

# Chapter 1: Roots of Commutative Algebra

Author: Meng-Gen Tsai

Email: plover@gmail.com

## Noetherian Rings and Modules

**Exercise 1.1.** Prove that the following conditions on a module  $M$  over a commutative ring  $R$  are equivalent (the fourth is Hilbert's original formulation; the first and the third are the ones most often used). The case  $M = R$  is the case of ideals.

- (1)  $M$  is Noetherian (that is, every submodule of  $M$  is finitely generated).
- (2) Every ascending chain of submodules of  $M$  terminates ("ascending chain condition").
- (3) Every set of submodules of  $M$  contains elements maximal under inclusion.
- (4) Given any sequence of elements  $f_1, f_2, \dots \in M$ , there is a number  $m$  such that for each  $n > m$  there is an expression  $f_n = \sum_{i=1}^m a_i f_i$  with  $a_i \in R$ .

*Idea.* (1)  $\Rightarrow$  (2)  $\Rightarrow$  (4)  $\Rightarrow$  (3)  $\Rightarrow$  (1).

*Proof of (1)  $\Rightarrow$  (2).* Given any ascending chain of submodules  $N_1 \subseteq N_2 \subseteq \dots$ , let

$$N = \bigcup_{i=1}^{\infty} N_i.$$

- (a)  $N$  is a submodule. By the ascending chain condition, each pair of elements in  $N$  are in a common  $N_m$ .
- (b)  $N$  is finitely generated by assumption. By the ascending chain condition again, all generators of  $N$  are in a common  $N_m$ . So  $N = N_m$  for some  $m$ .
- (c) Since  $N_m = N \supseteq N_n$  whenever  $n \geq m$ ,  $N_m = N_{m+1} = \dots$ .

□

*Proof of (2)  $\Rightarrow$  (4).* Let  $N_k$  be generated by  $f_1, f_2, \dots, f_k$ .

- (a)  $N_1 \subseteq N_2 \subseteq \dots$  is an ascending chain of submodules of  $M$ .
- (b) By assumption there is a number  $m$  such that  $N_m = N_{m+1} = \dots$ .

- (c) Given any  $n \geq m$ ,  $f_n \in N_n = N_m$ . So we can write  $f_n = \sum_{i=1}^m a_i f_i$  with  $a_i \in R$  since  $N_m$  is generated by  $f_1, f_2, \dots, f_m$ .

□

*Proof of (4)  $\Rightarrow$  (3).* It suffices to show that  $\neg(3) \Rightarrow \neg(4)$ . There exists a nonempty collection  $\Sigma$  of submodules of  $M$  containing no maximal element under inclusion.

- (a) Start with any submodule  $N_1$  in  $\Sigma$ , and recursively pick submodule  $N_2, N_3, \dots$  such that  $N_1 \subsetneq N_2 \subsetneq N_3 \subsetneq \dots$ .
- (b) Pick  $f_1 \in N_1$  and  $f_i \in N_i - N_{i-1} \neq \emptyset$  for  $i \geq 2$ . The sequence of elements  $f_1, f_2, \dots \in M$  is what we want.

□

*Proof of (3)  $\Rightarrow$  (1).* Show that  $N$  is finitely generated if  $N$  is any submodule of  $M$ . Let  $\Sigma$  be the set of all finitely generated submodules of  $N$ .

- (a)  $\Sigma \neq \emptyset$  since  $0$  is a finitely generated submodules of  $N$ .
- (b) By assumption, there exists a maximal element  $N_0$  of  $\Sigma$ .  $N_0$  is finitely generated.
- (c) (Reductio ad absurdum) If  $N_0$  were not equal to  $N$ , there is  $x \in N - N_0$ . Clearly the submodule  $N_0 + xR$  of  $N$  is finitely generated and  $N_0 + xR \supsetneq N_0$ , contrary to the maximality of  $N_0$ .

□

*Proof of (2)  $\Rightarrow$  (3).* It is the part (a) of the proof of (4)  $\Rightarrow$  (3). □

*Proof of (3)  $\Rightarrow$  (2).* Given any ascending chain of submodules  $N_1 \subseteq N_2 \subseteq \dots$ . The set

$$\Sigma = \{N_i\}_{i \geq 1}$$

has a maximal element, say  $N_m$ . Hence  $N_m = N_{m+1} = \dots$  by the maximality of  $N_m$ . □

**Remark.** In general, let  $\Sigma$  be a set partially ordered by a relation  $\leq$ . Then the following conditions on  $\Sigma$  are equivalent:

- (1) Every increasing sequence  $x_1 \leq x_2 \leq \dots \in \Sigma$  is stationary.
- (2) Every non-empty subset of  $\Sigma$  has a maximal element.

