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 $f_1, f_2, \ldots \in M$, 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 $N_1 \subseteq N_2 \subseteq \cdots$, 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 $n \geq m$, $N_m = N_{m+1} = \cdots$.

□

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

(a) $N_1 \subseteq N_2 \subseteq \cdots$ is an ascending chain of submodules of M.

(b) By assumption there is a number m such that $N_m = N_{m+1} = \cdots$.

(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 $f_1, f_2, \ldots, f_m$.

$\square$

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

(a) Start with any submodule N_1 in Σ, and recursively pick submodule $N_2, N_3, \ldots$ such that $N_1 \subsetneq N_2 \subsetneq N_3 \subsetneq \cdots$.

(b) Pick $f_1 \in N_1$ and $f_i \in N_i - N_{i-1} \neq \varnothing$ for $i \geq 2$. The sequence of elements $f_1, f_2, \ldots \in M$ is what we want.

$\square$

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

(a) $\Sigma \neq \varnothing$ since 0 is a finitely generated submodules of N.

(b) By assumption, there exists a maximal element N_0 of Σ. 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.

$\square$

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

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

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

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

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

(1) Every increasing sequence $x_1 \leq x_2 \leq \cdots \in \Sigma$ is stationary.

(2) Every non-empty subset of Σ 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 reslt 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) ($\Longrightarrow$)

(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) ($\Longleftarrow$)

(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 $x_1, \ldots, x_k \in M''$ generate the image of M'' in M/M' and say $y_1, \ldots, y_h \in M''$ generate $M'' \cap M'$.

(c) Given any $x \in M''$, we have

$$\begin{aligned}
& x \equiv r_1 x_1 + \cdots + r_k x_k \pmod{M'} \text{ for some } r_i \in R \\
\Longrightarrow & x - \sum_{i=1}^{k} r_i x_k \equiv 0 \pmod{M'} \\
\Longrightarrow & x - \sum_{i=1}^{k} r_i x_k \in M' \\
\Longrightarrow & x - \sum_{i=1}^{k} r_i x_k \in M'' \cap M' \\
\Longrightarrow & x - \sum_{i=1}^{k} r_i x_k = \sum_{j=1}^{h} s_j y_j \text{ for some } s_j \in R \\
\Longrightarrow & x = \sum_{i=1}^{k} r_i x_k + \sum_{j=1}^{h} s_j y_j \\
\Longrightarrow & x \text{ is generated by } x_1, \ldots, x_k, y_1, \ldots, y_h
\end{aligned}$$

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 $I : \mathcal{X} \to \mathcal{J}$ and $Z : \mathcal{J} \to \mathcal{X}$ 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 $I \subseteq k[x_1, \ldots, x_n]$* ***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

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

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

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

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

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

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

(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 1.9. *Let $S = k[x_1, \ldots, x_r]$, with k an algebraically closed field. Show that under the correspondence of radical ideals in S and algebraic subsets of $\mathbb{A}^r$, the primes ideals correspond to the algebraic sets that cannot be written as a proper union of smaller algebraic sets.*

Proof. Let $I(X)$ be a prime ideal where X is some subset of k^n.

(1) (Reductio ad absurdum) If X were a proper union of smaller algebraic sets, write $X = X_1 \cup X_2$ where $X_1 \subsetneq X$ and $X_2 \subsetneq X$.

(2) Therefore, $I(X_1) \supsetneq I(X)$ and $I(X_2) \supsetneq I(X)$ (Exercise 1.8). Now we can take $f \in I(X_1) - I(X)$ and $g \in I(X_2) - I(X)$.

(3) By the definition of I,

$$f(P) = 0 \,\forall\, P \in X_1,$$
$$g(P) = 0 \,\forall\, P \in X_2,$$

or

$$f(P)g(P) = 0 \,\forall\, P \in X_1 \cup X_2 = X,$$

or $fg \in I(X)$.

(4) Since $I(X)$ is prime, $f \in I(X)$ or $g \in I(X)$, which is absurd.

