $\Sigma$ . Suppose  $x, y \notin \mathfrak{p}$ . Then there are non-zero-divisors in  $\mathfrak{p} + (x)$  and  $\mathfrak{p} + (y)$ , and their product is an element of  $\mathfrak{p} + (xy)$  that is again a non-zero-divisor. So  $xy \notin \mathfrak{p}$ .
- (5) Hence the set of zero-divisors in  $A$  is a union of prime ideals (by the construction in (2) and the result of (4)).

□

**The prime spectrum of a ring****Lemma 1.15.1.**

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

*Proof.*

- (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  $\mathfrak{p} \supseteq \mathfrak{b}$ . □

**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).*

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

□

*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 15.1.1,  $\mathfrak{p} \supseteq \mathfrak{a}$  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 15.1.1,  $\mathfrak{p} \supseteq \mathfrak{a}$  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 1.16.

*Draw pictures of  $\text{Spec}(\mathbb{Z})$ ,  $\text{Spec}(\mathbb{R})$ ,  $\text{Spec}(\mathbb{C}[x])$ ,  $\text{Spec}(\mathbb{R}[x])$ ,  $\text{Spec}(\mathbb{Z}[x])$ .*

*Proof.*

- (1) *Show that  $\text{Spec}(\mathbb{Z}) = \{(0)\} \cup \{(p) : p \text{ is a rational prime}\}$ .* Note that  $\mathbb{Z}$  is a PID. So all non-trivial prime ideals are of the form  $(\pi)$  where  $\pi$  are irreducible.

- (2) Show that  $\text{Spec}(\mathbb{R}) = \{(0)\}$ . Note that  $\mathbb{R}$  is a field.
- (3) Show that  $\text{Spec}(\mathbb{C}[x]) = \{(0)\} \cup \{(x - z) : z \in \mathbb{C}\}$ . Note that  $\mathbb{C}[x]$  is a PID and  $\mathbb{C}$  is algebraically closed. Hence all non-trivial prime ideals are of the form  $(x - z)$  where  $z \in \mathbb{C}$ .
- (4) Show that  $\text{Spec}(\mathbb{R}[x])$  are
- (i)  $(0)$ .
  - (ii)  $\{(x - r) : r \in \mathbb{R}\}$ .
  - (iii)  $\{(x - z)(x - \bar{z}) : z \in \mathbb{C}, \text{Im}(z) > 0\}$ .

Here is the proof.

- (a) Note that  $\mathbb{R}[x]$  is a PID and all non-trivial prime ideals are of the form  $(f)$  where  $f$  are irreducible. Might assume  $f$  is monic. By the fundamental theorem of algebra,  $f$  has a root  $z \in \mathbb{C}$ .
  - (b) The case  $r := z \in \mathbb{R}$ .  $x - r$  is a factor of  $f$ . Hence  $f = x - r$ .
  - (c) The case  $z \in \mathbb{C} \setminus \mathbb{R}$ . Since the conjugate of  $f$  is also in  $\mathbb{R}[x]$ ,  $\bar{z}$  is also a root of  $f$ . So  $(x - z)(x - \bar{z}) \in \mathbb{R}[x]$  is an irreducible factor of  $f$ . Hence  $f = (x - z)(x - \bar{z})$  by the irreducibility of  $f$ .
- (5) Show that  $\text{Spec}(\mathbb{Z}[x])$  are
- (i)  $(0)$ .
  - (ii)  $(p)$  where  $p$  are rational primes.
  - (iii)  $(f)$  where  $f \in \mathbb{Z}[x]$  are irreducible.
  - (iv)  $(p, f)$  where  $p$  are rational primes and  $f \in \mathbb{Z}[x]$  are irreducible when viewed in  $\mathbb{F}_p[x]$ .

Before giving a proof, it is worth taking a look at the book: *David Mumford, The red book of varieties and schemes*.

- (a) Let  $\phi : \mathbb{Z} \rightarrow \mathbb{Z}[x]$  be the natural inclusion map. Hence  $\phi^* : \text{Spec}(\mathbb{Z}[x]) \rightarrow \text{Spec}(\mathbb{Z})$  is continuous (Exercise 1.21). Suppose  $\mathfrak{P} \in \text{Spec}(\mathbb{Z}[x])$ , then  $\phi^*(\mathfrak{P}) = (0)$  or  $(p)$  where  $p$  is a rational prime.
- (b) The case  $\phi^*(\mathfrak{P}) = (0)$ . A non-trivial prime ideal  $\mathfrak{P}$  must be generated by a set of nonconstant polynomials which, since  $\mathfrak{P}$  is prime, may be assumed to be irreducible in  $\mathbb{Z}[x]$ . Note that  $\mathbb{Z}[x]$  is not a PID.
- (c) By Gauss' lemma, these polynomials are also irreducible in  $\mathbb{Q}[x]$ . Since  $\mathbb{Q}[x]$  is a Euclidean domain, if there are at least two distinct irreducible polynomials  $f, g$  generating  $\mathfrak{P}$ , then  $1 = af + bg$  for some  $a, b \in \mathbb{Q}[x]$ . Clearing all denominators to get that  $n = \tilde{a}f + \tilde{b}g$  for some  $\tilde{a}, \tilde{b} \in \mathbb{Z}[x]$  and some  $n \in \mathbb{Z} \setminus \{0\}$ , contrary to  $\phi^*(\mathfrak{P}) = (0)$ . Therefore,  $\mathfrak{P} = (f)$  for one irreducible polynomial  $f \in \mathbb{Z}[x]$ .

(d) The case  $\phi^*(\mathfrak{P}) = (p)$  where  $p$  is a rational prime. Note that

$$\begin{aligned}\mathbb{Z}[x]/\mathfrak{P} &\cong (\mathbb{Z}[x]/p\mathbb{Z}[x]) / (\mathfrak{P}/p\mathbb{Z}[x]) \\ &\cong \underbrace{(\mathbb{Z}/p\mathbb{Z})}_{:=\mathbb{F}_p}[x] / (\mathfrak{P}/p\mathbb{Z}[x])\end{aligned}$$

is an integral domain (since  $\mathfrak{P}$  is prime). So  $\mathfrak{P}/p\mathbb{Z}[x]$  is a prime ideal in  $\mathbb{F}_p[x]$ . Note that  $\mathbb{F}_p[x]$  is a PID and all non-trivial prime ideals are of the form  $(f)$  where  $f$  are irreducible.

(e) As  $\mathfrak{P}/p\mathbb{Z}[x] = (0)$ ,  $\mathfrak{P} = p\mathbb{Z}[x] = (p) \in \mathbb{Z}[x]$ .

(f) As  $\mathfrak{P}/p\mathbb{Z}[x] = (f)$  where  $f \in \mathbb{Z}[x]$  is irreducible when viewed in  $\mathbb{F}_p[x]$ ,  $\mathfrak{P} = (p, f)$ .

□

### 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).*

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

$\square$

*Proof of (ii) (Using (iv)).*

$$\begin{aligned} X_f = \emptyset &\iff X_f = X_0 && \text{(Exercise 15(ii))} \\ &\iff r(f) = r(0) && \text{((iv))} \\ &\iff f \in r(f) = r(0) \\ &\iff f^m = 0 \text{ for some } m > 0 \\ &\iff f \text{ is nilpotent} \end{aligned}$$

$\square$

*Proof of (iii).*

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

$\square$

*Proof of (iii)(Using (iv)).*

$$\begin{aligned}
X_f = X &\iff X_f = X_1 && \text{(Exercise 15(ii))} \\
&\iff r(f) = r(1) && \text{((iv))} \\
&\iff f \in r(f) = r(1) \\
&\iff f^m = 1 \text{ for some } m > 0 \\
&\iff f \text{ is unit}
\end{aligned}$$

□

*Proof of (iv).*

(1) *Show that  $X_f \subseteq X_g \iff r((f)) \subseteq r((g))$ . Actually,*

$$\begin{aligned}
X_f \subseteq X_g &\implies V(f) \supseteq V(g) \\
&\implies \{\mathfrak{p} \in \text{Spec}(A) : \mathfrak{p} \supseteq (f)\} \supseteq \{\mathfrak{p} \in \text{Spec}(A) : \mathfrak{p} \supseteq (g)\} \\
&\implies \bigcap_{(f) \subseteq \mathfrak{p} \in \text{Spec}(A)} \mathfrak{p} \subseteq \bigcap_{(g) \subseteq \mathfrak{p} \in \text{Spec}(A)} \mathfrak{p} \\
&\stackrel{1.14}{\implies} r(f) \subseteq r(g) \\
&\implies V(r(f)) \supseteq V(r(g)) \\
&\implies V(f) \supseteq V(g) \\
&\implies X_f \subseteq X_g.
\end{aligned}$$

(2) By (1),

$$\begin{aligned}
X_f \subseteq X_g &\iff r((f)) \subseteq r((g)), \\
X_f \supseteq X_g &\iff r((f)) \supseteq r((g)).
\end{aligned}$$

Hence,

$$X_f = X_g \iff r((f)) = r((g)).$$

□

*Proof of (v).* Notice that it is enough to consider a covering of  $X$  by basic open sets  $X_{f_i}$  ( $i \in I$ ).

(1) Since  $X$  is covered by  $X_{f_i} (i \in I)$ ,

$$\begin{aligned}
X = \bigcup_{i \in I} X_{f_i} &\implies X - V(1) = \bigcup_{i \in I} (X - V(f_i)) \\
&\implies V(1) = \bigcap_{i \in I} V(f_i) \\
&\implies V(1) = V\left(\sum_{i \in I} f_i\right) \\
&\implies r(1) = r\left(\sum_{i \in I} f_i\right).
\end{aligned}$$

Hence,  $1 \in r(1) = r\left(\sum_{i \in I} f_i\right)$  can be expressed as

$$1 = 1^m = \sum_{j \in J} g_j f_j$$

where  $J$  is a finite subset of  $I$  and  $g_j \in A$ . That is,  $(1) = \sum_{j \in J} f_j$ .

(2) Hence,  $V(1) = V\left(\sum_{j \in J} f_j\right)$ . Therefore,  $X$  is covered by finite subcovering  $\{X_{f_j}\} (j \in J)$ .

□

*Proof of (v)(Using (vi)).* Since  $X = X_1$ ,  $X$  is quasi-compact by (vi). □

*Proof of (vi).* Notice that it is enough to consider a covering of  $X_f$  by basic open sets  $X_{f_i} (i \in I)$ .

