Commutative Algebra 1

Labix

October 12, 2024

Abstract

Contents

1 Basic Notions of Commutative Rings

1.1 Local Rings

Definition 1.1.1: 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.

We will discuss more of local rings in the topic of localizations. For now, here is one example. Let k be a field. It is easy to see that (x) is the unique maximal ideal of $R = k[[x]]$. The residue field in this case is simply k.

Proposition 1.1.2

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. □

1.2 Radical Ideals

The radical of an ideal is a very different notion from the radical of module.

Definition 1.2.1: Radical of an Ideal

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

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

Proposition 1.2.2

Let R be a commutative ring. Let I be an ideal. Then the following are true.

- $I \subseteq \sqrt{I}$
- $\sqrt{\sqrt{I}} = \sqrt{I}$

Proof.

- Let $r \in I$. Then $r^1 \in I$ Thus by choosing $n = 1$ we shows that $r^n \in I$. Thus $r \in \sqrt{I}$.
- By the above, we already know that $\sqrt{I} \subseteq \sqrt{\sqrt{I}}$. So let $r \in \sqrt{\sqrt{I}}$. Then there exists some $n \in \mathbb{N}$ such that $r^n \in \sqrt{I}$. But $r^n \in \sqrt{I}$ means that there exists some $m \in \mathbb{N}$ such that $(r^n)^m \in I$. But $nm \in \mathbb{N}$ is a natural number such that $r^{nm} \in I$. Hence $r \in \sqrt{I}$ and so we conclude.

□

Proposition 1.2.3

Let R be a commutative ring. Let I, J be ideals of R. Then the following are true.
- $\sqrt{IJ} = \sqrt{I \cap J}$.

Proof.
- Let $x \in \sqrt{IJ}$. Then $x^n \in IJ$. This means that there exists $i \in I$ and $j \in J$ such that $x^n = ij$. Since I and J are two sided ideals, we can conclude that $x^n = ij \in I, J$. Hence $x^n = ij \in I \cap J$. We conclude that $x \in \sqrt{I \cap J}$. Now let $x \in \sqrt{I \cap J}$. Then there exists $n \in \mathbb{N}$ such that $x^n \in I \cap J$. Then $x^n \in I$ and $x^n \in J$ implies that $x^{2n} = x^n \cdot x^n \in IJ$. We conclude that $x \in \sqrt{IJ}$.

$\square$

Proposition 1.2.4

Let R be a commutative ring. Let I be an ideal. Then

$$\sqrt{I} = \bigcap_{\substack{p \text{ a prime ideal} \\ I \subseteq p \subseteq R}} p$$

Definition 1.2.5: Radical Ideals

Let R be a commutative ring. Let I be an ideal of R. We say that I is radical if

$$\sqrt{I} = I$$

In particular, by the above lemma it follows that the radical of an ideal is a radical ideal.

Theorem 1.2.6

Let R be a commutative ring. Let I be an ideal of R. Denote φ to be the inclusion preserving one-to-one bijection

$$\left\{ \substack{\text{Ideals of } R \\ \text{containing } I} \right\} \overset{1:1}{\longleftrightarrow} \{\text{Ideals of } R/I\}$$

from the correspondence theorem for rings. In other words, $\varphi(A) = A/I$. Let $J \subseteq R$ be an ideal containing I. Then the following are true.
- J is a radical ideal if and only if $\varphi(J) = J/I$ is a radical ideal.
- J is a prime ideal if and only if $\varphi(J) = J/I$ is a prime ideal.
- J is a maximal ideal if and only if $\varphi(J) = J/I$ is a maximal ideal.

Proof.
- Let J be a radical ideal. Suppose that $r + I \in \sqrt{J/I}$. This means that $(r + I)^n = r^n + I \in J/I$ for some $n \in \mathbb{N}$. But this means that $r^n \in J$. This implies that $r \in \sqrt{J} = J$. Thus $r + I \in J/I$ and we conclude that $\sqrt{J/I} \subseteq J/I$. Since we also have $J/I \subseteq \sqrt{J/I}$, we conclude.