□

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 $(0,0)$. $\square$

Exercise 1.13. *Suppose that I is an ideal in a commutative ring. Show that if $\mathrm{rad}(I)$ is finitely generated, then for some integer N we have $(\mathrm{rad}(I))^N \subseteq I$. Conclude that in a Noetherian ring the ideals I and J have the same radical iff there is some integer N such that $I^N \subseteq J$ and $J^N \subseteq I$. Use the Nullstellensatz to deduce that if $I, J \subseteq S = k[x_1, \ldots, x_n]$ are ideals and k is algebraically closed, then $Z(I) = Z(J)$ iff $I^N \subseteq J$ and $J^N \subseteq I$ for some N.*

Proof.

(1) *Show that if $\mathrm{rad}(I)$ is finitely generated, then for some integer N we have $(\mathrm{rad}(I))^N \subseteq I$.* Say $x_1, \ldots, x_m \in \mathrm{rad}(I)$ generate $\mathrm{rad}(I)$.

  (a) For each i, there exists an integer $n_i > 0$ such that $x_i^{n_i} \in I$ (since $\mathrm{rad}(I)$ is radical).

  (b) Let $N = n_1 + \cdots + n_m$. Given any $x = \sum_{i=1}^m r_i x_i \in \mathrm{rad}(I)$, so

$$\begin{aligned} x^N &= \left(\sum_{i=1}^m r_i x_i \right)^N \\ &= \sum_{k_1 + \cdots + k_m = N} \binom{N}{k_1, \ldots, k_m} r_1^{k_1} x_1^{k_1} \cdots r_m^{k_m} x_m^{k_m}. \end{aligned}$$

  (c) Note that for each term there is some j such that $k_j \geq n_j$. Hence,

$$\begin{aligned} & x_j^{k_j} = x_j^{k_j - n_j} x_j^{n_j} \in I && (I \text{ is an ideal}) \\ \Longrightarrow & r_1^{k_1} x_1^{k_1} \cdots r_m^{k_m} x_m^{k_m} \in I \text{ for each term} && (I \text{ is an ideal}) \\ \Longrightarrow & x^N \in I. && (I \text{ is an ideal}) \\ \Longrightarrow & (\mathrm{rad}(I))^N \subseteq I. \end{aligned}$$

(2) *Show that in a Noetherian ring the ideals I and J have the same radical iff there is some integer N such that $I^N \subseteq J$ and $J^N \subseteq I$.*

  (a) ($\Longrightarrow$) Since in a Noetherian ring every ideal is finitely generated, $\mathrm{rad}(I)$ and $\mathrm{rad}(J)$ are finitely generated. By (1), there is a common integer N such that

$$(\mathrm{rad}(I))^N \subseteq I \quad \text{and} \quad (\mathrm{rad}(J))^N \subseteq J.$$

  Note that $I^N \subseteq (\mathrm{rad}(I))^N$ and $J^N \subseteq (\mathrm{rad}(J))^N$. Since $\mathrm{rad}(I) = \mathrm{rad}(J)$ by assumption,

$$\begin{aligned} I^N &\subseteq (\mathrm{rad}(I))^N = (\mathrm{rad}(J))^N \subseteq J, \\ J^N &\subseteq (\mathrm{rad}(J))^N = (\mathrm{rad}(I))^N \subseteq I. \end{aligned}$$

(b) ($\Longleftarrow$) It suffices to show that $\text{rad}(I) \subseteq \text{rad}(J)$. $\text{rad}(J) \subseteq \text{rad}(I)$ is similar. Given any $x \in \text{rad}(I)$, there is an integer $M > 0$ such that $x^M \in I$. Hence $x^{MN} \in I^N \subseteq J$, or $x \in \text{rad}(J)$.

(3) *Show that if $I, J \subseteq S = k[x_1, \ldots, x_n]$ are ideals and k is algebraically closed, then $Z(I) = Z(J)$ iff $I^N \subseteq J$ and $J^N \subseteq I$ for some N.* Note that S is Noetherian and we can apply part (2). By the Nullstellensatz, $Z(I) = Z(J)$ iff $\text{rad}(I) = \text{rad}(J)$ iff $I^N \subseteq J$ and $J^N \subseteq I$ for some N.

$\square$