

Commutative Algebra notes

arnaucube

Abstract

Notes taken while studying Commutative Algebra, mostly from Atiyah & MacDonald book [1] and Reid's book [2].

Usually while reading books and papers I take handwritten notes in a notebook, this document contains some of them re-written to *LaTeX*.

The proofs may slightly differ from the ones from the books, since I try to extend them for a deeper understanding.

Contents

1	Ideals	1
1.1	Definitions	1
1.2	Lemmas, propositions and corollaries	1
2	Modules	2
2.1	Modules	2
2.2	Cayley-Hamilton theorem, Nakayama lemma, and corollaries . .	2
2.3	Noetherian rings	7
3	Exercises	7
3.1	Exercises Chapter 1	7
3.2	Exercises Chapter 2	9

1 Ideals

1.1 Definitions

1.2 Lemmas, propositions and corollaries

Theorem 1.X. Zorn's lemma TODO

Theorem 1.3. Every ring $A \neq 0$ has at least one maximal ideal.

Proof. By Zorn's lemma 1.X. □

Corollary 1.4. if $I \neq (1)$ an ideal of A , \exists a maximal ideal of A containing I .

Corollary 1.5. Every non-unit of A is contained in a maximal ideal.

Definition Jacobson radical. The *Jacobson radical* of a ring A is the intersection of all the maximal ideals of A .

Denoted $Jac(A)$.

$Jac(A)$ is an ideal of A .

Proposition 1.9. $x \in Jac(A)$ iff $(1 - xy)$ is a unit in A , $\forall y \in A$.

Proof. Suppose $1 - xy$ not a unit.

By 1.5, $1 - xy \in \mathfrak{m}$ for \mathfrak{m} some maximal ideal.

But $x \in Jac(A) \subseteq \mathfrak{m}$, since $Jac(A)$ is the intersection of all maximal ideals of A .

Hence $xy \in \mathfrak{m}$, and therefore $1 \in \mathfrak{m}$, which is absurd, thus $1 - xy$ is a unit.

Conversely:

Suppose $x \notin \mathfrak{m}$ for some maximal ideal \mathfrak{m} .

Then \mathfrak{m} and x generate the unit ideal (1), so that we have $u + xy = 1$ for some $u \in \mathfrak{m}$ and some $y \in A$.

Hence $1 - xy \in \mathfrak{m}$, and is therefore not a unit. \square

2 Modules

2.1 Modules

2.2 Cayley-Hamilton theorem, Nakayama lemma, and corollaries

Proposition 2.4. (Cayley-Hamilton Theorem) Let M a fingen A -module. Let \mathfrak{a} an ideal of A , let ψ an A -module endomorphism of M such that $\psi(M) \subseteq \mathfrak{a}M$.

Then ψ satisfies

$$\psi^n + a_1\psi^{n-1} + \dots + a_{n-1}\psi + a_n = 0$$

with $a_i \in \mathfrak{a}$.

Proof. Since M fingen, let $\{x_1, \dots, x_n\}$ be generators of M .

By hypothesis, $\psi(M) \subseteq \mathfrak{a}M$; so for any generator x_i , it's image $\psi(x_i) \in \mathfrak{a}M$.

Any element in $\mathfrak{a}M$ is a linear combination of the generators with coefficients in the ideal \mathfrak{a} , thus

$$\psi(x_i) = \sum_{j=1}^n a_{ij}x_j$$

with $a_{ij} \in \mathfrak{a}$.

Thus, for a module with n generators, we have n different $\psi(x_i)$ equations:

$$\left. \begin{array}{l} \psi(x_1) = a_{1,1}x_1 + a_{1,2}x_2 + \dots + a_{1,n}x_n \\ \psi(x_2) = a_{2,1}x_1 + a_{2,2}x_2 + \dots + a_{2,n}x_n \\ \dots \\ \psi(x_n) = a_{n,1}x_1 + a_{n,2}x_2 + \dots + a_{n,n}x_n \end{array} \right\} \begin{array}{l} n \text{ elements } \psi(x_i) \in \mathfrak{a}M \text{ which} \\ \text{are linear combinations of the} \\ n \text{ generators of } M \end{array}$$

Next step: rearrange in order to use matrix algebra.