  Now suppose that J/I is a radical ideal. Let $r \in \sqrt{J}$. This means that $r^n \in J$ for some $n \in \mathbb{N}$. Now $r^n + I = (r + I)^n \in J/I$ implies that $r + I \in \sqrt{J/I} = J/I$. Hence $r \in J$ and so $\sqrt{J} \subseteq J$. Since we also have that $J \subseteq \sqrt{J}$, we conclude.
- Let J be a prime ideal. Then R/J is an integral domain. By the second isomorphism theorem, we have that $R/J \cong (R/I)/(J/I)$ and hence $(R/I)/(J/I)$ is also an integral domain. Hence J/I is a prime ideal. The converse is also true.
- Let J be a maximal ideal. Then R/J is a field. By the second isomorphism theorem, we have that $R/J \cong (R/I)/(J/I)$ and hence $(R/I)/(J/I)$ is also a field. Hence J/I is a maximal ideal. The converse is also true.

□

1.3 Nilradical and Jacobson Ideals

Let R be a ring. Recall that an element $r \in R$ is nilpotent if $r^n = 0_R$ for some $n \in \mathbb{N}$. When R is commutative, we can form an ideal out of nilpotent elements.

Definition 1.3.1: Nilradicals

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

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

Note that this is different from nilpotent ideals, as nilpotency is a property of an ideal. However the Nilradical ideal is a nil ideal and every sub-ideal of the nilradical is a nil ideal.

Proposition 1.3.2

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 1.3.3

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. □

Example 1.3.4

Consider the ring

$$R = \frac{\mathbb{C}[x,y]}{(x^2 - y, xy)}$$

Then its nilradical is given by $N(R) = (x, y)$.

Proof. Notice that in the ring R, $x^3 = x(x^2) = xy = 0$ and $y^3 = x^6 = (x^3)^2 = 0$ and hence x and y are both nilpotent elements of R. By definition of the nilradical, we conclude that $(x, y) \subseteq N(R)$. Now (x, y) is a maximal ideal of $\mathbb{C}[x, y]$ because $\mathbb{C}[x, y]/(x, y) \cong \mathbb{C}$. Also notice that $(x, y) \supseteq (x^2 - y, xy)$ because for any element $f(x)(x^2 - y) + g(x)(xy) \in (x^2 - y, xy)$, we have that

$$\begin{aligned} f(x)(x^2-y)+g(x)(xy) \in (x^2-y,xy) &= (xf(x))x - f(x)y + (g(x)x)y \\ &= (xf(x))x + (xg(x)-f(x))y \in (x,y) \end{aligned}$$

By the correspondence theorem, $(x,y)/(x^2-y)$ is an maximal ideal of R. In particular, (x,y) is also a prime ideal. But the $N(R)$ is the intersection of all prime ideals and hence $N(R) \subseteq (x,y)$. We conclude that $N(R) = (x,y)$. □

Recall the notion of the Jacobson radical from Rings and Modules.

Proposition 1.3.5

Let R be a commutative ring. Then

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

Proposition 1.3.6

Let R be a commutative ring. Then $x \in J(R)$ if and only if $1 - xy \neq 0$ for all $y \in R$.

Proof. □

1.4 Extensions and Contractions of Ideals

Definition 1.4.1: Extension of Ideals

Let R, S be commutative rings. Let $f : R \to S$ be a ring homomorphism. Let I be an ideal of R. Define the extension I^e of I to S to be the ideal

$$I^e \langle f(i) \mid i \in I \rangle$$

Proposition 1.4.2

Let R, S be commutative rings. Let $f : R \to S$ be a ring homomorphism. Let I, I_1, I_2 be an ideal of R. Then the following are true regarding the extension of ideals.
- Closed under sum: $(I_1 + I_2)^e = I_1^e + I_2^e$
- $(I_1 \cap I_2)^e \subseteq I_1^e \cap I_2^e$
- Closed under products: $(I_1 I_2)^e = I_1^e I_2^e$
- $(I_1/I_2)^e \subseteq I_1^e / I_2^e$
- $\text{rad}(I)^e \subseteq \text{rad}(I^e)$

