Commutative Algebra 1

Labix

February 16, 2024

Abstract

Contents

1 Basic Notions of Rings

1.1 Radical Ideals

Definition 1.1.1: Radical of an Ideal

Let I be an ideal of a ring R. Define the radical of I to be

$$\sqrt{I} = \{r \in R | r^n \in I \text{ for some } n \in \mathbb{N}\}$$

We say that an ideal is radical if $\sqrt{I} = I$.

1.2 Nilradical and Jacobson Ideals

Recall that we say an element $r \in R$ is nilpotent if there is some $n \in \mathbb{N}$ such that $r^n = 0$.

Definition 1.2.1: Nilradicals

Let R be a ring. Define the nilradical of R to be

$$N(R) = \{r \in R | r \text{ is nilpotent } \}$$

Proposition 1.2.2

Let R be a ring and $N(R)$ its nilradical. Then the following are true.

- $N(R)$ is an ideal of R
- $N(R/N(R)) = 0$

Proof.

- Suppose that r, s are nilpotent, meaning that $r^n = 0$ and $s^m = 0$. Then $(r + s)^{n+m} = 0$. Moreover, if $t \in R$ then $t \cdot r$ is also nilpotent
- Let $r \notin N(R)$. Every element $r + N(R) \in R/N(R)$ has the property that $r^n \neq 0$. Consider $(r + N(R))^n = r^n + N(R)$. If $r^n \in N(R)$ then $r^n = u$ for some nilpotent u, which means that r^n is nilpotent and thus r is nilpotent, a contradiction. This means that $r + N(R) \notin N(R/N(R))$ for all $r \notin N(R)$ and thus $N(R/N(R)) = 0$

□

Proposition 1.2.3

Let R be a commutative ring. The nilradical of R is the intersection of all prime ideals of R.

Proof. We want to show that

$$N(R) = \bigcap_{\substack{P \text{ a prime} \\ \text{ideal of } R}} P$$

Trivially $N(R)$ is a prime ideal. Now suppose that $r \in R$ is in the intersection of all prime ideals. Then r^n also lies in every prime ideal. □

Definition 1.2.4: Jacobson Radical of a Ring

Let R be a ring. Define the Jacobson radical of R to be

$$J(R) = \bigcap_{\substack{M \text{ is a} \\ \text{maximal ideal} \\ \text{of } R}} M$$

2 Basic Notions of Modules

2.1 Nakayama's Lemma

Lemma 2.1.1: Nakayama's Lemma

Let R be a ring and I an ideal of R. Let M be a finitely generated R-module. If $IM = M$ then there exists $r \in R$ with $r \equiv 1 \pmod I$ such that $rM = 0$.

Lemma 2.1.2

Let R be a local ring with maximal ideal m. Let M be a finitely generated R-module. If $M = mM$, then $M = 0$.

Lemma 2.1.3

Let R be a local ring with maximal ideal m. Let M be a finitely generated R-module. Let $a_1, \dots, a_n \in M$ such that $a_1 + mM, \dots, a_n + mM$ spans M/mM as a vector space over R/m. Then $a_1, \dots, a_n$ generate M.

2.2 Exact Sequences

2.3 Change of Rings

3 Localization

3.1 Localization of a Ring

Definition 3.1.1: Multiplicative Set

Let R be a commutative ring. $S \subseteq R$ is a multiplicative set if $1 \in S$ and S is closed under multiplication: $x, y \in S$ implies $xy \in S$

Definition 3.1.2: Localization of a Ring

Let R be a commutative ring and $S \subseteq R$ be a multiplicative set. Define the ring of fractions of R with respect to S by

$$S^{-1}R = \left\{\frac{r}{s} | r \in R, s \in S\right\} / \sim$$

where $\sim$ is defined by

$$\frac{r}{s} \sim \frac{r'}{s'} \text{ if and only if } \exists v \in S \text{ such that } v(ru' - r'u) = 0$$

If $S = \{1, f, f^2, \dots\}$ then we write $S^{-1}R = R_f = R[1/f]$.

Proposition 3.1.3

Let $S^{-1}R$ be a ring of fractions.

- $\sim$ as defined in the ring of fractions is an equivalence relation
- $(S^{-1}R, +, \times)$ is a ring
- The map $\phi : R \to S^{-1}R$ defined by $\phi(r) \to \frac{r}{1}$ is a ring homomorphism

Proof.

