Unique Factorization Domains in Commutative Algebra

Yongjian Huang

Advisor: Prof. Daniel Katz

University of Kansas

May 20, 2021

1 Introduction

In this project, we learn about unique factorization domains in commutative algebra. Most importantly, we explore the relation between unique factorization domains and regular local rings, and prove the main theorem: *If R is a regular local ring, so is a unique factorization domain.*

2 Prime ideals

Before learning the section about unique factorization domains, we first need to know about definition and theorems about prime ideals.

Definition 2.1. In a commutative ring R, the ideal I is *prime* if $ab \in I$ implies $a \in I$ or $b \in I$. Alternatively, I is prime if R/I is an integral domain.

The following theorem tells us another way to define prime ideals.

Theorem 2.1. *Let S be a multiplicatively closed set in a ring R and let I be an ideal in R maximal with respect to the exclusion of S. Then I is prime.*

Proof. Given $ab \in I$, we want to show $a \in I$ or $b \in I$. We give a proof by contradiction, suppose $a \notin I$ and $b \notin I$, then the ideal (I, a) generated by I and a is strictly larger than I. So the ideal (I, a) intersects S. Thus, there exists an element $s \in S$ of the form $s_1 = i_1 + xa$, where $i_1 \in I$ and $x \in R$. Similarly, we have $s_2 = i_2 + yb$, where $i_2 \in I$ and $y \in R$.

$$\begin{aligned} s_1 \cdot s_2 &= (i_1 + xa)(i_2 + yb) \\ &= i_1 i_2 + i_1 yb + i_2 xa + xyab \end{aligned}$$

Thus, $s_1 s_2 \in I$. However, S is multiplicatively closed set, then $s_1 s_2 \in S$, which is a contradiction. Therefore, $a \in I$ or $b \in I$, which implies I is prime. $\square$

Definition 2.2. The set S is *saturated* if $x \in S$ with $s_1 \cdot s_2 = x$ and both $s_1, s_2 \in S$.

Theorem 2.2. *The following are equivalent:*
(1) S is a saturated multiplicatively closed set;
(2) The complement of S is a set theoretic union of prime ideals in R.

Proof. Assume (2) holds. Proof by contradiction. Suppose $s_1 \cdot s_2 \in S$ and s_1 or $s_2 \in \mathcal{I}$, where $\mathcal{I} = \bigcup I_i$ and I_i are prime ideals. Since I_i are the complement of S, $\mathcal{I}$ is the complement of S. Without loss of generality, suppose $s_1 \in \mathcal{I}$, then $s_1 \cdot s_2 \in \mathcal{I}$, which is a contradiction. Assume s_1,$s_2 \in S$ and $s_1 \cdot s_2 \notin S$, then $s_1 \cdot s_2 \in \mathcal{I}$, so s_1 or $s_2 \in \mathcal{I}$, which is a contradiction.

Assume (1) holds. We can take x in the complement of S. Then the principal ideal (x) is disjoint from S, since S is saturated. Then using the Zorn's Lemma, we can expand (x) to an ideal I maximal with respect to the disjointness from S. Then by Theorem 2.1, I is prime. Thus, every x not in S has been inserted in a prime ideal disjoint from S. Therefore, (2) holds. □

Prime elements and irreducible elements are very important concepts we need to learn for unique factorization domains.

Definition 2.3. $p \in R$ is called *prime* if $p \neq 0$, p is not a unit in R, and $p|ab$ implies $p|a$ or $p|b$. An ideal generated by a prime element p, denoted by (p), is called principal prime.

Definition 2.4. $p \in R$ is called *irreducible* if $p \neq 0$, p is not a unit in R, and $p = ab$ implies a is a unit or b is a unit.

Then we can find the relation between principal prime elements and irreducible elements in a integral domain.

Lemma 2.3. *In an integral domain R with unity, a principal prime element p is an irreducible element.*

Proof. Let p be a principal prime element is R, then (p) is a prime ideal in R. Assume p is not an irreducible element. Let $p = ab$, then neither a nor b is a unit in R. Moreover, $ab = p$ implies $ab \in (p)$. Since (p) is a prime ideal, we have either $a \in (p)$ or $b \in (p)$. Without loss of generality, suppose $a \in (p)$, then $a = pm$ for some $m \in R$, so we have $p = (pm) \cdot b$, which implies $mb = 1$, since p is nonzero in an integral domain R. Thus, b is a unit, which contradicts the assumption. Therefore, p is an irreducible element. □

Theorem 2.4. *If an element in an integral domain is expressible as a product $p_1 p_2 ... p_n$ of principal primes, then that expression is unique, up to a permutation of $p's$, and multiplication of them by unit factors.*

Proof. We prove by inducting on the number n of principal prime factors of an element a. When $n = 1$, we let $a = p$, where p is a principal prime. Assume $a = xy$, where x and y are not units, but this assumption contradicts Lemma 2.3, so either x or y is a unit. Without loss of generality, assume x is a unit. Then we have $(1/x)a = y$, then p is a principal prime, since the product of a unit $(1/x)$ and a principal prime a is a principal prime. Thus the case for $n = 1$ holds.