Definition 1.4.3: Contraction of Ideals

Let R, S be commutative rings. Let $f : R \to S$ be a ring homomorphism. Let J be an ideal of S. Define the contraction J^c of J to R to be the ideal

$$J^c = f^{-1}(J)$$

Proposition 1.4.4

Let R, S be commutative rings. Let $f : R \to S$ be a ring homomorphism. Let J, J_1, J_2 be an ideal of S. Then the following are true regarding the extension of ideals.

- $(J_1 + J_2)^e \supseteq J_1^e + J_2^e$
- Closed under intersections: $(J_1 \cap J_2)^e = J_1^e \cap J_2^e$
- $(J_1 J_2)^e \supseteq J_1^e J_2^e$
- $(J_1 / J_2)^e \subseteq J_1^e / J_2^e$
- Closed under taking radicals: $\text{rad}(J)^e = \text{rad}(J^e)$

Proposition 1.4.5

Let R, S be commutative rings. Let $f : R \to S$ be a ring homomorphism. Let I be an ideal of R and let J be an ideal of S. Then the following are true.

- $I \subseteq I^{ec}$
- $J^{ce} \subseteq J$
- $I^e = I^{ece}$
- $J^c = J^{cec}$

2 Modules over a Commutative Ring

2.1 Cayley-Hamilton Theorem

Definition 2.1.1: Characteristic Polynomial

Let R be a commutative ring. Let $A \in M_{n\times n}(R)$ be a matrix. Define the characteristic polynomial of A to be the polynomial

$$c_A(x) = \det(A - xI)$$

Theorem 2.1.2: Cayley-Hamilton Theorem

Let R be a commutative ring. Let $A \in M_{n\times n}(R)$ be a matrix. Then $c_A(A) = 0$.

Corollary 2.1.3

Let R be a commutative ring. Let M be a finitely generated R-module. Let I be an ideal of R. Let $\varphi \in \text{End}_R(M)$. If $\varphi(M) \subseteq IM$, then there exists $a_1, \dots, a_n \in I$ such that

$$\varphi^n + a_1\varphi^{n-1} + \cdots + a_{n-1}\varphi + \text{id}_M = 0 : M \to M$$

2.2 Nakayama's Lemma

Lemma 2.2.1: Nakayama's Lemma I

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

Lemma 2.2.2: Nakayama's Lemma II

Let R be a commutative ring. Let M be a finitely generated R-module. Let I be an ideal of R such that $I \subseteq J(R)$ and $IM = M$. Then $M = 0$.

Corollary 2.2.3

Let (R, m) be a local ring. Let M be a finitely generated R-module. Then the following are true.

- M/mM is a finite dimensional vector space over R/m.
- $a_1, \dots, a_n \in M$ generates M as an R-module if and only if $a_1 + mM, \dots, a_n + mM$ generates M/mM as a R/m vector space.

2.3 Exact Sequences

2.4 Change of Rings

Definition 2.4.1: Extension of Scalars

Let R, S be commutative rings. Let $\varphi : R \to S$ be a ring homomorphism. Let M be an R-module. Define the extension of M to the ring S to be the S-module

$$S \otimes_R M$$

Definition 2.4.2: Restriction of Scalars

Let R, S be commutative rings. Let $\varphi : R \to S$ be a ring homomorphism. Let M be an S-module. Define the restriction of M to the ring R to be the R-module M equipped with the action

$$r \cdot_R m = \varphi(r) \cdot_S m$$

for all $r \in R$.