Observe that each row equals 0, and rearranging the elements at each row we get

$$\begin{aligned}\psi(x_1) - (a_{1,1}x_1 + a_{1,2}x_2 + \dots + a_{1,n}x_n) &= 0 \\ \psi(x_2) - (a_{2,1}x_1 + a_{2,2}x_2 + \dots + a_{2,n}x_n) &= 0 \\ \dots \\ \psi(x_n) - (a_{n,1}x_1 + a_{n,2}x_2 + \dots + a_{n,n}x_n) &= 0\end{aligned}$$

Then, group the x_i terms together; as example, take the row $i = 1$:

$$(\psi - a_{1,1})x_1 - a_{1,2}x_2 - \dots - a_{1,n}x_n = 0$$

for $i = 2$:

$$-a_{2,1}x_1 + (\psi - a_{2,2})x_2 - \dots - a_{2,n}x_n = 0$$

So, $\forall i \in [n]$, as a matrix:

$$\begin{pmatrix} \psi - a_{1,1} & -a_{1,2} & \dots & -a_{1,n} \\ -a_{2,1} & \psi - a_{2,2} & \dots & -a_{2,n} \\ \vdots & & & \\ -a_{n,1} & -a_{n,2} & \dots & \psi - a_{n,n} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Kronecker delta: $\delta_{ij} = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{otherwise} \end{cases}$

With the Kronecker delta, $\psi(x_i)$ can be expressed as

$$\psi(x_i) = \sum_{j=1}^n \delta_{ij} \psi(x_j)$$

so the previous matrix can be characterized as

$$\sum_{j=1}^n (\delta_{ij} \psi - a_{ij}) x_j = 0$$

The entries of the matrix are *endomorphisms* (elements of the ring $A[\psi]$)

- the term $(\psi - a_{11})$ is an operator that acts on x_1 ; as $(\psi(x_1) - a_{11} \cdot x_1)$
- the term $(-a_{12})$ is an operator that acts on x_2 ; as multiplication by it, ie. $(-a_{12} \cdot x_2)$

Since A is a commutative ring, and ψ commutes with any $a \in A$, the ring of operators $A[\psi]$ is a commutative ring.

\implies so we can treat the matrix as a matrix of real numbers and calculate its determinant.

We're interested in the determinant because it is the only way to turn a system of multiple equations in a single scalar-like equation that describes the endomorphism ψ .

→ Because in module theory, we lack of "division", so can not "solve for ψ " the system of equations.

→ The determinant provides a way to find a polynomial that *annihilates* the module; the *characteristic polynomial*, which related ψ to the ideal \mathfrak{a}

$$\det(M) \cdot x_i = 0 \quad \forall i$$

where x_i are the generators of M .

Since $\det(M)$ kills every generator, it must kill every element in M

⇒ $\det(M)$ is the zero map.

Leibniz formula of the determinant of an $n \times n$ matrix:

$$\det(M) = \sum_{\sigma \in S_n} \text{sign}(\sigma) \prod_{i=1}^n M_{i, \sigma(i)}$$

so,

$$(\psi - a_{11})(\psi - a_{22}) \dots (\psi - a_{nn})$$

expanding it,

- highest power is $1 \cdot \psi^n$
- coefficient of ψ^{n-1} is $-(\underbrace{a_{11} + a_{22} + \dots + a_{nn}}_{a_1})$,

where, since each $a_{ii} \in \mathfrak{a}$, $a_1 \in \mathfrak{a}$

- the rest of coefficients of ψ^k are also elements in \mathfrak{a}

So we have

$$p(\psi) = \psi^n + a_1 \psi^{n-1} + a_2 \psi^{n-2} + \dots + a_{n-1} \psi + a_n$$

with $a_i \in \mathfrak{a}$.

Since this determinant annihilates the generators (ie. $\det(M)x_i = 0$), the resulting endomorphism $p(\psi)$ is the zero map on the entire module M , so:

$$\psi^n + a_1 \psi^{n-1} + a_2 \psi^{n-2} + \dots + a_{n-1} \psi + a_n = 0$$

with $a_i \in \mathfrak{a}$, as stated in the Cayley-Hamilton theorem. □

Corollary 2.5. Let M a finitely generated A -module, let \mathfrak{a} an ideal of A such that $\mathfrak{a}M = M$.