- Trivial
- Define addition by $\frac{r}{s} + \frac{r'}{s'} = \frac{rs'+r's}{ss'}$ and multiplication by $\frac{r}{s} \cdot \frac{r'}{s'} = \frac{rr'}{ss'}$. Clearly addition is abelian, and has identity $\frac{0}{1}$ and inverse $\frac{-r}{s}$ for any $\frac{r}{s} \in S^{-1}R$. Multiplication also has identity $\frac{1}{1}$.
- We have that $\phi(r+s) = \frac{r+s}{1} = \frac{r}{1} + \frac{s}{1} = \phi(r) + \phi(s)$ and $\phi(rs) = \frac{rs}{1} = \frac{r}{1} \cdot \frac{s}{1} = \phi(r) \cdot \phi(s)$ for any $r, s \in R$.

□

Theorem 3.1.4: Universal Property

Let $g : A \to B$ be a ring homomorphism such that $g(s)$ is a unit in B for all $s \in S$. Then there exists a unique ring homomorphism $h : S^{-1}A \to B$ such that $g = h \circ \phi$. In other words, the following diagram commutes:

$$\begin{tikzcd} A \arrow[r, "\phi"] \arrow[dr, "g"'] & S^{-1}A \arrow[d, dashed, "\exists! h"] \\ & B \end{tikzcd}$$

3.2 Localization at a Prime Ideal

Lemma 3.2.1

Let R be a ring and P a prime ideal of R. Then $R \setminus P$ is a multiplicative set.

Proof. By definition, $xy \in P$ implies $x \in P$ or $y \in P$, since $R \setminus P$ removes all these elements, we have that $x \notin P$ and $y \notin P$ implies that $xy \notin P$. □

Definition 3.2.2: Localization on Prime Ideals

Let R be a commutative ring. Let P be a prime ideal. Denote

$$R_p = (R \setminus P)^{-1}R$$

the localization of R at P.

Lemma 3.2.3

Let R be an integral domain. Then the localization

$$(R \setminus (0))^{-1}R$$

is exactly the field of fractions of R.

3.3 Properties of Localization

Proposition 3.3.1

Localization commutes with direct sum of modules and quotient modules.

3.4 Local Rings

Definition 3.4.1: Local Rings

A ring R is said to be a local ring if it has a unique maximal ideal m. In this case, we say that R/m is the residue field of R.

Proposition 3.4.2

Let R be a ring and I an ideal of R. Then I is the unique maximal ideal of R if and only if I is the set containing all non-units of R.

Proof. Let I be the unique maximal ideal of R. Clearly I does not contain any unit else $I = R$. Now suppose that r is a non-unit. Suppose that $r \notin I$. Define $J = \{sr | s \in R\}$ Clearly J is an ideal. It must be contained in some maximal ideal. Since I is the unique maximal ideal, $J \subseteq I$. But this means that $r \in I$, a contradiction. Thus every non-unit is in I.

Suppose that I contains all non-units of R. Let $r \notin I$. Then there exists $s \notin I$ such that $rs = 1$. Then $(r + I)(s + I) = 1 + I$ in R/I. This means that every element of R/I has a multiplicative inverse which means that R/I is a field and thus I is a maximal ideal. Now let $J \neq I$ be another maximal ideal. Then J contains some unit r. This implies that $J = R$ and thus I is the unique maximal ideal. □

Proposition 3.4.3

Every localization R_p is a local ring.

Proof. Let I be the set of all non-units of R_p. It is sufficient to show that I is an ideal by the above lemma. Clearly if $i \in I$ then $r \cdot i$ is also not invertible. Explicitly, we have

$$I = \left\{ \frac{r}{s} \in R_p \middle| r \in p \right\}$$

Let $\frac{r_1}{s_1}, \frac{r_2}{s_2} \in I$, then $\frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{r_1 s_2 + r_2 s_1}{s_1 s_2}$ is in I since $r_1, r_2 \in P$ and P being an ideal implies $r_1 s_2 + r_2 s_1 \in P$. □

Be wary that in general localizations does not result in a local ring. This happens only when we are localizing with respect to a prime ideal. The importance of prime ideals is not explicit in the above because only using prime ideals P can $R \setminus P$ be a multiplicative set which ultimately allows localization to make sense.

3.5 Localization of a Module

Definition 3.5.1: Localization of a Module

Let R be a commutative ring and $S \subseteq R$ be a multiplicative set Let M be a R-module. Define the ring of fractions of M with respect to S by

$$S^{-1}M = \left\{ \frac{m}{s} | m \in M, s \in S \right\} / \sim$$

where $\sim$ is defined by

$$\frac{m}{s} \sim \frac{m'}{s'} \text{ if and only if } \exists v \in S \text{ such that } v(mu' - m'u) = 0$$

If $S = \{1, f, f^2, \dots\}$ then we write $S^{-1}M = M_f = M[1/f]$.