Theorem 2.4.3

Let R, S be commutative rings. Let $\varphi : R \to S$ be a ring homomorphism. Then there is an isomorphism

$$\mathrm{Hom}_S(S \otimes_R M, N) \cong \mathrm{Hom}_R(M, N)$$

for any R-module M and S-module N given as follows.

- For $f \in \mathrm{Hom}_S(S \otimes_R M, N)$, define the map $f^+ \in \mathrm{Hom}_R(M, N)$ by

$$f^+(m) = f(1 \otimes m)$$

- For $g \in \mathrm{Hom}_R(M, N)$, define the map $g^- \in \mathrm{Hom}_S(S \otimes_R M, N)$ by

$$g^-(s \otimes m) = s \cdot g(m)$$

3 Algebra Over a Commutative Ring

3.1 Commutative Algebras

Definition 3.1.1: Commutative Algebras

Let R be a commutative ring. A commutative R-algebra is an R-algebra A that is commutative.

Proposition 3.1.2

Let R be a commutative ring. Then the following are equivalent characterizations of a commutative R-algebra.
- A is a commutative R-algebra
- A is a commutative ring together with a ring homomorphism $f : R \to A$

Proof. Suppose that A is an R-algebra. Then define a map $f : R \to A$ by $f(r) = r \cdot 1$ where $r \cdot 1$ is the module operation on A. Then clearly this is a ring homomorphism.

Suppose that A is a commutative ring together with a ring homomorphism $f : R \to A$. Define an action $\cdot : R \times A \to A$ by $r \cdot a = f(r)a$. Then this action clearly allows A to be an R-module. □

Under the correspondence of associative algebra, the above proposition gives a another correspondence between the first one.

$$\left\{(A, R) \;\middle|\; \substack{A \text{ is a commutative} \\ R\text{-algebra}}\right\} \overset{1:1}{\longleftrightarrow} \left\{\phi : R \to A \;\middle|\; \substack{\phi \text{ is a ring homomorphism} \\ \text{such that } f(R) \subseteq Z(A) = A}\right\}$$

In particular, the construction above are inverses of each other so that it gives the one-to-one correspondence.

3.2 Finitely Generated Algebra

Definition 3.2.1: Finitely Generated Algebra

Let A be a commutative algebra over a ring R. We say that A is a finitely generated algebra if there exists a finite set of elements $a_1, \dots, a_n$ such that A is generated by $a_1, \dots, a_n$. Explicitly, this means that for all $a \in A$, there exists $c_{i_1,\dots,i_n} \in R$ for $i_1, \dots, i_n \in \mathbb{N}$ such that

$$a = \sum_{i_1,\dots,i_n} c_{i_1,\dots,i_n} a_1^{i_1} \cdots a_n^{i_n}$$

Finitely generated algebras are also called algebra of finite type.

Theorem 3.2.2

Let A be a commutative algebra over a ring R. Then the following are equivalent.
- A is a finitely generated algebra over R
- There exists elements $a_1, \dots, a_n \in A$ such that the evaluation homomorphism
$$\phi : R[x_1, \dots, x_n] \to A$$
given by $\phi(f) = f(a_1, \dots, a_n)$ is a surjection
- There is an isomorphism
$$A \cong \frac{R[x_1, \dots, x_n]}{I}$$
for some ideal I

Definition 3.2.3: Finitely Presented Algebra

Let R be a ring. Let $A = R[x_1, \dots, x_n]/I$ be a finitely generated algebra over R for some ideal I. We say that A is finitely presented if I is finitely generated.

Lemma 3.2.4

Let R be a ring, considered as an algebra over $\mathbb{Z}$. If R is finitely generated over $\mathbb{Z}$, then R is finitely presented.

Proof. Trivial since $\mathbb{Z}$ is a principal ideal domain. $\square$

4 Localization

4.1 Localization of a Ring

Definition 4.1.1: 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 4.1.2: 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 4.1.3

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 $r, s \in R$.