Then, $\exists x \equiv 1 \pmod{\mathfrak{a}}$ such that $xM = 0$.

Proof. take $\psi = \text{identity}$. Then in Cayley-Hamilton (2.4):

$$\begin{aligned} & \psi^n + a_1\psi^{n-1} + a_2\psi^{n-2} + \dots + a_{n-1}\psi + a_n = 0 \\ \implies & id_M + a_1id_M + a_2id_M + \dots + a_{n-1}id_M + a_n = 0 \\ \implies & (1 + a_1 + \dots + a_n)id_M = 0 \end{aligned}$$

apply it to $m \in M$, where since $id_M(m) = m$ (by definition of the identity), we then have

$$(1 + a_1 + \dots + a_n) \cdot m = 0$$

with $a_i \in \mathfrak{a}$.

part i. $xM = 0$:

Thus the scalar $x = (1 + a_1 + \dots + a_n)$ annihilates every $m \in M$, ie. the entire module M .

part ii. $x \equiv 1 \pmod{\mathfrak{a}}$:

$x \equiv 1 \pmod{\mathfrak{a}} \iff (x - 1) \in \mathfrak{a}$
then from $x = (1 + \underbrace{a_1 + \dots + a_n}_b) \in \mathfrak{a}$, set $b = a_1 + \dots + a_n$,

so that $x = (1 + b) \in \mathfrak{a}$.

Then $x - 1 = (1 + b) - 1 = b \in \mathfrak{a}$
so $x - 1 \in \mathfrak{a}$, thus $x \equiv 1 \pmod{\mathfrak{a}}$ as stated.

□

Proposition 2.6. Nakayama's lemma Let M a fingen A -module, let \mathfrak{a} an ideal of A such that $\mathfrak{a} \subseteq \text{Jac}(A)$.

Then $\mathfrak{a}M = M$ implies $M = 0$.

Proof. By 2.5: since $\mathfrak{a}M = M$, we have $xM = 0$ for some $x \equiv 1 \pmod{\text{Jac}(A)}$. (notice that at 2.5 is $\pmod{\mathfrak{a}}$ but here we use $\pmod{\text{Jac}(A)}$), since we have $\mathfrak{a} \subseteq \text{Jac}(A)$.

By 1.9, x is a unit in A .

Hence $M = x^{-1} \cdot \underbrace{x \cdot M}_{=0 \text{ (by 2.5)}} = 0$.

Thus, if $\mathfrak{a}M = M$ then $M = 0$.

□

Corollary 2.7. Let M a fingen A -module, let $N \subseteq M$ a submodule of M , let $\mathfrak{a} \subseteq \text{Jac}(A)$ an ideal.

Then $M = \mathfrak{a}M + N \xrightarrow{\text{implies}} M = N$.

Proof. The idea is to apply Nakayama (2.6) to M/N .

Since M fingen $\implies M/N$ is fingen and an A -module.

Since $\mathfrak{a} \subseteq \text{Jac}(A) \implies$ Nakayama applies to M/N too.

By definition,

$$\mathfrak{a}M = \left\{ \sum a_i \cdot m_i \mid a_i \in \mathfrak{a}, m_i \in M \right\}$$

where m_i are the generators of M .

Then, for M/N ,

$$\mathfrak{a}\left(\frac{M}{N}\right) = \left\{ \sum a_i \cdot (m_i + N) \mid a_i \in \mathfrak{a}, m_i \in M \right\}$$

observe that $a_i(m_i + N) = a_i m_i + N$, thus

$$\sum_i a_i \cdot (m_i + N) = \underbrace{\left(\sum_i a_i \cdot m_i \right)}_{\in \mathfrak{a}M} + N \in \mathfrak{a}M + N$$

Hence,

$$\mathfrak{a}\left(\frac{M}{N}\right) = \{x + N \mid x \in \mathfrak{a}M\} = \mathfrak{a}M + N \quad (1)$$

By definition, if we take $\frac{\mathfrak{a}M + N}{N}$, then

$$\frac{\mathfrak{a}M + N}{N} = \{y + N \mid y \in \mathfrak{a}M + N\} = \mathfrak{a}M + N$$

thus every $y \in \mathfrak{a}M + N$ can be written as

$$y = x + n, \text{ with } x \in \mathfrak{a}M, n \in N$$

which comes from (1).

