Commutative Algebra 1

Labix

December 5, 2023

Abstract

Contents

1 Noetherian Rings

1.1 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 1.1.1: 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 1.1.2: 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 1.1.3: 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 1.1.4: 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 1.1.5

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

Definition 1.1.6: 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 1.1.7: 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 1.1.8: Division Algorithm in $k[x_1, \dots, x_n]$

1.2 Monomial Ideals

Definition 1.2.1: 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 1.2.2

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 1.2.3: 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 $v_1, \dots, v_n \in A$.

1.3 Groebner Bases

1.4 Noetherian Rings

Definition 1.4.1: 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 1.4.2

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.

Theorem 1.4.3: Hilbert's Basis Theorem

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

Proposition 1.4.4

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

2 Commutative Rings

2.1 Localizations and Local Rings

Definition 2.1.1: 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 2.1.2: Ring of Fractions

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 2.1.3

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

Definition 2.1.4: Localization

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.

This means that locally at P, there is a ring of fractions there.

Lemma 2.1.5

Let R be a ring and I an ideal of R. Then I is the unique maximal ideal of R if and only if every element $r \notin I$ is a unit.

Lemma 2.1.6

Let R be an integral domain. Then the localization

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

is exactly the field of fractions of R.

Definition 2.1.7: 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 2.1.8

Every localization R_p is a local ring.

Proposition 2.1.9

If R is a noetherian ring with maximal ideal m and residue field k, then

$$\dim_k(m/m^2) \geq \dim(A/m)$$

Definition 2.1.10: Regular Local Rings

A local ring R is said to be regular if $\dim_k(m/m^2) = \dim(R)$ for k the residue field of R.

Theorem 2.1.11

Let A be a Noetherian local ring of dimension 1 with maximal ideal m. Then the following are equivalent:

- A is regular
- m is principal
- A is an integral domain, and all ideals are of the form m^n for $n \geq 0$ or (0)
- A is a principal ideal domain

2.2 Normalization

2.3 Graded Rings

Definition 2.3.1: Graded Rings

A graded ring R is a ring such that the underlying additive group is a direct sum of abelian groups R_i, meaning that

$$R = \bigoplus_{n\in\mathbb{N}} R_i$$

and such that for $r_i \in R_i$ and $r_j \in R_j$, $r_i r_j \in R_{i+j}$. A $\mathbb{Z}$ graded ring is a ring graded in $\mathbb{Z}$ instead of $\mathbb{N}$.

Proposition 2.3.2

The following are true for a graded ring $R = \bigoplus_{n\in\mathbb{N}} R_i$.

- R_0 is a subring of R
- R_n is an R_0 module for each n
- R is an associative R_0 algebra

Definition 2.3.3: Homogenous Ideals

An ideal I of a graded ring R is said to be homogenous if for each $a \in I$, the homogenous components of a is in I.

Proposition 2.3.4

If I is an homogenous ideal of a graded ring R, then R/I is also a graded ring.

2.4 Valuation Rings

Definition 2.4.1: 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 2.4.2: 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

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

Also define the set $R = \{x \in K | v(x) \geq 0\} \cup \{0\}$ the valuation ring of v.

Proposition 2.4.3

Valuation rings are indeed a ring, a subring of K.

Definition 2.4.4: Discrete Valuations

A valuation $v : K^* \to G$ is said to be discrete if $G = \mathbb{Z}$.

Definition 2.4.5: Valuation Rings

A intgeral domain A is said to be a valuation ring if there exists a valuation v on its fraction field $K(A)$, such that the valuation ring of v on $K(A)$ is precisely A. It is a discrete valuation ring if the valuation is discrete.

Theorem 2.4.6

Let A be an integral domain that is a Noetherian local ring of dimension 1. Then A is regular if and only if A is a discrete valuation ring.

2.5 Radical Ideals

Definition 2.5.1: 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 $\sqrt{I} = I$.

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 2.5.2: Nilradicals

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

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

Proposition 2.5.3

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

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

Proposition 2.5.4

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

Definition 2.5.5: Jacobson Radical of a Ring

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

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

2.6 Primary Ideals and 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 2.6.1: 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 2.6.2

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

Lemma 2.6.3

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 2.6.4: 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 2.6.5

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

Lemma 2.6.6

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.