$\square$

Theorem 4.1.4: 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:

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

4.2 Localization at a Prime Ideal

Lemma 4.2.1

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 4.2.2: 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 4.2.3

Let R be an integral domain. Then the localization

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

is exactly the field of fractions of R.

Proposition 4.2.4

Let R be a ring and let p be a prime ideal of R. Then 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.

4.3 Properties of Localization

Proposition 4.3.1

Localization commutes with direct sum of modules and quotient modules.

4.4 Localization of a Module

Definition 4.4.1: 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 4.4.2

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

Proposition 4.4.3

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

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

5 Noetherian Rings

5.1 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 5.1.1: 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 5.1.2: 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 5.1.3: 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 5.1.4: 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 5.1.5

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

Definition 5.1.6: 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 5.1.7: 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 5.1.8: Division Algorithm in $k[x_1, \dots, x_n]$

5.2 Monomial Ideals

Definition 5.2.1: 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 5.2.2

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

5.3 Groebner Bases

5.4 Hilbert's Basis Theorem

Proposition 5.4.1

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

Theorem 5.4.2: Hilbert's Basis Theorem

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

Proposition 5.4.3

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

Theorem 5.4.4

Let $R = \bigoplus_{i=1}^n R_i$ be a graded ring. Then R is Noetherian if and only if R_0 is Noetherian and R is finitely generated as an R_0-module.

6 Primary Decomposition

6.1 Support of a Module

Definition 6.1.1: Support of a Module

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

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

6.2 Associated Prime

Definition 6.2.1: 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 $P = \text{Ann}(m)$.

6.3 Primary Ideals

Definition 6.3.1: 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 6.3.2

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

Lemma 6.3.3

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 6.3.4: 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 6.3.5

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

6.4 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 6.4.1: 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 6.4.2

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

Lemma 6.4.3

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.

7 Integral Dependence

7.1 Integral Extensions

Definition 7.1.1: 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 7.1.2

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.

Proposition 7.1.3

Let B be a ring and let $A \subseteq B$ be a subring. Let $b_1, b_2 \in B$ be integral over A. Then $b_1 + b_2$ and $b_1 b_2$ are both integral over A.

Definition 7.1.4: Integral Extensions

Let B be a ring and let $A \subseteq B$ be a subring. We say that B is integral over A if all elements of B are integral over A.

Lemma 7.1.5

Let $A \subseteq B \subseteq C$ be rings. If C is integral over B and B is integral over A, then C is integral over A.

Definition 7.1.6: Integral Closure

Let B be an A-algebra. Define the subring

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

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

Lemma 7.1.7

Let B be a ring and let $A \subseteq B$ be a subring. Then $\overline{A}$ is an integral extension of A.

Definition 7.1.8: 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.

7.2 The Going-Up and Going-Down Theorems

7.3 Dedekind Domains

Definition 7.3.1: Dedekind Domains

Let R be a ring. We say that R is a dedekind domain if the following are true.

- R is an integral domain
- R is an integrally closed
- R is Noetherian
- Every non-zero prime ideal of R is maximal

8 Discrete Valuation Rings

8.1 Discrete Valuation Rings

Definition 8.1.1: 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 8.1.2: 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 8.1.3

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 8.1.4: 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 8.1.5

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 8.1.6

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.
- $(1) \implies (3)$:

□

9 Dimension Theory for Rings

9.1 Dimension and Height

Definition 9.1.1: Krull Dimension

Let R be a commutative ring. Define the Krull dimension of R to be

$$\dim(R) = \sup\{t \in \mathbb{N} | p_0 \subset \cdots \subset p_t \text{ for } p_0, \dots, p_t \text{ prime ideals } \}$$

Definition 9.1.2: Height of a Prime Ideal

Let p be a prime ideal in a ring R. Define the height of p to be

$$\text{ht}(p) = \sup\{t \in \mathbb{N} | p_0 \subset \cdots \subset p_t = p \text{ for } p_0, \dots, p_t \text{ prime ideals } \}$$