Thus, $y + N = (x + n) + N = x + N$, since $n \in N$ is zero in the quotient.

Hence, every element of $\frac{\mathfrak{a}M + N}{N}$ has the form

$$\frac{\mathfrak{a}M + N}{N} = \{x + N \mid x \in \mathfrak{a}M\}$$

as in (1).

Thus

$$\mathfrak{a}\left(\frac{M}{N}\right) = \mathfrak{a}M + N = \frac{\mathfrak{a}M + N}{N} \quad (2)$$

By the Collorary assumption, $M = \mathfrak{a}M + N$; quotient it by N :

$$\frac{M}{N} = \frac{\mathfrak{a}M + N}{N} \quad (3)$$

So, from (2) and (3):

$$\mathfrak{a}\left(\frac{M}{N}\right) = \mathfrak{a}M + N = \frac{\mathfrak{a}M + N}{N} = \frac{M}{N}$$

thus, $\mathfrak{a}(\frac{M}{N}) = \frac{M}{N}$.

By Nakayama's lemma 2.6, if $\mathfrak{a}(\frac{M}{N}) = \frac{M}{N} \xRightarrow{\text{implies}} \frac{M}{N} = 0$

Note that

$$\frac{M}{N} = \{m + N \mid m \in M\}$$

(the zero element in $\frac{M}{N}$ is the coset $N = 0 + N$)

Then, $\frac{M}{N} = 0$ means that the quotient has exactly one element, the zero coset N .

Thus, every coset $m + N$ equals the zero coset N , so $m - 0 \in N \implies m \in N$.

Hence every $m \in M$ lies in N , ie. $\forall m \in M, m \in N$.

So $M \subseteq N$. But notice that by the Corollary, we had $N \subseteq M$, therefore $M = N$.

Thus, if $M = \mathfrak{a}M + N \xRightarrow{\text{implies}} M = N$. □

Proposition 2.8. Let $x_i \forall i \in [n]$ be elements of M whose images $\frac{M}{mM}$ form a basis of this vector space. Then the x_i generate M .

Proof. Let N submodule M , generated by the x_i .

Then the composite map $N \longrightarrow M \longrightarrow \frac{M}{mM}$ maps N onto $\frac{M}{mM}$, hence $N + \mathfrak{a}M = M$, which by 2.7 implies $N = M$. □

2.3 Noetherian rings

3 Exercises

For the exercises, I follow the assignments listed at [3].

The exercises that start with **R** are the ones from the book [2], and the ones starting with **AM** are the ones from the book [1].

3.1 Exercises Chapter 1

Exercise R.1.1. Ring A and ideals I, J such that $I \cup J$ is not an ideal. What's the smallest ideal containing I and J ?

Proof. Take ring $A = \mathbb{Z}$. Set $I = 2\mathbb{Z}$, $J = 3\mathbb{Z}$.

I, J are ideals of $A (= \mathbb{Z})$. And $I \cup J = 2\mathbb{Z} \cup 3\mathbb{Z}$.

Observe that for $2 \in I, 3 \in J \implies 2, 3 \in I \cup J$, but $2 + 3 = 5 \notin I \cup J$.

Thus $I \cup J$ is not closed under addition; thus is not an ideal.

Smallest ideal of $\mathbb{Z} (= A)$ containing I and J is their sum:

$$I + J = \{a + b \mid a \in I, b \in J\}$$

$\gcd(2, 3) = 1$, so $I + J = \mathbb{Z}$.

Therefore, smallest ideal containing I and J is the whole ring \mathbb{Z} . □

Exercise R.1.5. let $\psi : A \longrightarrow B$ a ring homomorphism. Prove that ψ^{-1} takes prime ideals of B to prime ideals of A .
In particular if $A \subset B$ and P a prime ideal of B , then $A \cap P$ is a prime ideal of A .

Proof. (Recall: prime ideal is if $a, b \in R$ and $a \cdot b \in P$ (with $R \neq P$), implies $a \in P$ or $b \in P$).