(1) Since  $X_f$  is covered by  $X_{f_i} (i \in I)$ ,

$$\begin{aligned}
X_f = \bigcup_{i \in I} X_{f_i} &\implies X - V(f) = \bigcup_{i \in I} (X - V(f_i)) \\
&\implies V(f) = \bigcap_{i \in I} V(f_i) \\
&\implies V(f) = V\left(\sum_{i \in I} f_i\right) \\
&\implies r(f) = r\left(\sum_{i \in I} f_i\right).
\end{aligned}$$

Hence,  $f \in r(f) = r\left(\sum_{i \in I} f_i\right)$  can be expressed as

$$f^m = \sum_{j \in J} g_j f_j$$

where  $J$  is a finite subset of  $I$  and  $g_j \in A$ . That is,  $f^m \in \sum_{j \in J} f_j$ .

(2) Show that  $V\left(\sum_{j \in J} f_j\right) = V(f)$ .

(a)  $(\subseteq)$  For any prime ideal  $\mathfrak{p} \supseteq \sum_{j \in J} f_j$ ,  $f^m \in \mathfrak{p}$  or  $f \in \mathfrak{p}$  (since  $\mathfrak{p}$  is prime). So  $\mathfrak{p} \supseteq (f)$ , or  $V\left(\sum_{j \in J} f_j\right) \subseteq V(f)$ .

(b)  $(\supseteq)$

$$\sum_{j \in J} f_j \subseteq \sum_{i \in I} f_i \implies V\left(\sum_{j \in J} f_j\right) \supseteq V\left(\sum_{i \in I} f_i\right) = V(f).$$

(3) Therefore,  $X_f$  is covered by finite subcovering  $\{X_{f_j}\}(j \in J)$ .

□

*Proof of (vi) (Using (v)).* Exercise 3.21 (i) shows that  $X_f$  is the spectrum of  $A_f$ . By (v),  $X_f$  is quasi-compact. □

*Proof of (vii).*

(1)  $(\implies)$  Given an open subset  $O$ . Since  $X_f$  form a basis of open sets,

$$O = \bigcup_{f \in \mathfrak{a}} X_f \text{ for some ideal } \mathfrak{a} \text{ of } A$$

Especially,  $\{X_f\}_{f \in \mathfrak{a}}$  is an open covering of  $O$ . Since  $O$  is quasi-compact, there exists a finite subcovering  $\{X_f\}_{f \in J}$  of  $O$ , where  $J$  is a finite subset of  $\mathfrak{a}$  (as a set). That is,  $O = \bigcup_{f \in J} X_f$  is a finite union of sets  $X_f$ .

(2)  $(\impliedby)$  Since  $X_f$  is quasi-compact, any finite union of quasi-compact sets is quasi-compact again.

□

### Exercise 1.18.

For psychological reasons it is sometimes convenient to denote a prime ideal of  $A$  by a letter such as  $x$  or  $y$  when thinking of it as a point of  $X = \text{Spec}(A)$ . When thinking of  $x$  as a prime ideal of  $A$ , we denote it by  $\mathfrak{p}_x$  (logically, of course, it is the same thing). Show that

- (i) The set  $\{x\}$  is closed (we say that  $x$  is a “closed point”) in  $\text{Spec}(A)$  if and only if  $\mathfrak{p}_x$  is maximal;
- (ii)  $\overline{\{x\}} = V(\mathfrak{p}_x)$ ;
- (iii)  $y \in \overline{\{x\}}$  if and only if  $\mathfrak{p}_x \subseteq \mathfrak{p}_y$ ;

- (iv)  $X$  is a  $T_0$ -space (this means that if  $x, y$  are distinct points of  $X$ , then either there is a neighborhood of  $x$  which does not contain  $y$ , or else there is a neighborhood of  $y$  which does not contain  $x$ ).

*Proof of (i).*

$$\{x\} = \overline{\{x\}} \stackrel{(ii)}{\iff} \{x\} = V(\mathfrak{p}_x) \iff \mathfrak{p}_x \text{ is maximal.}$$

□

*Proof of (ii).* Since  $\overline{\{x\}}$  is the intersection of all closed sets containing  $x$  and Exercise 1.15 (iii), we have

$$\overline{\{x\}} = \bigcap_{\mathfrak{a} \subseteq \mathfrak{p}_x} V(\mathfrak{a}) = V\left(\sum_{\mathfrak{a} \subseteq \mathfrak{p}_x} \mathfrak{a}\right) = V(\mathfrak{p}_x).$$

□

*Proof of (iii).*

$$y \in \overline{\{x\}} \stackrel{(ii)}{\iff} y \in V(\mathfrak{p}_x) \iff \mathfrak{p}_y \supseteq \mathfrak{p}_x.$$

□

*Proof of (iv).*

- (1) Suppose  $x$  and  $y$  are two points in  $X$  such that  $y \in \overline{\{x\}}$  and  $x \in \overline{\{y\}}$ . Note that  $x = y$  implies that  $X$  is a  $T_0$ -space. So it suffices to show that  $x = y$ .
- (2) By (iii),  $\mathfrak{p}_y \supseteq \mathfrak{p}_x$  and  $\mathfrak{p}_x \supseteq \mathfrak{p}_y$ . So  $\mathfrak{p}_x = \mathfrak{p}_y$  or  $x = y$ .

□

### Exercise 1.19.

A topological space  $X$  is said to be irreducible if  $X \neq \emptyset$  and if every pair of non-empty open sets in  $X$  intersect, or equivalently if every non-empty open set is dense in  $X$ . Show that  $\text{Spec}(A)$  is irreducible if and only if the nilradical of  $A$  is a prime ideal.

*Proof.* Use the notations in Proposition 1.7 and Exercise 1.17.

$\text{Spec}(A)$  is irreducible

$$\begin{aligned} &\iff X_f \cap X_g \neq \emptyset \text{ for nonempty } X_f, X_g \in \text{Spec}(A) \\ &\iff X_{fg} \neq \emptyset \text{ for nonempty } X_f, X_g \in \text{Spec}(A) && \text{(Exercise 1.17 (i))} \\ &\iff fg \notin \mathfrak{N} \text{ for } f, g \notin \mathfrak{N} && \text{(Exercise 1.17 (ii))} \\ &\iff \mathfrak{N} \text{ is prime.} \end{aligned}$$



□

**Exercise 1.20.**

Let  $X$  be a topological space.

- (i) If  $Y$  is an irreducible subspace of  $X$ , then the closure  $\overline{Y}$  of  $Y$  in  $X$  is irreducible.
- (ii) Every irreducible subspace of  $X$  is contained in a maximal irreducible subspace.
- (iii) The maximal irreducible subspaces of  $X$  are closed and cover  $X$ . They are called the irreducible components of  $X$ . What are the irreducible components of a Hausdorff space?
- (iv) If  $A$  is a ring and  $X = \text{Spec}(A)$ , then the irreducible components of  $X$  are the closed sets  $V(\mathfrak{p})$ , where  $\mathfrak{p}$  is a minimal prime ideal of  $A$  (Exercise 1.8).

*Proof of (i).*

- (1)  $Y$  is irreducible if and only if  $Y$  cannot be represented as the union of two proper closed subspaces.

$$\begin{aligned}
& \forall \text{ nonempty open sets } U_1 \text{ and } U_2, U_1 \cap U_2 \neq \emptyset \\
& \iff \forall \text{ nonempty open sets } U_1 \text{ and } U_2, X - (U_1 \cap U_2) \neq X \\
& \iff \forall \text{ nonempty open sets } U_1 \text{ and } U_2, (X - U_1) \cup (X - U_2) \neq X \\
& \iff \forall \text{ proper closed sets } Y_1 \text{ and } Y_2, Y_1 \cup Y_2 \neq X \\
& \iff \nexists \text{ proper closed sets } Y_1 \text{ and } Y_2, Y_1 \cup Y_2 = X.
\end{aligned}$$

- (2) If  $\overline{Y}$  were reducible, there are two closed set  $Y_1$  and  $Y_2$  such that

$$\overline{Y} \subseteq Y_1 \cup Y_2, \quad \overline{Y} \not\subseteq Y_i (i = 1, 2).$$

- (a)  $Y \subseteq \overline{Y} \subseteq Y_1 \cup Y_2$ .
- (b)  $Y \not\subseteq Y_i (i = 1, 2)$ . If not,  $Y \subseteq Y_i$  for some  $i$ . Take closure to get  $\overline{Y} \subseteq \overline{Y_i} = Y_i$  (since  $Y_i$  is closed), contrary to the assumption.

By (a)(b),  $Y$  is reducible, which is absurd.

□

*Proof of (ii).*

- (1) This is a standard application of Zorn's lemma.

- (2) Suppose  $Y$  is an irreducible subspace of  $X$ . Let  $\Sigma$  be the set of all irreducible subspaces of  $X$  containing  $Y$ . Order  $\Sigma$  by inclusion.  $\Sigma$  is not empty, since  $Y \in \Sigma$ . To apply Zorn's lemma we must show that every chain in  $\Sigma$  has an upper bound in  $\Sigma$ ; let then  $(Y_\alpha)$  be a chain in  $\Sigma$ . Let  $Z = \bigcup_\alpha Y_\alpha$ .  $Z \supseteq Y$  clearly.
- (3) *Show that  $Z$  is irreducible.* Given two non-empty open sets  $U$  and  $V$  contained in  $Z = \bigcup_\alpha Y_\alpha$ . Then  $U \cap Y_\alpha \neq \emptyset$  and  $V \cap Y_\beta \neq \emptyset$  for some  $\alpha, \beta$ . Since  $(Y_\alpha)$  is a chain, we might have  $V \cap Y_\alpha \supseteq V \cap Y_\beta \neq \emptyset$  if  $\beta \leq \alpha$ . (The case  $\alpha \leq \beta$  is similar.) So  $U \cap V \cap Z \supseteq U \cap V \cap Y_\alpha \neq \emptyset$  since  $Z$  contains an irreducible subspace  $Y_\alpha$  in  $X$ .
- (4) Hence  $Z \in \Sigma$ , and  $Z$  is an upper bound of the chain  $(Y_\alpha)$ . Hence by Zorn's lemma  $\Sigma$  has a maximal element.

□

*Proof of (iii).*

- (1) *Show that the maximal irreducible subspaces of  $X$  are closed.* Suppose  $Y$  is a maximal irreducible subspaces of  $X$ . So  $\overline{Y}$  of  $Y$  in  $X$  is irreducible (by part (i)). The maximality of  $Y$  implies that  $Y = \overline{Y}$ .
- (2) *Show that the maximal irreducible subspaces of  $X$  cover  $X$ .* Note that each element  $P \in X$  forms an irreducible subset  $\{P\}$  and thus  $\{P\}$  is contained in one irreducible component (by (ii)).
- (3) One point subsets are the irreducible components of a Hausdorff space.