Lemma 9.1.3

Let p be a prime ideal in a ring R. Then

$$\text{ht}(p) = \dim(R_p)$$

Theorem 9.1.4: Krull's Principal Ideal Theorem

Let R be a Noetherian ring. Let I be a proper and principal ideal of R. Let p be the smallest prime ideal containing I. Then

$$\text{ht}_R(p) \leq 1$$

9.2 Length of a Module

Definition 9.2.1: Length of a Module

Let R be a ring and let M be an R-module. Define the length of M to be

$$l_R(M) = \sup\{n \in \mathbb{N} \mid 0 = M_0 \subset M_1 \subset \cdots \subset M_n = M\}$$

Lemma 9.2.2

Let R be a ring. Let $0 \to M' \to M \to M'' \to 0$ be a short exact sequence of R-modules. Then

$$l_R(M) = l_R(M') + l_R(M'')$$

Lemma 9.2.3

Let (A, m) be a local ring and let M be an A-module. If $mM = 0$, then

$$l_A(M) = \dim_{A/m}(M)$$

Proposition 9.2.4

Let R be a ring and let M be an R-module. Then the following are equivalent.

- M is simple
- $l_R(M) = 1$
- $M \cong A/m$ for some maximal ideal m of A

9.3 The Hilbert Polynomial

Definition 9.3.1: The Hilbert Polynomial

Let $R = \bigoplus_{k=0}^{\infty} R_k$ be a Noetherian graded ring. Let $M = \bigoplus_{k=0}^{\infty} M_k$ be a graded R-module. Define the Hilbert function $H_M : \mathbb{N} \to \mathbb{N}$ of R to be the function defined by

$$H_M(n) = l_{R_0}(M_n)$$

Definition 9.3.2: The Hilbert Series

Let $R = \bigoplus_{k=0}^{\infty} R_k$ be a Noetherian graded ring. Let $M = \bigoplus_{k=0}^{\infty} M_k$ be a graded R-module. Define the Hilbert series $HS_M \in \mathbb{Z}[[t]]$ of M to be the formal series

$$HS_M(t) = \sum_{k=0}^{\infty} H_M(k)t^k = \sum_{k=0}^{\infty} l_{R_0}(M_k)t^k$$

Theorem 9.3.3

Let $R = \bigoplus_{k=0}^{\infty} R_k$ be a Noetherian graded ring such that R_0 is Artinian. Let $M = \bigoplus_{k=0}^{\infty} M_k$ be a graded R-module. Let $\lambda : \{M_i \mid i \in I\} \to \mathbb{Z}$ be an additive function Then the function

$$g(t) = \sum_{k=0}^{\infty} \lambda(M_k)t^k$$

is a rational function and can be written in the form

$$g(t) = \frac{f(t)}{\prod_{i=1}^{r}(1 - t^{d_i})}$$

for some $f(t) \in \mathbb{Z}[t]$ and $d_i \in \mathbb{N}$.

Theorem 9.3.4: The Fundamental Theorem of Dimension Theory

Let (R, m) be a local Noetherian ring. Let I be an m-primary ideal. Then the following numbers are equal.

- Let $J = \bigoplus_{k=0}^{\infty} \frac{I^k}{I^{k+1}}$. The order of the pole at 1 of the rational function HS_J.
- The minimum number of elements of R that can generate an m-primary ideal of R
- The dimension $\dim_{R/m}(R)$

The following is a generalization of Krull's principal ideal theorem. Both of the theorems can actually be deduced directly from the fundamental theorem.

Theorem 9.3.5: Krull's Height Theorem

Let R be a Noetherian ring. Let I be a proper ideal generated by n elements. Let p be the smallest prime ideal containing I. Then

$$\text{ht}_R(p) \leq n$$

Theorem 9.3.6

Let (R, m) be a Noetherian local ring and let $k = R/m$ be the residue field. Then

$$\dim(R) \leq \dim_k(m/m^2)$$

9.4 Global Dimension of a Ring