Suppose the theorem is true for all a that can be expressed as a product of $n-1$ principal primes. Let $a = p_1p_2 \cdots p_{n-1}p_n = q_1q_2 \cdots q_k$, where p_i and q_j are principal primes. Then q_k divides some p_i. Without loss of generality, assume q_k divides p_n, which implies $p_n = uq_k$, since p_n and q_k are irreducible. So we have

$$a/p_n = p_1p_2 \cdots p_{n-1} = q_1q_2 \cdots q_{k-1}((1/u)),$$

hence,

$$a = p_1p_2 \cdots p_{n-1}p_n = q_1q_2 \cdots q_{k-1}((1/u)p_n).$$

Since a/p_n is the product of $n-1$ principal primes, by the induction hypothesis $n-1 = k-1$. Therefore, $n = k$ and p_i, q_i differ by unit factors. □

Theorem 2.5. *Let R be an integral domain. Let S be the set of all elements in R expressible as a product of principal primes. Then S is a saturated multiplicatively closed set.*

Proof. It is clearly that S is a multiplicatively closed set. Then we need to show that for all $ab \in S$, $a \in S$ and $b \in S$. Suppose $ab = p_1p_2...p_n$, a product of principal primes, then p_1 must divide a or b. Say $a = p_1a_1$. Then $a_1b = p_2p_3...p_n$. By induction on n, we have that both a_1 and b are in S, and hence $a, b \in S$. □

3 Localization

Let S be a multiplicatively closed set in R. Let A be an R-module. Define A_S to be the set of equivalent classes of pairs (a, s) with $a \in A, s \in S$, the equivalent relation being $(a, s) \sim (a_1, s_1)$ if there exists $s_2 \in S$, such that $s_2(s_1a - sa_1) = 0$.

We can make A_S into an abelian group by $(a, s)+(a_1, s_1) = (s_1a+sa_1, ss_1)$, and then into an R-module by $x(a, s) = (xa, s)$. The notation for the equivalence class of (a, s) denoted as a/s or $\frac{a}{s}$. We assume S is saturated and $1 \in S$.

There is a natural ring homomorphism from R to R_S.

$I_S \subset R_S$ consists of all i/s with $i \in I, s \in S$. The ideal I "explodes" to R_S (i.e. $I_S = R_S$) if and only if I contains an element in S, and I collapses to 0 if every element of I is annihilated by some element of S.

Given an ideal $J \subset R_S$, there is a well-defined complete inverse image I in R, it consists of all x with $x/1 \in J$.

If we go from J to I and then back to I_S, we find $I_S = J$. If we start with $I \subset R$, pass to I_S, and then return to an ideal of R, we generally get a larger ideal.

Theorem 3.1. *The mappings described above implement a one-to-one order-preserving correspondence between all the prime ideals in R_S and those prime ideals in R disjoint from S.*

We note that the maximal ideals in R_S are the maximal primes disjoint from S.

Theorem 3.2. *The mappings described above implement a one-to-one order-preserving correspondence between all the prime ideals in R_P and all the prime ideals in R contained in P. Thus R_P is a local ring with maximal ideal P_P.*

We then define short exact sequences.

Definition 3.1.

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

is called *a short exact sequence* if $im(f) = ker(g)$ and f is one-to-one and g is onto.

When we localize each R-module on a short exact sequence with a multiplicatively closed set S, we still get a short exact sequence of R_S-modules, as the following theorem:

Theorem 3.3. *If*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

is an short exact sequence of R-modules, then

$$0 \longrightarrow A_S \xrightarrow{f_s} B_S \xrightarrow{g_s} C_S \longrightarrow 0$$

is an short exact sequence of R_S-modules.

Proof. Define f_s as $f_s(a/s) = f(a)/s$. Let $f_s(a/s) = 0/1$, which implies $f(a)/s = 0/1$, so there exists $s' \in S$ such that $s'f(a) = 0$, which means $f(s'a) = 0$. Then $s'a = 0$ implies $a/1 = 0$ in A_S. Thus, f_s is one-to-one.