□

*Proof of (iv).*

- (1) Suppose  $Y$  is an irreducible components of  $X$ . *Show that  $Y = V(\mathfrak{p})$  where  $\mathfrak{p}$  is a prime ideal.* Similar to the proof of Exercise 1.19.
- (2) *Show that  $\mathfrak{p}$  is a minimal prime ideal of  $A$ .* Suppose  $\mathfrak{q} \subseteq \mathfrak{p}$ . Then  $V(\mathfrak{q}) \supseteq V(\mathfrak{p})$ . By the maximality of  $Y = V(\mathfrak{p})$ ,  $V(\mathfrak{q}) = V(\mathfrak{p})$  or  $r(\mathfrak{q}) = r(\mathfrak{p})$  or  $\mathfrak{q} = \mathfrak{p}$ . Hence  $\mathfrak{p}$  is a minimal prime ideal of  $A$ .

□

### Exercise 1.21.

Let  $\phi : A \rightarrow B$  be a ring homomorphism. Let  $X = \text{Spec}(A)$  and  $Y = \text{Spec}(B)$ . If  $\mathfrak{q} \in Y$ , then  $\phi^{-1}(\mathfrak{q})$  is a prime ideal of  $A$ , i.e., a point of  $X$ . Hence  $\phi$  induces a mapping  $\phi^* : Y \rightarrow X$ . Show that

- (i) If  $f \in A$  then  $\phi^{*-1}(X_f) = Y_{\phi(f)}$ , and hence that  $\phi^*$  is continuous.
- (ii) If  $\mathfrak{a}$  is an ideal of  $A$ , then  $\phi^{*-1}(V(\mathfrak{a})) = V(\mathfrak{a}^e)$ .
- (iii) If  $\mathfrak{b}$  is an ideal of  $B$ , then  $\overline{\phi^*(V(\mathfrak{b}))} = V(\mathfrak{b}^c)$ .
- (iv) If  $\phi$  is surjective, then  $\phi^*$  is a homeomorphism of  $Y$  onto the closed subset  $V(\ker(\phi))$  of  $X$ . (In particular,  $\text{Spec}(A)$  and  $\text{Spec}(A/\mathfrak{N})$  (where  $\mathfrak{N}$  is the nilradical of  $A$ ) are naturally homeomorphic.)
- (v) If  $\phi$  is injective, then  $\phi^*(Y)$  is dense in  $X$ . More precisely,  $\phi^*(Y)$  is dense in  $X$  if and only if  $\ker(\phi) \subseteq \mathfrak{N}$ .
- (vi) Let  $\psi : B \rightarrow C$  be another ring homomorphism. Then  $(\psi \circ \phi)^* = \phi^* \circ \psi^*$ .
- (vii) Let  $A$  be an integral domain with just one nonzero prime ideal  $\mathfrak{p}$ , and let  $K$  be the field of fractions of  $A$ . Let  $B = (A/\mathfrak{p}) \times K$ . Define  $\phi : A \rightarrow B$  by  $\phi(x) = (\bar{x}, x)$ , where  $\bar{x}$  is the image of  $x$  in  $A/\mathfrak{p}$ . Show that  $\phi^*$  is bijective but not a homeomorphism.

*Proof of (i).* Since

$$\begin{aligned}
& \mathfrak{q} \in Y_{\phi(f)} = Y - V(\phi(f)) \\
& \iff \mathfrak{q} \notin V(\phi(f)) = \{\text{all prime ideals in } B \text{ containing } \phi(f)\} \\
& \iff \phi(f) \notin \mathfrak{q} \\
& \iff f \notin \phi^{-1}(\mathfrak{q}) \\
& \iff \phi^{-1}(\mathfrak{q}) \notin V(f) = \{\text{all prime ideals in } A \text{ containing } f\} \\
& \iff \phi^*(\mathfrak{q}) = \phi^{-1}(\mathfrak{q}) \in X_f,
\end{aligned}$$

$\phi^*$  is continuous.  $\square$

*Proof of (ii).*

- (1) Use the same notation of Proposition 1.17. Show that

$$\mathfrak{b}^c \supseteq \mathfrak{a} \iff \mathfrak{b} \supseteq \mathfrak{a}^e.$$

Suppose  $\mathfrak{b}^c \supseteq \mathfrak{a}$ , then  $\mathfrak{b}^{ce} \supseteq \mathfrak{a}^e$ . Proposition 1.17 (i) suggests that  $\mathfrak{b} \supseteq \mathfrak{b}^{ce} \supseteq \mathfrak{a}^e$ . The converse is similar.

- (2) So

$$\begin{aligned}
& \mathfrak{q} \in \phi^{*-1}(V(\mathfrak{a})) \\
& \iff \phi^*(\mathfrak{q}) \in V(\mathfrak{a}) = \{\text{all prime ideals containing } \mathfrak{a}\} \\
& \iff \phi^*(\mathfrak{q}) \supseteq \mathfrak{a} \\
& \iff \mathfrak{q}^c \supseteq \mathfrak{a} \\
& \iff \mathfrak{q} \supseteq \mathfrak{a}^e \\
& \iff \mathfrak{q} \in V(\mathfrak{a}^e) = \{\text{all prime ideals containing } \mathfrak{a}^e\}.
\end{aligned} \tag{1}$$

□

*Proof of (iii).*

- (1) Might assume that  $\mathfrak{b} = r(\mathfrak{b})$  is radical by Exercise 1.15 (i).
- (2) Show that  $\overline{\phi^*(V(\mathfrak{b}))} \supseteq V(\mathfrak{b}^c)$ . Write  $\overline{\phi^*(V(\mathfrak{b}))} = V(\mathfrak{a})$  for some radical ideal  $\mathfrak{a}$  in  $A$  since  $\phi^*(V(\mathfrak{b}))$  is closed. So

$$\begin{aligned}
 V(\mathfrak{a}^e) &= \phi^{*-1}(V(\mathfrak{a})) = \phi^{*-1}(\overline{\phi^*(V(\mathfrak{b}))}) \supseteq V(\mathfrak{b}) & ((ii)) \\
 \implies r(\mathfrak{a}^e) &\subseteq r(\mathfrak{b}) \\
 \implies r(\mathfrak{a})^e &\subseteq r(\mathfrak{a}^e) \subseteq r(\mathfrak{b}) \\
 \implies \mathfrak{a}^e &\subseteq \mathfrak{b} \\
 \implies \mathfrak{a} &\subseteq \mathfrak{b}^c \\
 \implies V(\mathfrak{a}) &\supseteq V(\mathfrak{b}^c).
 \end{aligned}$$

- (3) Show that  $\overline{\phi^*(V(\mathfrak{b}))} \subseteq V(\mathfrak{b}^c)$ . It suffices to show that  $\phi^*(V(\mathfrak{b})) \subseteq V(\mathfrak{b}^c)$  since  $V(\mathfrak{b}^c)$  is closed. Suppose  $\mathfrak{p} \in \phi^*(V(\mathfrak{b}))$ . Then there is  $\mathfrak{q} \in V(\mathfrak{b})$  such that

$$\mathfrak{p} = \phi^*(\mathfrak{q}) = \mathfrak{q}^c \supseteq \mathfrak{b}^c.$$

So  $\mathfrak{p} \in V(\mathfrak{b}^c)$ .

□

*Proof of (iv).* Note that  $A/\ker \phi \cong B$  since  $\phi$  is surjective. The correspondence theorem shows that  $\phi^* : Y \rightarrow V(\ker \phi)$  is bijective. As the continuity of  $\phi^*$  is given by (i),  $\phi^*$  is a homeomorphism of  $Y$  onto  $V(\ker(\phi)) \subseteq X$ . □

*Proof of (v).*

- (1) It suffices to show that  $\phi^*(Y)$  is dense in  $X$  if and only if  $\ker(\phi) \subseteq \mathfrak{N}$ .
- (2)

$$\begin{aligned}
 &\phi^*(Y) \text{ is dense in } X \\
 \iff &X = \overline{\phi^*(Y)} = \overline{\phi^*(V(0))} = V(0^c) = V(\ker \phi) \\
 \iff &\ker \phi \text{ is contained in every prime ideal of } A \\
 \iff &\ker \phi \subseteq \mathfrak{N}.
 \end{aligned}$$

□

*Proof of (vi).*

$$(\psi \circ \phi)^*(\mathfrak{p}) = (\psi \circ \phi)^{-1}(\mathfrak{p}) = \phi^{-1}(\psi^{-1}(\mathfrak{p})) = \phi^*(\psi^*(\mathfrak{p})) = (\phi^* \circ \psi^*)(\mathfrak{p})$$

for every prime ideal  $\mathfrak{p}$  in  $\text{Spec}(C)$ . □

*Proof of (vii).*

- (1) Show that  $\phi^*$  is bijective. Note that

$$\begin{aligned} X &= \operatorname{Spec}(A) = \{(0), \mathfrak{p}\} \\ Y &= \operatorname{Spec}(B) = \{A/\mathfrak{p} \times (0), (0) \times K\} \end{aligned}$$

and thus

$$\begin{aligned} \phi^*(A/\mathfrak{p} \times (0)) &= (0) \\ \phi^*((0) \times K) &= (\mathfrak{p}). \end{aligned}$$

Hence  $\phi^*$  is a bijection.

- (2) Show that  $\phi^*$  is not a homeomorphism. Note that  $\overline{\{(0)\}} = X$  (Exercise 1.18 (iii)) and  $Y$  is equipped with the discrete topology since each prime ideal of  $B$  is maximal (Exercise 1.18 (i)). So  $\phi^*$  cannot be a homeomorphism.

□

### Exercise 1.22.

Let  $A = \prod_{i=1}^n A_i$  be a direct product of rings  $A_i$ . Show that  $\operatorname{Spec}(A)$  is the disjoint union of open (and closed) subspaces  $X_i$ , where  $X_i$  is canonically homeomorphic with  $\operatorname{Spec}(A_i)$ .

Conversely, let  $A$  be any ring. Show that the following statements are equivalent:

- (i)  $X = \operatorname{Spec}(A)$  is disconnected.
- (ii)  $A \cong A_1 \times A_2$  where neither of the rings  $A_1, A_2$  is the zero ring.
- (iii)  $A$  contains an idempotent  $\neq 0, 1$ . In particular, the spectrum of a local ring is always connected (Exercise 1.12).