**Exercise 1.2 (Emmy Noether).** Prove that if  $R$  is Noetherian, and  $I \subsetneq R$  is an ideal, then among the primes of  $R$  containing  $I$  there are only finitely many that are minimal with respect to inclusion (these are usually called the **minimal primes of  $I$** , or the **primes minimal over  $I$** ) as follows: Assuming that the proposition fails, the Noetherian hypothesis guarantees the existence of an ideal  $I$  maximal among ideals in  $R$  for which it fails. Show that  $I$  cannot be prime, so we can find elements  $f$  and  $g$  in  $R$ , not in  $I$ , such that  $fg \in I$ . Now show that every prime minimal over  $I$  is minimal over one of the larger ideals  $(I, f)$  and  $(I, g)$ .

*Note.* With Hilbert's basis theorem and the Nullstellensatz (see Exercise 1.9), Exercise 1.2 gives one of the fundamental finiteness theorems of algebraic geometry: An algebraic set can have only finitely many irreducible components. Originally the result was proved by difficult inductive arguments and elimination theory. For a further discussion of the significance of this result see the beginning of Chapter 3, and particularly example 2 there. The result of this exercise is strengthened in Theorem 3.1.

**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  $\mathfrak{p} \supseteq \mathfrak{b}$ .  $\square$

*Proof.* (Reductio ad absurdum)

- (1) Assuming that the proposition fails, the Noetherian hypothesis of  $R$  guarantees the existence of an ideal  $I$  maximal among ideals in  $R$  for which it fails.
- (2) Show that  $I$  cannot be prime. (Reductio ad absurdum) If  $I$  were prime, then there were only one minimal prime  $I$  itself, which is absurd.
- (3) Therefore, there exist elements  $f, g \in R$  such that  $fg \in I$  but  $f \notin I$  and  $g \notin I$ .  $(I, f) \supsetneq I$ ,  $(I, g) \supsetneq I$  and  $(I, f)(I, g) \subseteq I$ .
- (4) By Lemma, any prime containing  $I$  must contain either  $(I, f)$  or  $(I, g)$ . In particular, any prime minimal over  $I$  is minimal over either  $(I, f)$  or  $(I, g)$ . However, by the choice of  $I$ , both  $(I, f)$  and  $(I, g)$  have only finitely many minimal primes, which is absurd.

$\square$

**Exercise 1.3.** Let  $M'$  be a submodule of  $M$ . Show that  $M$  is Noetherian iff both  $M'$  and  $M/M'$  are Noetherian.

*Proof.*

(1) ( $\implies$ )

- (a) Show that  $M'$  is Noetherian if  $M$  is Noetherian. This is an immediate consequence of the definition of a Noetherian module since a submodule of a submodule is a submodule.
- (b) Show that  $M/M'$  is Noetherian if  $M$  is Noetherian. Every submodule of  $M/M'$  has the form  $M''/M'$  where  $M''$  is a submodule of  $M$  with  $M' \subseteq M'' \subseteq M$ . Since  $M$  is Noetherian,  $M''$  is finitely generated, and the reduction of those generators mod  $M'$  will generate  $M''/M'$  as a finitely generated module.

(2) ( $\impliedby$ )

- (a) Given any submodule  $M''$  of  $M$ . Then the image of  $M''$  in  $M/M'$  is finitely generated and  $M'' \cap M'$  is finitely generated too.
- (b) Say  $x_1, \dots, x_k \in M''$  generate the image of  $M''$  in  $M/M'$  and say  $y_1, \dots, y_h \in M''$  generate  $M'' \cap M'$ .
- (c) Given any  $x \in M''$ , we have

$$\begin{aligned}
 x &\equiv r_1x_1 + \dots + r_kx_k \pmod{M'} \text{ for some } r_i \in R \\
 \implies x - \sum_{i=1}^k r_ix_k &\equiv 0 \pmod{M'} \\
 \implies x - \sum_{i=1}^k r_ix_k &\in M' \\
 \implies x - \sum_{i=1}^k r_ix_k &\in M'' \cap M' \\
 \implies x - \sum_{i=1}^k r_ix_k &= \sum_{j=1}^h s_jy_j \text{ for some } s_j \in R \\
 \implies x &= \sum_{i=1}^k r_ix_k + \sum_{j=1}^h s_jy_j \\
 \implies x &\text{ is generated by } x_1, \dots, x_k, y_1, \dots, y_h
 \end{aligned}$$

Hence  $M''$  is finitely generated for any submodule  $M''$  of  $M$ , that is,  $M$  is Noetherian.