We claim that $im(f_s) = ker(g_s)$. Indeed, firstly let $f_s(a/s) = 0$. Since $a/s \in A_S$, $f_s(a/s) = f(a)/s$, then $g_s(f(a)/s) = g(f(a))/s = 0/s = 0$. Thus, $im(f_s) \subseteq ker(g_s)$. Next, suppose $b/s \in ker(g_s)$, then $g_s(b/s) = 0/1$ in C_S, which implies $g(b)/s = 0$ in C_S. So there exists $s_0 \in S$ such that $s_0 g(b) = 0$, which implies $g(s_0 b) = 0$. Thus, $s_0 b \in ker(g) = im(f)$. So $s_0 b = f(a), a \in A$, then $b = f(a)/s_0$ in B_S. So $b/s = f(a)/ss_0 = f_s(a/ss_0) \in im(f_s)$. Thus, $ker(g_s) \subseteq im(f_s)$. Therefore, $im(f_s) = ker(g_s)$.

Since g is onto, for all $c \in C$, there exists $b \in B$ such that $g(b) = c$. So $g(b)/s = c/s$ for $0 \neq s \in S$. Then by definition, $g_s(b/s) = c/s$, where $b/s \in B_S, c/s \in C_S$. Thus, g_s is onto. Therefore,

$$0 \longrightarrow A_S \xrightarrow{f_s} B_S \xrightarrow{g_s} C_S \longrightarrow 0$$

is an short exact sequence of R_S-modules. □

4 Noetherian Rings

Definition 4.1. A commutative ring R is *Noetherian* if it satisfies one of the followings:

(1) Every ideal in R is finitely generated;

(2) The ideals in R satisfy the ascending chain condition (ACC);

(3) If X is nonempty and is a collection of ideals, X has a maximal element, not need to be ideal.

Theorem 4.1 (Hilbert basis Theorem)**.** *If R is Noetherian, then $R[x]$ is also Noetherian.*

Proof. Suppose R is Noetherian. Let I be an ideal of $R[x]$, to prove $R[x]$ is Noetherian, we need to show that I is finitely generated. We want to prove by contradiction, then suppose there exists an ideal I in $R[x]$ which is not finitely generated. We set $I_0 = (0)$. Let $f_1 \in I$ be a polynomial in I of least degree and $I_1 = (f_1)$. Let f_2 be a polynomial of least degree in $I \backslash (f_1)$ and $I_2 = (f_1, f_2)$. Repeating the process, we let f_m be a polynomial of lease degree in $I \backslash (f_1, \ldots, f_{m-1})$ and $I_m = (f_1, \ldots, f_m)$. By this setting, we have

(1)$\deg(f_1) \leq \deg(f_2) \leq \deg(f_3) \leq \cdots$

(2)$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$

Next, we let a_m be the leading coefficient of f_m and $J_m = (a_1, \ldots, a_m)$, so we get a chain of ideals $J_1 \subseteq J_2 \subseteq J_3 \subseteq \cdots$. Since this is a chain of ideals in R and R is Noetherian, there exists $n \in \mathbb{N}$ such that $J_n = J_{n+1} = J_{n+2} = \cdots$. Thus, a_{n+1}, which is the leading coefficient of f_{n+1}, is in J_n, so we can write $a_{n+1} = \sum_{i=1}^{b} r_i a_i$ for some $r_i \in R$. We then let

$$f = f_{n+1} - \sum_{i=1}^{n} r_i (x^{deg(f_{n+1}) - deg(f_i)}) f_i,$$

so $\deg(f) < \deg(f_{n+1})$ and $f \in I_{n+1}$. Since f_{n+1} is a polynomial of least degree in $I \backslash (f_1, ..., f_n)$, we have $f \in I_n$. Moreover, because

$$f_{n+1} = f + \sum_{i=1}^{n} r_i (x^{deg(f_{n+1}) - deg(f_i)}) f_i,$$

we then have $f_{n+1} \in I_n$, which is a contradiction by the setting of f_{n+1}. Thus, every I in $R[x]$ is finitely generated, which implies $R[x]$ is Noetherian.

□

Corollary 4.2. *Let n be a positive integer. If R is a Noetherian ring, then the polynomial ring $R[x_1, ..., x_n]$ is also a Noetherian ring.*

Proof. By iterating Hilbert basis Theorem. □

Then we want to prove the Krull Intersection Theorem. Before the proof, we need to define *Jacobson radical*.

Definition 4.2. $J(R) = \{x \in R : \forall y \in R, 1 + xy \in U(R)\}$ is called the *Jacobson radical* of R, where $U(R)$ is the group of units of R.