*Proof.*

- (1) Show that  $\operatorname{Spec}(A)$  is the union of closed subspaces  $X_i$ , where  $X_i \cong \operatorname{Spec}(A_i)$ . Let  $\phi_i : A \rightarrow A_i$  be the projection map. So

$$\ker \phi_i = A_1 \times \cdots \times A_{i-1} \times 0 \times A_{i+1} \times \cdots \times A_n.$$

So

$$\operatorname{Spec}(A) = V(0) = V\left(\bigcap_{i=1}^n \ker \phi_i\right) = \bigcup_{i=1}^n V(\ker \phi_i)$$

where  $X_i := V(\ker \phi_i) \cong \operatorname{Spec}(A_i)$  (Exercise 1.21).

(2) Show that  $V(\ker \phi_i)$  and  $V(\ker \phi_j)$  are disjoint if  $i \neq j$ .

$$V(\ker \phi_i) \cap V(\ker \phi_j) = V(\ker \phi_i + \ker \phi_j) = V(A) = V(1) = \emptyset.$$

(3) Show that  $V(\ker \phi_i)$  is open.  $\text{Spec}(A) = \bigcup_{j=1}^n V(\ker \phi_j)$  and  $V(\ker \phi_i) \cap V(\ker \phi_j) = \emptyset$  (if  $i \neq j$ ) implies that  $\text{Spec}(A) \setminus V(\ker \phi_i) = \bigcup_{j \neq i} V(\ker \phi_j)$  is closed. Thus  $V(\ker \phi_i)$  is open.

(4) ((ii)  $\implies$  (i)) See (1)(2)(3).

(5) ((i)  $\implies$  (iii)) Write  $X$  as a disjoint union of two nonempty closed sets  $V(\mathfrak{a}), V(\mathfrak{b})$  where  $\mathfrak{a}, \mathfrak{b}$  are radical ideals in  $A$  (Exercise 1.15). Since

$$\begin{aligned} V(0) = X &= V(\mathfrak{a}) \cup V(\mathfrak{b}) = V(\mathfrak{ab}) \\ V(1) = \emptyset &= V(\mathfrak{a}) \cap V(\mathfrak{b}) = V(\mathfrak{a} + \mathfrak{b}), \end{aligned}$$

there exist  $a \in \mathfrak{a}, b \in \mathfrak{b}$  such that  $a + b = 1$  and  $(ab)^n = 0$  for one positive integer  $n$ . So  $ab = 0$  since  $\mathfrak{ab}$  is radical. (Note that  $\mathfrak{a} + \mathfrak{b} = 1$  and Exercise 1.13 on page 9.) So

$$a^2 = a(1 - b) = a - ab = a$$

is an idempotent. Also  $a \neq 0, 1$  since  $V(\mathfrak{a}), V(\mathfrak{b})$  are proper subsets of  $X$ .

(6) ((iii)  $\implies$  (ii)) Take an idempotent  $e \neq 0, 1$  in  $A$ . Two ideals  $(e)$  and  $(1 - e)$  are proper and coprime. So  $(e) \cap (1 - e) = (e)(1 - e) = (0)$  (Proposition 1.10 (i)). Proposition 1.10 (ii) and (iii) imply that the ring homomorphism

$$A \rightarrow A/(e) \times A/(1 - e)$$

is an isomorphism. Also  $A/(e), A/(1 - e) \neq 0$  since  $e \neq 0, 1$ .

□

### Exercise 1.23.

Let  $A$  be a Boolean ring (Exercise 1.11), and let  $X = \text{Spec}(A)$ .

- (i) For each  $f \in A$ , the set  $X_f$  (Exercise 1.17) is both open and closed in  $X$ .
- (ii) Let  $f_1, \dots, f_n \in A$ . Show that  $X_{f_1} \cup \dots \cup X_{f_n} = X_f$  for some  $f \in A$ .
- (iii) The sets  $X_f$  are the only open subsets of  $X$  which are both open and closed.
- (iv)  $X$  is a compact Hausdorff space.

*Proof of (i).*

- (1) Show that  $X$  is the disjoint union of subspaces  $X_f$  and  $X_{1-f}$ . Note that every element in a Boolean ring is an idempotent. Hence

$$\begin{aligned} X_f \cap X_{1-f} &= X_{f(1-f)} = X_0 = \emptyset \\ X_f \cup X_{1-f} &= X \setminus (V(f) \cap V(1-f)) = X \setminus \underbrace{V(f + (1-f))}_{=V(1)=\emptyset} = X. \end{aligned}$$

- (2) Hence  $X_f = X \setminus X_{1-f}$  is both open and closed.

□

*Proof of (ii).* Similar to (i),

$$\begin{aligned} X_{f_1} \cup \cdots \cup X_{f_n} &= X \setminus (V(f_1) \cap \cdots \cap V(f_n)) \\ &= X \setminus V(f_1, \dots, f_n) \\ &= X \setminus V(f) && \text{(Exercise 1.11 (iii))} \\ &= X_f \end{aligned}$$

for some  $f \in A$ . □

*Proof of (iii).*

- (1) Suppose  $Y$  is both open and closed in  $X$ .
- (2) Since  $Y$  is closed and  $X$  is quasi-compact (Exercise 1.17 (vi)),  $Y$  is quasi-compact.
- (3) Since  $Y$  is open,  $Y$  is a finite union of sets  $X_{f_i}$  for  $i = 1, \dots, n$  (Exercise 1.17 (vii)). Hence  $Y = X_f$  for some  $f \in A$  (by (ii)).

□

*Proof of (iv).*

- (1) The compactness of  $X$  is followed by Exercise 1.17 (v).
- (2) Show that  $X$  is Hausdorff. Exercise 1.18 shows that  $X$  is a  $T_0$ -space. This means that if  $x, y$  are distinct points of  $X$ , we might assume that there is a neighborhood  $U$  of  $x$  which does not contain  $y$ .
- (3) Write  $U = X_f$  for some  $f \in A$  (by Exercise 1.17 and (ii)). As  $x \in X_f$ ,  $y \in X \setminus X_f = X_{1-f}$  and  $X_f \cap X_{1-f} = \emptyset$  by (i). Hence  $X$  is Hausdorff.

□

**Exercise 1.24. (Boolean lattice)**

Let  $L$  be a lattice, in which the sup and inf of two elements  $a, b$  are denoted by  $a \vee b$  and  $a \wedge b$  respectively.  $L$  is a **Boolean lattice** (or **Boolean algebra**) if

- (i)  $L$  has a least element and a greatest element (denoted by  $0, 1$  respectively);
- (ii) Each of  $\vee, \wedge$  is distributive over the other;
- (iii) Each  $a \in L$  has a unique “complement”  $a' \in L$  such that  $a \vee a' = 1$  and  $a \wedge a' = 0$ .

(For example, the set of all subsets of a set, ordered by inclusion, is a Boolean lattice.)

Let  $L$  be a Boolean lattice. Define addition and multiplication in  $L$  by the rules

$$a + b = (a \wedge b') \vee (a' \wedge b), \quad ab = a \wedge b.$$

Verify that in this way  $L$  becomes a Boolean ring, say  $A(L)$ .

Conversely, starting from a Boolean ring  $A$ , define an ordering on  $A$  as follows:  $a \leq b$  means that  $a = ab$ . Show that, with respect to this ordering,  $A$  is a Boolean lattice. In this way we obtain a one-to-one correspondence between (isomorphism classes of) Boolean rings and (isomorphism classes of) Boolean lattices.

*Proof.*

- (1) Some properties about  $\vee$  and  $\wedge$ :

- (a) (Commutativity) Show that

$$a \vee b = b \vee a, \quad a \wedge b = b \wedge a.$$

Say  $z_1 := a \vee b$  and  $z_2 := b \vee a$ . By the definition of the sup,

$$z_1 \geq a, b \text{ such that for all other } w_1 \geq a, b \text{ we have } w_1 \geq z_1$$

$$z_2 \geq b, a \text{ such that for all other } w_2 \geq b, a \text{ we have } w_2 \geq z_2.$$

So  $z_1 \geq z_2$  and  $z_2 \geq z_1$  and thus  $z_1 = z_2$ . Hence  $a \vee b = b \vee a$ .

Similarly,  $a \wedge b = b \wedge a$ .

- (b) (Associativity) Show that

$$(a \vee b) \vee c = a \vee b \vee c = a \vee (b \vee c),$$

$$(a \wedge b) \wedge c = a \wedge b \wedge c = a \wedge (b \wedge c).$$

Say  $z_1 := (a \wedge b) \wedge c$ ,  $z_2 := a \wedge b \wedge c$ , and  $z_3 := a \wedge (b \wedge c)$ . By the definition of inf,  $z_1$  is a unique greatest element such that  $z_1 \leq a \wedge b, c$ . So  $z_1 \leq a, b, c$  or  $z_1 \leq z_2$ . Besides,  $z_2 \leq a, b, c$  implies that  $z_2 \leq a, b \wedge c$ . So  $z_2 \leq z_3$ . Hence  $z_1 \leq z_2 \leq z_3$ . Similarly,  $z_3 \leq z_2 \leq z_1$ . So  $z_1 = z_2 = z_3$ . Similarly,  $(a \vee b) \vee c = a \vee b \vee c = a \vee (b \vee c)$



(c) (De Morgan's laws) *Show that*

$$(a \vee b)' = a' \wedge b', \quad (a \wedge b)' = a' \vee b'.$$

Since

$$\begin{aligned} (a \vee b) \vee (a' \wedge b') &= (a \vee b \vee a') \wedge (a \vee b \vee b') \\ &= (a \vee a' \vee b) \wedge (a \vee b \vee b') \\ &= (1 \vee b) \wedge (a \vee 1) \\ &= 1 \wedge 1 \\ &= 1. \end{aligned}$$

and

$$\begin{aligned} (a \vee b) \wedge (a' \wedge b') &= (a \wedge a' \wedge b') \vee (b \wedge a' \wedge b') \\ &= (a \wedge a' \wedge b') \vee (a' \wedge b \wedge b') \\ &= (0 \wedge b') \vee (a' \wedge 0) \\ &= 0 \vee 0 \\ &= 0, \end{aligned}$$

The complement of  $a \vee b$  is  $a' \wedge b'$ . Similarly,  $(a \wedge b)' = a' \vee b'$ .