Proposition 3.5.2

Let S be a multiplicative set of a ring R. Then localization at S preservers exact sequences.

Proposition 3.5.3

Let M be an A-module. Then the $S^{-1}A$ modules $S^{-1}M$ is isomorphic to $S^{-1}A \otimes_A M$. More precisely, there exists a unique isomorphism $f : S^{-1}A \otimes_A M \to S^{-1}M$ such that

$$f((a/s) \otimes m) = am/s$$

3.6 Local Properties

Definition 3.6.1: Local Properties

A property P of a ring A or of an A-module M is said to be a local property if the following is true. A (M) has the property P if and only if A_p (M_p) has the property P for every prime ideal p.

4 Noetherian Rings

4.1 Ordering on the Monomials

Recall that a monomial in $R[x_1, \dots, x_n]$ is an element in the polynomial ring of the form $x_1^{a_1} \cdots x_n^{a_n}$. For simplicity we write this as $x^{(a_1,\dots,a_n)}$.

Definition 4.1.1: Monomial Ordering

A monomial ordering on a polynomial ring $k[x_1, \dots, x_n]$ is a relation $>$ on $\mathbb{N}^n$. This means that the following are true.

- $>$ is a total ordering on $\mathbb{N}^n$
- If $a > b$ and $c \in \mathbb{N}^n$ then $a + c > b + c$
- $>$ is a well ordering on $\mathbb{N}^n$ (any nonempty subset of $\mathbb{N}^n$ has a smallest element)

Definition 4.1.2: Lexicographical Order

Let $a = (a_1, \dots, a_n)$ and $b = (b_1, \dots, b_n)$ in $\mathbb{N}^n$. We say that $a >_{\text{lex}} b$ if in the first nonzero entry of $a - b$ is positive.

In practise this means that the we value more powers of x_1

Definition 4.1.3: Graded Lex Order

Let $a = (a_1, \dots, a_n)$ and $b = (b_1, \dots, b_n)$ in $\mathbb{N}^n$. We say that $a >_{\text{grlex}} b$ if either of the following holds.

- $|a| = \sum_{k=1}^n a_k > \sum_{k=1}^n b_k = |b|$
- $|a| = |b|$ and $a >_{\text{lex}} b$

Definition 4.1.4: Graded Lex Order

Let $a = (a_1, \dots, a_n)$ and $b = (b_1, \dots, b_n)$ in $\mathbb{N}^n$. We say that $a >_{\text{grlex}} b$ if either of the following holds.

- $|a| = \sum_{k=1}^n a_k > \sum_{k=1}^n b_k = |b|$
- $|a| = |b|$ and the last nonzero entry of $a - b$ is negative.

In practise we value lower powers of the last variable x_n.

Proposition 4.1.5

The above three orders are all monomial orderings of $k[x_1, \dots, x_n]$.

Definition 4.1.6: Multidegree

Let $f \in k[x_1, \dots, x_n]$ be a polynomial in the form $f = \sum_{v \in \mathbb{N}^n} c_v x^v$. Define the multidegree of f to be

$$\text{multideg}(f) = \max_{>}\{v \in \mathbb{N}^n | a_v \neq 0\}$$

where $>$ is a monomial ordering on $k[x_1, \dots, x_n]$.

Definition 4.1.7: Leading Objects

Let $f \in k[x_1, \dots, x_n]$ be a polynomial in the form $f = \sum_{v \in \mathbb{N}^n} c_v x^v$.

- Define the leading coefficient of f to be $\text{LC}(f) = c_{\text{multideg(f)}} \in k$
- Define the leading monomial of f to be $\text{LM}(f) = c_{\text{multideg(f)}} \in k$
- Define the leading term of f to be $\text{LT} = \text{LC}(f) \cdot \text{LM}(f)$

Proposition 4.1.8: Division Algorithm in $k[x_1, \dots, x_n]$

4.2 Monomial Ideals

Definition 4.2.1: Monomial Ideals

An ideal $I \subset k[x_1, \dots, x_n]$ is said to be a monomial ideal if I is generated by a set of monomials $\{x^v | v \in A\}$ for some $A \subset \mathbb{N}^n$. In this case we write

$$I = \langle x^v | v \in A \rangle$$

Lemma 4.2.2

Let $I = \langle x^v | v \in A \rangle$ be an ideal of $k[x_1, \dots, x_n]$. Then a monomial x^w lies in I if and only if $x^v | x^w$ for some $v \in A$. Moreover, if $f = \sum_{w \in \mathbb{N}^n} c_w x^w \in k[x_1, \dots, x_n]$ lies in I, then each x^w is divisible by x^v for some $v \in A$.