□

## Algebra and Geometry

**Exercise 1.8 (A formal Nullstellensatz).** Let  $\mathcal{X}$  and  $\mathcal{J}$  be partially ordered sets, and suppose that  $I : \mathcal{X} \rightarrow \mathcal{J}$  and  $Z : \mathcal{J} \rightarrow \mathcal{X}$  are functions such that

- (i)  $I$  and  $Z$  reverse the order in the sense that  $x \leq y \in \mathcal{X}$  implies  $I(x) \geq I(y)$ , and  $i \leq j \in \mathcal{J}$  implies  $Z(i) \geq Z(j)$ .
  - (ii)  $ZI$  and  $IZ$  are increasing functions, in the sense that  $x \in \mathcal{X}$  implies  $ZI(x) \geq x$ , and  $i \in \mathcal{J}$  implies  $IZ(i) \geq i$ .
- (a) Show that  $I$  and  $Z$  establish a one-to-one correspondence between the subsets  $I(\mathcal{X}) \subseteq \mathcal{J}$  and  $Z(\mathcal{J}) \subseteq \mathcal{X}$ .
  - (b) Let  $k$  be a field. Call an ideal  $I \subseteq k[x_1, \dots, x_n]$  **formally radical** if it is of the form  $I(X)$  for some set  $X \subseteq k^n$ . Use part (a) to prove that there is a one-to-one correspondence between formally radical ideals and algebraic subsets of  $k^n$ . (Hilbert's Nullstellensatz identifies the formally radical ideals with the ordinary radical ideals when  $k$  is algebraically closed.)

*Proof of (a).*

- (1) It suffices to show that  $IZ$  is the identity map on  $I(\mathcal{X})$  and  $ZI$  is the identity map on  $Z(\mathcal{J})$ . By symmetry, it suffices to show the first statement.
- (2) Given any  $y \in I(\mathcal{X})$ , there exists  $x \in \mathcal{X}$  such that  $y = I(x)$ . Take  $IZ$  on the both sides, we have  $IZ(y) \geq y$  by (ii). Hence  $IZI(x) \geq I(x)$ .
- (3) Besides,  $ZI(x) \geq x$  by (ii). Take  $I$  on the both sides, we have  $I(x) \geq IZI(x)$  by (i). Since  $\mathcal{J}$  is a partially ordered set,  $I(x) = IZI(x)$  or  $y = IZ(y)$  for all  $y \in I(\mathcal{X})$ , or  $IZ$  is the identity map on  $I(\mathcal{X})$ .

□

*Proof of (b).*

- (1) Let

$$\begin{aligned}\mathcal{X} &= \{\text{subsets } X \subseteq k^n\}, \\ \mathcal{J} &= \{\text{ideals } \mathfrak{a} \subseteq k[x_1, \dots, x_n]\}.\end{aligned}$$

Define the partially order of  $\mathcal{X}$  or  $\mathcal{J}$  by the set inclusion.

- (2) Let  $I : \mathcal{X} \rightarrow \mathcal{J}$  defined by

$$I(X) = \{f \in k[x_1, \dots, x_n] : f(a_1, \dots, a_n) = 0 \forall (a_1, \dots, a_n) \in X\}$$

and  $Z : \mathcal{J} \rightarrow \mathcal{X}$  defined by

$$Z(\mathfrak{a}) = \{(a_1, \dots, a_n) \in k^n : f(a_1, \dots, a_n) = 0 \forall f \in \mathfrak{a}\}.$$

(3) It is clear that

(a)  $I(X) \supseteq I(Y)$  if  $Y \supseteq X$ .

(b)  $Z(\mathfrak{a}) \supseteq Z(\mathfrak{b})$  if  $\mathfrak{b} \supseteq \mathfrak{a}$ .

(c)  $ZI(X) \supseteq X$  and  $IZ(\mathfrak{a}) \supseteq \mathfrak{a}$ .

(4) By (a), there a one-to-one correspondence between the subsets  $I(\mathcal{X}) \subseteq \mathcal{J}$  and  $Z(\mathcal{J}) \subseteq \mathcal{X}$ , or there a one-to-one correspondence between formally radical ideals and algebraic subsets of  $k^n$ .

□

**Exercise 1.12.** Find equations for a parabola meeting a circle just once in the complex plane, represented by Figure 1.5 (see the textbook).

*Proof.*

$$\begin{cases} x^2 + (y - 1)^2 - 1 = 0 \\ x^2 - 2y = 0 \end{cases}$$

meets at  $(0, 0)$ . □