(2) *Show that  $A(L)$  is an abelian group under addition.*

(a) (Commutativity) *Show that  $a + b = b + a$ .* By (1)(a),

$$\begin{aligned} a + b &= (a \wedge b') \vee (a' \wedge b) \\ &= (a' \wedge b) \vee (a \wedge b') \\ &= (b \wedge a') \vee (b' \wedge a) \\ &= b + a. \end{aligned}$$

(b) (Associativity) *Show that  $(a + b) + c = a + (b + c)$ .* By (1)(a)(b),

$$\begin{aligned} &(a + b) + c \\ &= ((a + b) \wedge c') \vee ((a + b)' \wedge c) \\ &= (((a \wedge b') \vee (a' \wedge b)) \wedge c') \\ &\quad \vee (((a \wedge b') \vee (a' \wedge b))' \wedge c) \\ &= (a \wedge b' \wedge c') \vee (a' \wedge b \wedge c') \\ &\quad \vee ((a' \vee b) \wedge (a \vee b') \wedge c) \quad ((ii), (1)(c)) \\ &= (a \wedge b' \wedge c') \vee (a' \wedge b \wedge c') \\ &\quad \vee (((a' \wedge a) \vee (a' \wedge b') \vee (b \wedge a) \vee (b \wedge b')) \wedge c) \quad ((ii)) \\ &= (a \wedge b' \wedge c') \vee (a' \wedge b \wedge c') \\ &\quad \vee ((a' \wedge b') \vee (a \wedge b)) \wedge c \quad ((iii), (1)(a)) \\ &= (a \wedge b' \wedge c') \vee (a' \wedge b \wedge c') \\ &\quad \vee (a' \wedge b' \wedge c) \vee (a \wedge b \wedge c) \quad ((ii)) \end{aligned}$$

and

$$\begin{aligned}
& a + (b + c) \\
&= (b + c) + a && ((a)) \\
&= (c \wedge b' \wedge a') \vee (c' \wedge b \wedge a') \vee (c' \wedge b' \wedge a) \vee (c \wedge b \wedge a) \\
&= (a' \wedge b' \wedge c) \vee (a' \wedge b \wedge c') \vee (a \wedge b' \wedge c') \vee (a \wedge b \wedge c) && ((1)(a)) \\
&= (a \wedge b' \wedge c') \vee (a' \wedge b \wedge c') \vee (a' \wedge b' \wedge c) \vee (a \wedge b \wedge c). && ((1)(a))
\end{aligned}$$

Thus  $(a + b) + c = a + (b + c)$ .

- (c) (Identity) *Show that  $a + 0 = 0 + a = a$ . The complement of 0 in  $L$  is  $0' = 1$  and vice versa ((iii)). Hence*

$$\begin{aligned}
a + 0 &= (a \wedge 0') \vee (a' \wedge 0) \\
&= (a \wedge 1) \vee (a' \wedge 0) \\
&= a \vee 0 \\
&= a.
\end{aligned}$$

Note that  $A(L)$  is commutative under addition.

- (d) (Invertibility) *Show that  $a + a = 0$ , that is,  $a$  itself is the additive inverse of  $a$ .*

$$a + a = (a \wedge a') \vee (a' \wedge a) = 0 \vee 0 = 0.$$

- (3) *Show that  $A(L)$  is commutative under multiplication. It is (1)(a).*

- (4) *Show that  $A(L)$  is a monoid under multiplication.*

- (a) (Associativity) *Show that  $(ab)c = a(bc)$ . It is (1)(b).*

- (b) (Identity) *Show that  $a1 = 1a = a$ .*

$$a1 = a \wedge 1 = a, \quad 1a = 1 \wedge a = a.$$

- (5) *Show that multiplication is distributive with respect to addition in  $A(L)$ .*

- (a) (Left distributivity) *Show that  $a(b + c) = ab + ac$ . Note that*

$$\begin{aligned}
a(b + c) &= a \wedge (b + c) \\
&= a \wedge ((b \wedge c') \vee (b' \wedge c)) \\
&= (a \wedge b \wedge c') \vee (a \wedge b' \wedge c) && ((ii))
\end{aligned}$$

and

$$\begin{aligned}
ab + ac &= (a \wedge b) + (a \wedge c) \\
&= ((a \wedge b) \wedge (a \wedge c)') \vee ((a \wedge b)' \wedge (a \wedge c)) \\
&= ((a \wedge b) \wedge (a' \vee c')) \vee ((a' \vee b') \wedge (a \wedge c)) \quad ((1)(c)) \\
&= ((a \wedge b \wedge a') \vee (a \wedge b \wedge c')) \\
&\quad \vee ((a' \wedge a \wedge c) \vee (b' \wedge a \wedge c)) \quad ((ii)) \\
&= ((a \wedge a' \wedge b) \vee (a \wedge b \wedge c')) \\
&\quad \vee ((a' \wedge a \wedge c) \vee (a \wedge b' \wedge c)) \quad ((1)(a)) \\
&= 0 \vee (a \wedge b \wedge c') \vee 0 \vee (a \wedge b' \wedge c) \quad ((iii)) \\
&= (a \wedge b \wedge c') \vee (a \wedge b' \wedge c). \quad ((i))
\end{aligned}$$

(b) (Right distributivity) The left distributivity implies the right distributivity by (1)(a).

- (6) (2)-(5) show that  $A(L)$  is a commutative ring. Also  $a^2 = a \wedge a = a$  implies that  $A(L)$  is a Boolean ring.
- (7) Conversely, starting from a Boolean ring  $A$ , define an ordering on  $A$  as follows:  $a \leq b$  means that  $a = ab$ . The ordering is well-defined (since  $A$  is a Boolean ring).
- (8) Define  $a \vee b = a + b + ab$  and  $a \wedge b = ab$ . Show that  $a \vee b$  is the sup and  $a \wedge b$  is the inf. Similar to the proof of Exercise 1.11 (iii),

$$a(a \vee b) = a(a + b + ab) = a^2 + ab + a^2b = a + ab + ab = a.$$

So  $a \leq a \vee b$ . Similarly,  $b \leq a \vee b$ . So  $a \vee b$  is an upper bound of  $a$  and  $b$ . To show  $a \vee b$  is the least upper bound, it suffices to show that all other  $z \geq a, b$  we have  $z \geq a \vee b$ . In fact,

$$(a \vee b)z = (a + b + ab)z = az + bz + abz = a + b + ab = a \vee b.$$

Hence  $a \vee b$  is the sup. Similarly,  $a \wedge b$  is the inf. Therefore we define a lattice  $L(A)$  on a Boolean ring  $A$ .

- (9) Show that  $L(A)$  is a Boolean lattice.  $0 \in A$  is a least element,  $1$  is a greatest element, each of  $\vee$  and  $\wedge$  is distributive over the other, and  $a' = 1 - a$  is the unique complement of  $a$ .
- (10) It is easy to see that  $A(L(A)) = A$  and  $L(A(L)) = L$  (up to isomorphism). Hence there is a one-to-one correspondence between Boolean rings and Boolean lattices.

□

**Exercise 1.25. (Stone's theorem)**

From the last two exercises deduce Stone's theorem, that every Boolean lattice is isomorphic to the lattice of open-and-closed subsets of some compact Hausdorff topological space.

*Proof.*

- (1) Suppose  $L$  is a Boolean lattice and  $A = A(L)$  is the corresponding Boolean ring (Exercise 1.24). Observe that  $X = \text{Spec}(A)$  is a compact Hausdorff space (Exercise 1.23).

- (2) Define a map

$$\alpha : L \rightarrow \mathcal{P}(X)$$

by  $\alpha(f) = X_f$  where  $\mathcal{P}(X)$  is the power set of a set  $X$ . View  $\mathcal{P}(X)$  as a Boolean lattice, ordered by inclusion.

- (3) The image of  $\alpha$  is the collection of all open-and-closed sets in  $X$  (Exercise 1.23). Note that  $\text{im}(\alpha)$  is a Boolean lattice (Exercises 1.17 and 1.23).

- (4) Show that  $\alpha : L \rightarrow \text{im}(\alpha)$  is injective. Suppose  $X_f = X_g$ . Exercise 1.17 shows that  $r((f)) = r((g))$ . In particular,  $f \in r((g))$ . So  $f = g^n$  for some  $n \geq 1$ . Hence  $f = g^n = g^{n-1} = \cdots = g$  since  $A$  is a Boolean ring.

- (5) Since

$$\begin{aligned} f \leq g &\iff f = fg \\ &\iff X_f = X_{fg} && \text{(Injectivity of } \alpha) \\ &\iff X_f = X_f \cap X_g \\ &\iff X_f \subseteq X_g, \end{aligned}$$

$\alpha : L \rightarrow \text{im}(\alpha)$  preserves the ordering. Hence  $\alpha$  is an isomorphism between two Boolean lattices.

□

**Exercise 1.26. (Maximal spectrum)**

Let  $A$  be a ring. The subspace of  $\text{Spec}(A)$  consisting of the maximal ideals of  $A$ , with the induced topology, is called the **maximal spectrum** of  $A$  and is denoted by  $\text{Max}(A)$ . For arbitrary commutative rings it does not have the nice functorial properties of  $\text{Spec}(A)$  (see Exercise 1.21), because the inverse image of a maximal ideal under a ring homomorphism need not be maximal.

Let  $X$  be a compact Hausdorff space and let  $C(X)$  denote the ring of all real-valued continuous functions on  $X$  (add and multiply functions by adding and multiplying

their values). For each  $x \in X$ , let  $\mathfrak{m}_x$  be the set of all  $f \in C(X)$  such that  $f(x) = 0$ . The ideal  $\mathfrak{m}_x$  is maximal, because it is the kernel of the (surjective) homomorphism  $C(X) \rightarrow \mathbb{R}$  which takes  $f$  to  $f(x)$ . If  $\tilde{X}$  denotes  $\text{Max}(C(X))$ , we have therefore defined a mapping  $\mu : X \rightarrow \tilde{X}$ , namely  $x \mapsto \mathfrak{m}_x$ .

We shall show that  $\mu$  is a homeomorphism of  $X$  onto  $\tilde{X}$ .