Let

$$\psi^{-1}(P) = \{a \in A \mid \psi(a) \in P\} = A \cap P$$

The claim is that $\psi^{-1}(P)$ is prime ideal of A .

i. show that $\psi^{-1}(P)$ is an ideal of A :

$0_A \in \psi^{-1}(P)$, since $\psi(0_A) = 0_B \in P$ (since every ideal contains 0).

If $a, b \in \psi^{-1}(P)$, then $\psi(a), \psi(b) \in P$, so

$$\psi(a - b) = \psi(a) - \psi(b) \in P$$

hence $a - b \in \psi^{-1}(P)$.

If $a \in \psi^{-1}(P)$ and $r \in A$, then $\psi(ra) = \psi(r)\psi(a) \in P$, since P is an ideal.
Thus $ra \in \psi^{-1}(P)$.

\implies so ψ^{-1} is an ideal of A .

ii. show that $\psi^{-1}(P)$ is prime:

$\psi^{-1}(P) \neq A$, since if $\psi^{-1}(P) = A$, then $1_A \in \psi^{-1}(P)$, so $\psi(1_A) = 1_B \in P$, which would mean that $P = B$, a contradiction since P is prime ideal of B .

Take $a, b \in A$ with $ab \in \psi^{-1}(P)$; then $\psi(ab) \in P$, and since ψ is a ring homomorphism, $\psi(ab) = \psi(a)\psi(b)$.

Since P prime ideal, then $\psi(a)\psi(b) \in P$ implies either $\psi(a) \in P$ or $\psi(b) \in P$.
Thus $a \in \psi^{-1}(P)$ or $b \in \psi^{-1}(P)$.

Hence $\psi^{-1}(P)$ ($= A \cap P$) is a prime ideal of A .

□

Exercise R.1.6. prove or give a counter example:

- the intersection of two prime ideals is prime
- the ideal $P_1 + P_2$ generated by 2 prime ideals P_1, P_2 is prime
- if $\psi : A \longrightarrow B$ ring homomorphism, then ψ^{-1} takes maximal ideals of B to maximal ideals of A

Proof. a. let $I = 2\mathbb{Z} = (2)$, $J = 3\mathbb{Z} = (3)$ be ideals of \mathbb{Z} , both prime.

Then $I \cap J = (2) \cap (3) = (6)$.

The ideal (6) is not prime in \mathbb{Z} , since $2 \cdot 3 \in (6)$, but $2 \notin (6)$ and $3 \notin (6)$.

Thus the intersection of two primes can not be prime.

- b. $P_1 = (2)$, $P_2 = (3)$, both prime.

Then,

$$P_1 + P_2 = (2) + (3) = \{a + b \mid a \in P_1, b \in P_2\}$$

—→ in a principal ideal domain (like \mathbb{Z}), the sum of two principal ideals is again principal, and given by $(m) + (n) = (\gcd(m, n))$.

(recall: principal = generated by a single element)

So, $P_1 + P_2 = (2) + (3) = (\gcd(2, 3)) = (1) = \mathbb{Z}$.

The whole ring is not a prime ideal (by the definition of the prime ideal), so $P_1 + P_2$ is not a prime ideal.

Henceforth, the sum of two prime ideals is not necessarily prime.

- c. let $A = \mathbb{Z}$, $B = \mathbb{Q}$, $\psi : A \rightarrow B$.

Since \mathbb{Q} is a field, its only maximal ideal is (0) .

Then

$$\begin{aligned} \psi^{-1}((0)) &= (0) \subset \mathbb{Z} \\ \text{ie. } \psi^{-1}(m_B) &= (m_B) \subset A \end{aligned}$$

But (0) is not maximal in \mathbb{Z} , because $\mathbb{Z}/(0) \cong \mathbb{Z}$ is not a field.

Thus the preimages of maximal ideals under arbitrary ring homomorphisms need not be maximal.

□

3.2 Exercises Chapter 2

References

- [1] M. F. Atiyah and I. G. MacDonald. Introduction to Commutative Algebra, 1969.
- [2] Miles Reid. Undergraduate Commutative Algebra, 1995.
- [3] Steven Kleiman. Commutative Algebra - MIT OpenCourseWare, 2008. <https://ocw.mit.edu/courses/18-705-commutative-algebra-fall-2008/>.