Theorem 4.2.3: Dickson's Lemma

Every monomial ideal is finitely generated. In particular, every monomial ideal $I = \langle x^v | v \in A \rangle$ is of the form

$$I = \langle x^{v_1}, \dots, x^{v_n} \rangle$$

where $v_1, \dots, v_n \in A$.

4.3 Groebner Bases

4.4 Noetherian Rings

Definition 4.4.1: Noetherian Ring

A commutative ring is said to be Noetherian if it satisfies the ascending chain condition on ideals. Meaning if every chain oif ideals $I_0 \subseteq I_1 \subseteq I_2 \subseteq \dots$ is eventually constant for some $n \in \mathbb{N}$, with $I_n = I_{n+1} = I_{n+2} = \dots$.

Proposition 4.4.2

The following are equivalent for a ring R.

- R is a Noetherian ring
- Every ideal in R is finitely generated
- Every nonempty set of ideal has a maximal element.

Proposition 4.4.3

If A is a Noetherian and ϕ is a homomorphism of A onto a ring B, then B is Noetherian.

Theorem 4.4.4: Hilbert's Basis Theorem

If R is a Noetherian ring, then $R[x_1, \dots, x_n]$ is a Noetherian ring.

Proposition 4.4.5

Let R be a Noetherian ring and I be an ideal in R. Then R/I is Noetherian.

5 Primary Decomposition

5.1 Support of a Module

Definition 5.1.1: Support of a Module

Let M be an A-module. The support of M is the subset

$$\text{Supp}(M) = \{P \text{ a prime ideal of } A | M_P \neq 0\}$$

Definition 5.1.2: Annihilator

Let M be an A-module. Let $m \in M$. Define the annihilator of m to be

$$\text{Ann}(m) = \{f \in A | fm = 0\}$$

Also define the annihilator of M to be

$$\text{Ann}(M) = \{f \in A | fM = 0\}$$

5.2 Associated Prime

Definition 5.2.1: Associated Prime

Let M be an A-module. An associated prime P of M is a prime ideal of A such that there exists some $m \in M$ such that $P = \text{Ann}(m)$.

5.3 Primary Ideals

Definition 5.3.1: Primary Ideals

Let R be a ring. An ideal Q of R is called primary if

- $Q \neq R$
- $fg \in Q$ implies $f \in Q$ or $g^m \in Q$ for some $m > 0$

Lemma 5.3.2

If Q is primary, then $\sqrt{Q}$ is prime.

Lemma 5.3.3

Let R be a Noetherian ring and I be a proper ideal that is not primary. Then

$$I = J_1 \cap J_2$$

for some ideals $J_1, J_2 \neq I$.

Definition 5.3.4: P-Primary Ideals

Let A be a ring and P a prime ideal. An ideal Q is P-primary if Q is primary and $Q = \text{rad}(P)$

Theorem 5.3.5

Let A be a Noetherian ring and Q an ideal of A. Then Q is P-primary if and only if $\text{Ann}(A/Q) = \{P\}$.

5.4 Primary Decomposition

We want to express ideal I in R as $I = P_1^{e_1} \cdots P_n^{e_n}$ similar to a factorization of natural numbers, for some prime ideals $P_1, \dots, P_n$. However this notion fails and thus we have the following new type of ideal.

Definition 5.4.1: Primary Decompositions

A primary decomposition of an ideal I is an expression $I = Q_1 \cap \cdots \cap Q_r$ with each Q_i primary.

The decomposition is said to be irredundant if $I \neq \cap_{i \neq j} Q_i$ for any j. The decomposition is said to be minimal if r is the smallest possible such decomposition for I.

Irredundant in this sense means that removing any one primary ideal in the intersection fails to become a decomposition of I.

Theorem 5.4.2

Every proper ideal in a Noetherian ring has a primary decomposition.

Lemma 5.4.3

Let $\phi : R \to S$ be a ring homomorphism and Q be a primary ideal in S. Then $\phi^{-1}(Q)$ is primary in R.

6 Integral Dependence

6.1 Integral Extensions

Definition 6.1.1: Integral Elements

Let B be a ring and let $A \subseteq B$ be a subring. Let $b \in B$. We say that b is integral over A if there exists a monic polynomial $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in A[x]$ such that $p(b) = 0$.

Proposition 6.1.2

Let B be a ring and let $A \subseteq B$. Let $b \in B$. Then the following are equivalent.