- (i) Let  $\mathfrak{m}$  be any maximal ideal of  $C(X)$ , and let  $V = V(\mathfrak{m})$  be the set of common zeros of the functions in  $\mathfrak{m}$ : that is,

$$V = \{x \in X : f(x) = 0 \text{ for all } f \in \mathfrak{m}\}.$$

Suppose that  $V$  is empty. Then for each  $x \in X$  there exists  $f_x \in \mathfrak{m}$  such that  $f_x(x) \neq 0$ . Since  $f_x$  is continuous, there is an open neighborhood  $U_x$  of  $x$  in  $X$  on which  $f_x$  does not vanish. By compactness a finite number of the neighborhoods, say  $U_{x_1}, \dots, U_{x_n}$ , cover  $X$ . Let

$$f = f_{x_1}^2 + \dots + f_{x_n}^2.$$

Then  $f$  does not vanish at any point of  $X$ , hence is a unit in  $C(X)$ . But this contradicts  $f \in \mathfrak{m}$ , hence  $V$  is not empty. Let  $x$  be a point of  $V$ . Then  $\mathfrak{m} \subseteq \mathfrak{m}_x$ , hence  $\mathfrak{m} = \mathfrak{m}_x$  because  $\mathfrak{m}$  is maximal. Hence  $\mu$  is surjective.

- (ii) By Urysohn's lemma (this is the only non-trivial fact required in the argument) the continuous functions separate the points of  $X$ . Hence  $x \neq y \implies \mathfrak{m}_x \neq \mathfrak{m}_y$ , and therefore  $\mu$  is injective.

- (iii) Let  $f \in C(X)$ ; let

$$U_f = \{x \in X : f(x) \neq 0\}$$

and let

$$\tilde{U}_f = \{\mathfrak{m} \in \tilde{X} : f \notin \mathfrak{m}\}.$$

Show that  $\mu(U_f) = \tilde{U}_f$ . The open sets  $U_f$  (resp.  $\tilde{U}_f$ ) form a basis of the topology of  $X$  (resp.  $\tilde{X}$ ) and therefore  $\mu$  is a homeomorphism. Thus  $X$  can be reconstructed from the ring of functions  $C(X)$ .

*Proof.*

- (1) Show that the inverse image of a maximal ideal under a ring homomorphism need not be maximal. Let  $\phi : \mathbb{Z}[x] \rightarrow \mathbb{R}[x]$  be a natural inclusion map. The ideal  $\mathfrak{P} = (x)$  in  $\mathbb{R}[x]$  is maximal. But  $\phi^{-1}(\mathfrak{P}) = (x)$  in  $\mathbb{Z}[x]$  is not maximal since  $(x) \subsetneq (x, 2)$  in  $\mathbb{Z}[x]$ .
- (2) Show that  $\mu(U_f) = \tilde{U}_f$ .

$$\begin{aligned} x \in U_f &\iff x \in X \text{ such that } f(x) \neq 0 \\ &\iff x \in X \text{ such that } f \notin \mathfrak{m}_x \\ &\iff \mathfrak{m}_x \in \tilde{X} \text{ such that } f \notin \mathfrak{m}_x \\ &\iff \mu(x) = \mathfrak{m}_x \in \tilde{U}_f. \end{aligned}$$

- (3) Show that  $U_f$  form a basis of the topology of  $X$ . Let  $U$  be open in  $X$ . For any  $x \in U$ , it suffices to find  $f \in C(X)$  such that  $x \in U_f \subseteq U$ . Note that one-point set  $\{x\}$  is closed (since  $X$  is Hausdorff). By Urysohn's lemma, there is  $f \in C(X)$  such that  $f = 1$  on  $\{x\}$  and  $f = 0$  on  $X \setminus U$ .
- (4) Show that  $\tilde{U}_f$  form a basis of the topology of  $\tilde{X}$ . Let  $\tilde{U} = \widetilde{W} \cap \tilde{X}$  be open in  $\tilde{X}$  where  $\widetilde{W}$  is open in  $\text{Spec}(C(X))$  (w.r.t. the induced topology). For any  $\mathfrak{m} \in \tilde{U} = \widetilde{W} \cap \tilde{X} \subseteq \widetilde{W}$ , Exercise 1.17 shows that

$$\mathfrak{m} \in \text{Spec}(C(X))_f \subseteq \widetilde{W}$$

for some  $f \in C(X)$ . So

$$\mathfrak{m} \in \underbrace{\text{Spec}(C(X))_f}_{=\tilde{U}_f} \cap \tilde{X} \subseteq \underbrace{\widetilde{W} \cap \tilde{X}}_{=\tilde{U}}.$$

□

## Affine algebraic varieties

### Exercise 1.27. (Hilbert's Nullstellensatz)

Let  $k$  be an algebraically closed field and let

$$f_\alpha(t_1, \dots, t_n) = 0$$

be a set of polynomial equations in  $n$  variables with coefficients in  $k$ . The set  $X$  of all points  $x = (x_1, \dots, x_n) \in k^n$  which satisfy these equations is an **affine algebraic variety**.

Consider the set of all polynomials  $g \in k[t_1, \dots, t_n]$  with the property that  $g(x) = 0$  for all  $x \in X$ . This set is an ideal  $I(X)$  in the polynomial ring, and is called the **ideal of the variety**  $X$ . The quotient ring

$$P(X) = k[t_1, \dots, t_n]/I(X)$$

is the ring of polynomial functions on  $X$ , because two polynomials  $g, h$  define the same polynomial function on  $X$  if and only if  $g - h$  vanishes at every point of  $X$ , that is, if and only if  $g - h \in I(X)$ .

Let  $\xi_i$  be the image of  $t_i$  in  $P(X)$ . The  $\xi_i$  ( $1 \leq i \leq n$ ) are the **coordinate functions** on  $X$ : if  $x \in X$ , then  $\xi_i(x)$  is the  $i$ th coordinate of  $x$ .  $P(X)$  is generated as a  $k$ -algebra by the coordinate functions, and is called the **coordinate ring** (or affine algebra) of  $X$ .

As in Exercise 1.26, for each  $x \in X$  let  $\mathfrak{m}_x$  be the ideal of all  $f \in P(X)$  such that  $f(x) = 0$ ; it is a maximal ideal of  $P(X)$ . Hence, if  $\tilde{X} = \text{Max}(P(X))$ , we have defined a mapping  $\mu : X \rightarrow \tilde{X}$ , namely  $x \mapsto \mathfrak{m}_x$ . It is easy to show that  $\mu$  is injective: if  $x \neq y$ , we must have  $x_i \neq y_i$  for some  $i$  ( $1 \leq i \leq n$ ), and hence  $\xi_i - x_i$  is in  $\mathfrak{m}_x$  but not in  $\mathfrak{m}_y$ , so that  $\mathfrak{m}_x \neq \mathfrak{m}_y$ . What is less obvious (but still true) is that  $\mu$  is surjective. This is one form of Hilbert's Nullstellensatz (see Chapter 7).

*Proof.*

- (1) Show that  $\mu$  is surjective. If  $\mathfrak{m}$  is a maximal ideal of  $P(X)$ , then  $B := P(X)/\mathfrak{m}$  is a finitely generated  $k$ -algebra. Note that  $B$  is also a field, Corollary 5.24 implies that  $B$  is a finite algebraic extension of  $k$ .
- (2) In fact,  $B \cong k$  since  $k = \bar{k}$ . Let  $x_i$  be the image of  $\xi_i$  in  $k$  for each  $i$ . So  $\xi_i - x_i = 0 \in k \cong B$  or  $\xi_i - x_i \in \mathfrak{m}$ . So

$$\mathfrak{m} \subseteq (\xi_1 - x_1, \dots, \xi_n - x_n) = \mathfrak{m}_x.$$

Hence  $\mathfrak{m} = \mathfrak{m}_x$  by the maximality of  $\mathfrak{m}$ .

□

### Exercise 1.28.

Let  $f_1, \dots, f_m$  be elements of  $k[t_1, \dots, t_n]$ . They determine a **polynomial mapping**  $\phi : k^n \rightarrow k^m$ : if  $x \in k^n$ , the coordinates of  $\phi(x)$  are  $f_1(x), \dots, f_m(x)$ .

Let  $X, Y$  be affine algebraic varieties in  $k^n, k^m$  respectively. A mapping  $\phi : X \rightarrow Y$  is said to be **regular** if  $\phi$  is the restriction to  $X$  of a polynomial mapping from  $k^n$  to  $k^m$ .

If  $\eta$  is a polynomial function on  $Y$ , then  $\eta \circ \phi$  is a polynomial function on  $X$ . Hence  $\phi$  induces a  $k$ -algebra homomorphism  $P(Y) \rightarrow P(X)$ , namely  $\eta \mapsto \eta \circ \phi$ . Show that in this way we obtain a one-to-one correspondence between the regular mappings  $X \rightarrow Y$  and the  $k$ -algebra homomorphisms  $P(Y) \rightarrow P(X)$ .

*Proof.*

- (1) Let  $P(X) = k[t_1, \dots, t_n]/I(X)$  and  $P(Y) = k[s_1, \dots, s_m]/I(Y)$ . Let  $\eta_j$  be the image of  $s_j$  in  $P(Y)$ . Suppose  $\phi$  induces a  $k$ -algebra homomorphism  $P(Y) \rightarrow P(X)$  by  $\tilde{\phi} : \eta \mapsto \eta \circ \phi$ .
- (2) Show that the correspondence is injective. Suppose  $\tilde{\alpha} = \tilde{\beta}$  for some regular mappings  $\alpha = (\alpha_1, \dots, \alpha_m)$  and  $\beta = (\beta_1, \dots, \beta_m)$ . Hence

$$\alpha_j = \eta_j \circ \alpha = \tilde{\alpha}(\eta_j) = \tilde{\beta}(\eta_j) = \eta_j \circ \beta = \beta_j$$

for  $1 \leq j \leq m$ . Hence  $\alpha_j = \beta_j$  on  $X$  and thus  $\alpha = \beta$  on  $X$ .

- (3) *Show that the correspondence is surjective.* Suppose  $\Psi : P(Y) \rightarrow P(X)$  is a  $k$ -algebra homomorphism. Say  $\psi_j + I(X) := \Psi(\eta_j) \in P(X)$  for some  $\psi_j \in k[t_1, \dots, t_n]$  (where  $1 \leq j \leq m$ ).
- (4) Define  $\psi : X \rightarrow k^m$  by

$$\psi(P) = (\psi_1(P), \dots, \psi_m(P))$$

where  $P = (t_1, \dots, t_n) \in X$ .  $\psi$  is well-defined (since  $\psi$  is independent of the choice of  $\psi_j$ ). To show  $\psi$  is regular, it suffices to show that the image of  $\psi$  is contained in  $Y$ . It is guaranteed by  $\Psi(0) = 0$ . Lastly note that  $\tilde{\psi} = \Psi$ .

□



## Chapter 2: Modules

### Exercise 2.1.

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

It suffices to show that

$$(\mathbb{Z}/m\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/d\mathbb{Z}$$

where  $d$  is the greatest common divisor of  $m$  and  $n$ .

*Outlines.*

- (1) Define  $\tilde{\varphi}$  by

$$\begin{array}{ccc} \tilde{\varphi}: & (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}) & \longrightarrow \mathbb{Z}/d\mathbb{Z} \\ & \Downarrow & \Downarrow \\ & (x + m\mathbb{Z}, y + n\mathbb{Z}) & \longmapsto xy + d\mathbb{Z}. \end{array}$$

$\tilde{\varphi}$  is well-defined and  $\mathbb{Z}$ -bilinear.

- (2) By the universal property,  $\tilde{\varphi}$  factors through a  $\mathbb{Z}$ -bilinear map

$$\varphi: (\mathbb{Z}/m\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/n\mathbb{Z}) \rightarrow \mathbb{Z}/d\mathbb{Z}$$

(such that  $\varphi(x \otimes y) = \tilde{\varphi}(x, y)$ ).

- (3) To show that  $\varphi$  is isomorphic, might find the inverse map  $\psi: \mathbb{Z}/d\mathbb{Z} \rightarrow (\mathbb{Z}/m\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/n\mathbb{Z})$  of  $\varphi$ . Define  $\psi$  by

$$\begin{array}{ccc} \psi: & \mathbb{Z}/d\mathbb{Z} & \longrightarrow (\mathbb{Z}/m\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/n\mathbb{Z}) \\ & \Downarrow & \Downarrow \\ & z + d\mathbb{Z} & \longmapsto (z + m\mathbb{Z}) \otimes (1 + n\mathbb{Z}). \end{array}$$

$\psi$  is well-defined and  $\mathbb{Z}$ -linear.

- (4)  $\psi \circ \varphi = \text{id}$ .

- (5)  $\varphi \circ \psi = \text{id}$ .

*Proof of (1).*

- (a)  $\tilde{\varphi}$  is well-defined. Say  $x' = x + am$  for some  $a \in \mathbb{Z}$  and  $y' = y + bn$  for some  $b \in \mathbb{Z}$ . Then  $x'y' - xy = yam + xbn + abmn \in \mathbb{Z}/d\mathbb{Z}$ . That is,  $\tilde{\varphi}$  is independent of coset representative.

(b)  $\tilde{\varphi}$  is  $\mathbb{Z}$ -bilinear.

(i) For any  $\lambda \in \mathbb{Z}$ ,  $\tilde{\varphi}(\lambda x, y) = \tilde{\varphi}(x, \lambda y) = \lambda \tilde{\varphi}(x, y)$ . In fact,

$$\begin{aligned}\tilde{\varphi}(\lambda(x + m\mathbb{Z}), y + n\mathbb{Z}) &= \tilde{\varphi}(\lambda x + m\mathbb{Z}, y + n\mathbb{Z}) = \lambda xy + d\mathbb{Z}, \\ \tilde{\varphi}(x + m\mathbb{Z}, \lambda(y + n\mathbb{Z})) &= \tilde{\varphi}(x + m\mathbb{Z}, \lambda y + n\mathbb{Z}) = \lambda xy + d\mathbb{Z}, \\ \tilde{\varphi}(x_1 + m\mathbb{Z}, y + n\mathbb{Z}) &= \lambda(xy + d\mathbb{Z}) = \lambda xy + d\mathbb{Z}.\end{aligned}$$

(ii)  $\tilde{\varphi}(x_1 + x_2, y) = \tilde{\varphi}(x_1, y) + \tilde{\varphi}(x_2, y)$ . In fact,

$$\begin{aligned}\tilde{\varphi}((x_1 + x_2) + m\mathbb{Z}, y + n\mathbb{Z}) &= (x_1 + x_2)y + d\mathbb{Z}, \\ \tilde{\varphi}(x_1 + m\mathbb{Z}, y + n\mathbb{Z}) + \tilde{\varphi}(x_2 + m\mathbb{Z}, y + n\mathbb{Z}) &= (x_1 y + d\mathbb{Z}) + (x_2 y + d\mathbb{Z}) \\ &= (x_1 + x_2)y + d\mathbb{Z}.\end{aligned}$$

(iii)  $\tilde{\varphi}(x, y_1 + y_2) = \tilde{\varphi}(x, y_1) + \tilde{\varphi}(x, y_2)$ . Similar to (ii).

□

*Proof of (3).*

(a)  $\psi$  is well-defined. Say  $z' = z + cd$  for some  $c \in \mathbb{Z}$ . Note that  $d = \alpha m + \beta n$  for some  $\alpha, \beta \in \mathbb{Z}$ . Thus

$$\begin{aligned}\psi(z' + d\mathbb{Z}) &= \psi(z + cd + d\mathbb{Z}) \\ &= \psi(z + c(\alpha m + \beta n) + d\mathbb{Z}) \\ &= (z + c(\alpha m + \beta n) + m\mathbb{Z}) \otimes (1 + n\mathbb{Z}) \\ &= (z + c\beta n + m\mathbb{Z}) \otimes (1 + n\mathbb{Z}) \\ &= (z + m\mathbb{Z}) \otimes (1 + n\mathbb{Z}) + (c\beta n + m\mathbb{Z}) \otimes (1 + n\mathbb{Z}) \\ &= \psi(z + d\mathbb{Z}) + (1 + m\mathbb{Z}) \otimes (c\beta n + n\mathbb{Z}) \\ &= \psi(z + d\mathbb{Z}).\end{aligned}$$

(b)  $\psi$  is  $\mathbb{Z}$ -linear.

(i) For any  $\lambda \in \mathbb{Z}$ ,  $\psi(\lambda z) = \lambda \psi(z)$ . In fact,

$$\begin{aligned}\psi(\lambda(z + d\mathbb{Z})) &= \psi(\lambda z + d\mathbb{Z}) = (\lambda z + m\mathbb{Z}) \otimes (1 + n\mathbb{Z}), \\ \lambda \psi(z + d\mathbb{Z}) &= \lambda((z + m\mathbb{Z}) \otimes (1 + n\mathbb{Z})) = (\lambda z + m\mathbb{Z}) \otimes (1 + n\mathbb{Z}).\end{aligned}$$

(ii)  $\psi(z_1 + z_2) = \psi(z_1) + \psi(z_2)$ .

$$\begin{aligned}\psi((z_1 + z_2) + d\mathbb{Z}) &= (z_1 + z_2 + m\mathbb{Z}) \otimes (1 + n\mathbb{Z}), \\ \psi(z_1 + d\mathbb{Z}) + \psi(z_2 + d\mathbb{Z}) &= (z_1 + m\mathbb{Z}) \otimes (1 + n\mathbb{Z}) + (z_2 + m\mathbb{Z}) \otimes (1 + n\mathbb{Z}) \\ &= (z_1 + z_2 + m\mathbb{Z}) \otimes (1 + n\mathbb{Z}).\end{aligned}$$

□

*Proof of (4).* For any  $(x + m\mathbb{Z}) \otimes (y + n\mathbb{Z}) \in (\mathbb{Z}/m\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/n\mathbb{Z})$ ,

$$\begin{aligned}\psi(\varphi((x + m\mathbb{Z}) \otimes (y + n\mathbb{Z}))) &= \psi(xy + d\mathbb{Z}) \\ &= (xy + m\mathbb{Z}) \otimes (1 + n\mathbb{Z}) \\ &= (x + m\mathbb{Z}) \otimes (y + n\mathbb{Z}).\end{aligned}$$

□

*Proof of (5).* For any  $z + d\mathbb{Z} \in \mathbb{Z}/d\mathbb{Z}$ ,

$$\begin{aligned}\varphi(\psi(z + d\mathbb{Z})) &= \varphi((z + m\mathbb{Z}) \otimes (1 + n\mathbb{Z})) \\ &= z + d\mathbb{Z}.\end{aligned}$$

□

### Exercise 2.2.

Let  $A$  be a ring,  $\mathfrak{a}$  an ideal,  $M$  an  $A$ -module. Show that  $(A/\mathfrak{a}) \otimes_A M$  is isomorphic to  $M/\mathfrak{a}M$ . (Hint: Tensor the exact sequence  $0 \rightarrow \mathfrak{a} \rightarrow A \rightarrow A/\mathfrak{a} \rightarrow 0$  with  $M$ .)

*Proof (Hint).* There is a natural exact sequence  $E$ :

$$E : 0 \rightarrow \mathfrak{a} \xrightarrow{i} A \xrightarrow{\pi} A/\mathfrak{a} \rightarrow 0$$

where  $i$  is the inclusion map (and  $\pi$  is the projection map). Tensor  $E$  with  $M$ :

$$E' : \mathfrak{a} \otimes_A M \xrightarrow{i \otimes 1} A \otimes_A M \xrightarrow{\pi \otimes 1} (A/\mathfrak{a}) \otimes_A M \rightarrow 0$$

is exact, or

$$(A/\mathfrak{a}) \otimes_A M \cong A \otimes_A M / \text{im}(i \otimes 1).$$

By Proposition 2.14, There is an unique isomorphism  $A \otimes_A M \rightarrow M$  defined by  $a \otimes x \mapsto ax$ . This isomorphism sends  $\text{im}(i \otimes 1)$  to  $\mathfrak{a}M$ . Therefore,

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

□

*Proof (Brute-force).*

(1) Define  $\tilde{\varphi}$  by

$$\begin{array}{ccc} \tilde{\varphi}: & A/\mathfrak{a} \times M & \longrightarrow M/\mathfrak{a}M \\ & \Downarrow & \Downarrow \\ & (a + \mathfrak{a}, x) & \longmapsto ax + \mathfrak{a}M. \end{array}$$

$\tilde{\varphi}$  is well-defined and  $A$ -bilinear.

- (2) By the universal property,  $\tilde{\varphi}$  factors through a  $A$ -bilinear map

$$\varphi: A/\mathfrak{a} \otimes_A M \rightarrow M/\mathfrak{a}M$$

(such that  $\varphi(a \otimes x) = \tilde{\varphi}(a, x)$ ).

- (3) To show that  $\varphi$  is isomorphic, might find the inverse map  $\psi: M/\mathfrak{a}M \rightarrow A/\mathfrak{a} \otimes_A M$  of  $\varphi$ . Define  $\psi$  by

$$\begin{array}{ccc} \psi: & M/\mathfrak{a}M & \longrightarrow A/\mathfrak{a} \otimes_A M \\ & \Downarrow & \Downarrow \\ & x + \mathfrak{a}M & \longmapsto (1 + \mathfrak{a}) \otimes x. \end{array}$$

$\psi$  is well-defined and  $A$ -linear.