- b is integral over A
- The subring $A[b] \subseteq B$ is finite over A
- There exists an A sub-algebra $A' \subseteq B$ such that $A[b] \subseteq A'$ and A' is finite over A.

Definition 6.1.3: Integral Closure

Let B be an A-algebra. Define the subring

$$\tilde{A} = \{b \in B | b \text{ is integral over } A\}$$

to be the integral closure of A in B. If $\tilde{A} = A$, then we say that A is integrally closed in B.

Definition 6.1.4: Normal Domains

Let R be a domain. We say that R is normal (intergrally closed) if A is integrally closed in its field of fractions.

The integral closure of R in $\text{Frac}(R)$ is called the normalization of R.

6.2 The Going-Up and Going-Down Theorems

7 Discrete Valuation Rings

7.1 Discrete Valuation Rings

Definition 7.1.1: Totally Ordered Group

A totally ordered group is a group G with a total order "$\leq$" such that it is

- a left ordered group: $a \leq b$ implies $ca \leq cb$ for all $a, b, c \in G$
- a right ordered group: $a \leq b$ implies $ac \leq bc$ for all $a, b, c \in G$

Definition 7.1.2: Valuation on a Field

Let K be a field. Let G be a totally ordered abelian group. A valuation on K with values in G is a map $v : K \setminus \{0\} \to G$ such that for all $x, y \in K^*$, we have

- $v(xy) = v(x) + v(y)$
- $v(x + y) \geq \min\{v(x), v(y)\}$

We use the convention that $v(0) = \infty$.

v is said to be a discrete valuation if $G = \mathbb{Z}$.

Proposition 7.1.3

Let K be a field and $v : K \to \mathbb{Z}$ a discrete valuation. Then

$$\{x \in K | v(x) \geq 0\}$$

is a subring of K.

Definition 7.1.4: Discrete Valuation Rings

The discrete valuation ring of a discrete valuation $v : K \to \mathbb{Z}$ is the subset

$$A = \{x \in K | v(x) \geq 0\}$$

Alternatively, any ring isomorphic to a discrete valuation ring of some discrete valuation is also called a discrete valuation.

Proposition 7.1.5

Let R be a discrete valuation ring with respect to the valuation v. Let $t \in R$ be such that $v(t) = 1$. Then the following are true.

- A nonzero element $u \in R$ is a unit if and only if $v(u) = 0$
- Every non-zero ideal of R is a principal ideal of the form (t^n) for some $n \geq 0$
- Every $r \in R \setminus \{0\}$ can be written in the form $r = ut^n$ for some unit u and $n \geq 0$.

Proof.

- Let R be a discrete valuation ring. Suppose that $x \in R$ is a unit. Then $v(x^{-1}) = -v(x)$. Then $-v(x), v(x) \geq 0$ implies $v(x) = 0$. Now if $v(y) > 0$, suppose for contradiction that $u \in R$ is an inverse of y, then

$$0 = v(1) = v(uy) = v(u) + v(y)$$

But $v(y) > 0$ implies that $v(u) < 0$ which implies that $u \notin R$, a contradiction.

- Let $t \in R$ such that $v(t) = 1$. Let $x \in m$ where $v(x) = n > 0$. Then $v(x) = nv(t) = v(t^n)$ means that every $x \in m$ is of the form t^n. Thus $m = (t)$. Since every ideal I is a subset of this maximal ideal, any ideal is of the form $I = (t^n)$ for some $n > 0$.
- Follows from the fact that (t^n) is the unique maximal ideal.

□

Proposition 7.1.6

Let R be an integral domain. Then the following are equivalent.

- R is a discrete valuation ring
- R is a UFD with a unique irreducible element up to multiplication of a unit
- R is a Noetherian local ring with a principal maximal ideal

Proof.

- (1) $\implies$ (3): We have seen that the set of non-units is precisely the set $m = \{x \in K | v(x) > 0\}$. We show that this is an ideal. Clearly $x, y \in m$ implies $v(x + y) = \min\{v(x), v(y)\} > 0$. Let $u \in R$. Then $v(ux) = v(u) + v(x) > 0$ since $v(x) > 0$ and $v(u) \geq 0$.

  We have seen that every ideal is of the form (t^n) for some $n > 0$. Thus every ascending chains of ideal must be of the form

  $$(t^{n_1}) \subset (t^{n_2}) \subset \dots$$

  for $n_1 > n_2 > \dots$. Since $n_1, n_2, \dots$ is strictly decreasing, the chain must eventually stabilizes. This proves that R is Noetherian and has principal maximal ideal.
- (1) $\implies$ (3):

□