- (4)  $\psi \circ \varphi = \text{id}$ .

- (5)  $\varphi \circ \psi = \text{id}$ .

□

### Exercise 2.3.

Let  $A$  be a local ring,  $M$  and  $N$  finitely generated  $A$ -modules. Prove that if  $M \otimes_A N = 0$ , then  $M = 0$  or  $N = 0$ . (Hint: Let  $\mathfrak{m}$  be the maximal ideal,  $k = A/\mathfrak{m}$  the residue field. Let  $M_k = k \otimes_A M \cong M/\mathfrak{m}M$  by Exercise 2.2. By Nakayama's lemma,  $M_k = 0 \implies M = 0$ . But  $M \otimes_A N = 0 \implies (M \otimes_A N)_k = 0 \implies M_k \otimes_k N_k = 0 \implies M_k = 0$  or  $N_k = 0$  since  $M_k, N_k$  are vector spaces over a field.)

The conclusion might be false if  $A$  is not local. For example, Exercise 2.1.

*Proof (Hint).* Let  $\mathfrak{m}$  be the maximal ideal,  $k = A/\mathfrak{m}$  the residue field. Let  $M_k = k \otimes_A M$ .

- (1) (*Base extension*) Show that  $(M \otimes_A N)_k = M_k \otimes_k N_k$ . In fact, by Proposition 2.14

$$\begin{aligned}
 (M \otimes_A N)_k &= k \otimes_A (M \otimes_A N) \\
 &= (k \otimes_A M) \otimes_A N \\
 &= M_k \otimes_A N \\
 &= (M_k \otimes_k k) \otimes_A N \\
 &= M_k \otimes_k (k \otimes_A N) \\
 &= M_k \otimes_k N_k.
 \end{aligned}$$

(2)

$$\begin{aligned}
 M \otimes_A N = 0 &\implies (M \otimes_A N)_k = 0 \\
 &\implies M_k \otimes_k N_k = 0 && ((1)) \\
 &\implies M_k = 0 \text{ or } N_k = 0 && (M_k, N_k: \text{ vector spaces}) \\
 &\implies M/\mathfrak{m}M = 0 \text{ or } M/\mathfrak{m}M = 0 && (\text{Exercise 2.2}) \\
 &\implies M = 0 \text{ or } N = 0. && (\text{Nakayama's lemma})
 \end{aligned}$$

□

#### Exercise 2.4.

Let  $M_i$  ( $i \in I$ ) be any family of  $A$ -modules, and let  $M$  be their direct sum. Prove that  $M$  is flat  $\Leftrightarrow$  each  $M_i$  is flat.

*Proof.* Given any  $A$ -module homomorphism  $f : N' \rightarrow N$ .

- (1) Similar to Proposition 2.14 (iii), we have two isomorphisms

(a)

$$\varphi : \bigoplus_{i \in I} (N' \otimes M_i) \cong N' \otimes_A \bigoplus_{i \in I} M_i$$

defined by

$$\varphi((x \otimes m_i)_{i \in I}) = x \otimes (m_i)_{i \in I}$$

where  $x \in N'$ ,  $m_i \in M_i$  ( $i \in I$ ).

(b)

$$\psi : N \otimes_A \bigoplus_{i \in I} M_i \cong \bigoplus_{i \in I} (N \otimes M_i)$$

defined by

$$\psi(y \otimes (m_i)_{i \in I}) = (y \otimes m_i)_{i \in I}$$

where  $y \in N$ ,  $m_i \in M_i$  ( $i \in I$ ).

(2)  $f : N' \rightarrow N$  induces an  $A$ -module homomorphism

$$f \otimes \text{id}_M : N' \otimes_A M \rightarrow N \otimes_A M.$$

(3)  $\psi \circ f \otimes \text{id}_M \circ \varphi$  defines an  $A$ -module homomorphism

$$\psi \circ f \otimes \text{id}_M \circ \varphi : \bigoplus_{i \in I} (N' \otimes M_i) \rightarrow \bigoplus_{i \in I} (N \otimes M_i)$$

which sends  $(x \otimes m_i)_{i \in I}$  to  $(f(x) \otimes m_i)_{i \in I}$ . That is,

$$\psi \circ f \otimes \text{id}_M \circ \varphi = \bigoplus_{i \in I} f \otimes \text{id}_{M_i}.$$

(4) Show that  $M$  is flat if and only if each  $M_i$  is flat. Suppose  $f$  is injective.

$$\begin{aligned} & M_i \text{ is flat } \forall i \in I \\ \iff & f \otimes \text{id}_{M_i} \text{ is injective } \forall i \in I \\ \iff & \bigoplus_{i \in I} f \otimes \text{id}_{M_i} \text{ is injective} && \text{(Injectivity)} \\ \iff & \psi \circ f \otimes \text{id}_M \circ \varphi \text{ is injective} && ((3)) \\ \iff & f \otimes \text{id}_M \text{ is injective} && (\varphi \text{ and } \psi \text{ are isomorphic}) \\ \iff & M \text{ is flat.} \end{aligned}$$

□

### Exercise 2.5.

Let  $A[x]$  be the ring of polynomials in one indeterminate over a ring  $A$ . Prove that  $A[x]$  is a flat  $A$ -algebra. (Hint: Use Exercise 2.4.)

*Proof (Hint).*

(1)  $A$  is a flat  $A$ -module by Proposition 2.14(iv).

(2) As an  $A$ -module,

$$A[x] \cong \bigoplus_{n \in \mathbb{Z}^+} Ax^n \cong \bigoplus_{n \in \mathbb{Z}^+} A$$

(since  $Ax^n \cong A$ ).

(3) By Exercise 2.4,  $A[x] \cong \bigoplus_{n \in \mathbb{Z}^+} A$  is flat.

□

**Exercise 2.8.**

- (i) If  $M$  and  $N$  are flat  $A$ -modules, then so is  $M \otimes_A N$ .
- (ii) If  $B$  is a flat  $A$ -algebra and  $N$  is a flat  $B$ -module, then  $N$  is flat as  $A$ -module.

*Proof of (i).* Given any exact sequence of  $A$ -modules  $0 \rightarrow N_1 \rightarrow N_2 \rightarrow N_3 \rightarrow 0$ . Since  $M$  is flat,

$$0 \rightarrow N_1 \otimes_A M \rightarrow N_2 \otimes_A M \rightarrow N_3 \otimes_A M \rightarrow 0$$

is exact. Since  $N$  is flat,

$$0 \rightarrow (N_1 \otimes_A M) \otimes_A N \rightarrow (N_2 \otimes_A M) \otimes_A N \rightarrow (N_3 \otimes_A M) \otimes_A N \rightarrow 0$$

is exact. By Proposition 2.14 (ii),

$$0 \rightarrow N_1 \otimes_A (M \otimes_A N) \rightarrow N_2 \otimes_A (M \otimes_A N) \rightarrow N_3 \otimes_A (M \otimes_A N) \rightarrow 0$$

is exact, or  $M \otimes_A N$  is flat.  $\square$

*Proof of (ii).* Given any exact sequence of  $A$ -modules  $0 \rightarrow N_1 \rightarrow N_2 \rightarrow N_3 \rightarrow 0$ . Since  $B$  is a flat  $A$ -algebra ( $A$ -module),

$$0 \rightarrow N_1 \otimes_A B \rightarrow N_2 \otimes_A B \rightarrow N_3 \otimes_A B \rightarrow 0$$

is exact. Since  $N$  is a flat  $B$ -module,

$$0 \rightarrow (N_1 \otimes_A B) \otimes_B N \rightarrow (N_2 \otimes_A B) \otimes_B N \rightarrow (N_3 \otimes_A B) \otimes_B N \rightarrow 0$$

is exact. By “Exercise 2.15” on page 27,

$$0 \rightarrow N_1 \otimes_A (B \otimes_B N) \rightarrow N_2 \otimes_A (B \otimes_B N) \rightarrow N_3 \otimes_A (B \otimes_B N) \rightarrow 0$$

is exact. By Proposition 2.14 (iv),

$$0 \rightarrow N_1 \otimes_A N \rightarrow N_2 \otimes_A N \rightarrow N_3 \otimes_A N \rightarrow 0$$

is exact, or  $N$  is flat.  $\square$

**Exercise 2.9.**

Let  $0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$  be an exact sequence of  $A$ -modules. If  $M'$  and  $M''$  are finitely generated, then so is  $M$ .

*Proof.*

(1) Write

$$0 \rightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \rightarrow 0.$$

Also write

$$\begin{aligned} x_1, \dots, x_n &\text{ as generators of } M', \\ z_1, \dots, z_m &\text{ as generators of } M'' \end{aligned}$$

(since  $M'$  and  $M''$  are finitely generated).

(2) Since the map  $g : M \rightarrow M''$  is surjective, there exists  $y_j \in M$  such that  $g(y_j) = z_j$  for  $j = 1, \dots, m$ .

(3) Show that  $M$  is generated by

$$f(x_1), \dots, f(x_n), y_1, \dots, y_m.$$

Given any  $y \in M$ .

$$\begin{aligned} y \in M &\implies g(y) \in M'' \\ &\implies g(y) = \sum_{j=1}^m s_j z_j \text{ where } s_j \in A \\ &\implies g(y) = \sum_{j=1}^m s_j g(y_j) \\ &\implies g(y) = g\left(\sum_{j=1}^m s_j y_j\right) \\ &\implies y - \sum_{j=1}^m s_j y_j \in \ker(g) = \text{im}(f) \\ &\implies \exists x \in M' \text{ such that } f(x) = y - \sum_{j=1}^m s_j y_j \end{aligned}$$

Write  $x = \sum_{i=1}^n r_i x_i$  where  $r_i \in A$ . So,

$$\begin{aligned} y \in M &\implies f\left(\sum_{i=1}^n r_i x_i\right) = y - \sum_{j=1}^m s_j y_j \\ &\implies \sum_{i=1}^n r_i f(x_i) = y - \sum_{j=1}^m s_j y_j \\ &\implies y = \sum_{i=1}^n r_i f(x_i) + \sum_{j=1}^m s_j y_j. \end{aligned}$$

Hence, every  $y \in M$  is a linear combination of  $f(x_1), \dots, f(x_n), y_1, \dots, y_m$ , or  $M$  is finitely generated (by  $f(x_1), \dots, f(x_n), y_1, \dots, y_m$ ).