Theorem 4.3 (The Krull Intersection Theorem)**.** *Let R be a commutative Noetherian ring, and let $I = a_1R + \cdots + a_nR$ be an ideal of R. If an element b of R belongs to $\bigcap_{k=1}^{\infty} I^k$, then b is an element of bI.*

In particular, if $a_1, \ldots, a_n \in J(R)$, or if R is an integral domain, then $b = 0$ and therefore, $\bigcap_{k=1}^{\infty} I^k = 0$.

Proof. For each $k \geq 1$, b belongs to I^k, there exists a homogeneous polynomial $P_k(x_1, \dots, x_n)$ of degree k such that $b = P_k(a_1, \dots, a_n)$. In the Noetherian ring $S = R[x_1, \dots, x_n]$, we consider the ascending chain of ideals defined by

$$J_k = P_1 S + \cdots + P_k S.$$

If we fix an integer m such that $J_m = J_{m+1}$, then we can write $P_{m+1} = Q_m P_1 + \cdots + Q_1 P_m$, where $Q_i(x_1, \dots, x_n)$ is homogeneous of degree i. Substituting $x_1 = a_1, \dots, x_n = a_n$, we obtain

$$b = b(Q_1(a_1, \dots, a_n) + \cdots + Q_m(a_1, \dots, a_n)). \tag{1}$$

Now for $i = 1, \dots, m$, the polynomial Q_i is homogeneous of positive degree, so $Q_i(a_1, \dots, a_n)$ is in the ideal (I). From this, it follows that b lies in bI.

In the particular case, with I is contained in $J(R)$, (1) leads to $(1 - \lambda)b = 0$, with $\lambda \in I \subseteq J(R)$. By the definition of $J(R)$, $1 - \lambda$ is a unit, so $b = 0$.

Suppose R is an integral domain. Since b lies in bI, then $b = bi$ with $i \in I$, so we have $b(1 - i) = 0$. Since $1 - i \neq 0$ and R is an integral domain, $b = 0$. Therefore, $\bigcap_{k=1}^{\infty} I^k = 0$ $\square$

Theorem 4.4 (Nakayama's Lemma). *Let R be a commutative ring, let M be a finitely generated left R-module, and assume that $J(R)M = M$, where $J(R)$ is the Jacobson of R. Then M=0.*

Proof. Let $m_1, \dots, m_r$ be a minimal generating set of M. Then we assume that $r > 0$ and want to reach a contradiction. Since $J(R)M = M$, we have $m_1 = j_1 m_1 + \cdots + j_r m_r$ for $j_1, ..., j_r \in J$, which is $(1 - j_1)m_1 = j_2 m_2 + \cdots + j_r m_r$. Since $(1 - j_1)$ is invertible, this enables us to express m_1 in terms of the remaining $m's$. However, $m_1, \dots, m_r$ is the minimal generating set, so this is a contradiction. Thus, $m_i = 0$, which implies $M = 0$. $\square$

5 Unique Factorization Domains

Now, we are ready to learn about unique factorization domains. This section includes important theorems and examples about unique factorization domains.

Definition 5.1. Suppose R is a commutative ring with unity 1_R, $a, b \in R$ are *associates* if there exits u which is a unit of R such that $a = u \cdot b$.

After know the definition about two elements being associates, we can give the definition of unique factorization domains.

Definition 5.2. An integral domain R is called a *unique factorization domain* (or UFD) if it satisfies the following two conditions:

(1) For all $a \in R$ with $a \neq 0$ and a is not unit, we can write $a = p_1 p_2 ... p_n$, where $n \in \mathbb{Z}_{>0}$, and each p_i is irreducible in R.

(2) If $a = p_1 p_2 ... p_n = q_1 q_2 ... q_m$ with each q_i is irreducible in R, then $n = m$, and after possible rearrangement, p_i and q_i are associates for all i.

Theorem 5.1. *Suppose R is a UFD. $p \in R$ is irreducible if and only if p is prime.*

Proof. ($\Leftarrow$) Suppose $p \in R$ is prime and $p = a \cdot b$, so $p \mid ab$, then by definition $p \mid a$ or $p \mid b$. Without loss of generality, assume $p \mid a$, so $\exists\, c \in R$ such that $a = p \cdot c$. Then $p = a \cdot b = p \cdot c \cdot b$, which implies $p(1 - c \cdot b) = 0$. Since R is a UFD, then is an integral domain, so $(1 - c \cdot b) = 0$, since $p \neq 0$ by definition. Thus, $c \cdot b = 1$, which implies b is a unit. So $p \in R$ is irreducible.

($\Rightarrow$) Suppose $p \in R$ is irreducible and $p \mid ab$, then $\exists\, c \in R$ such that $a \cdot b = p \cdot c$. Since R is a UFD, we can express $a = a_1 \cdots a_n$, $b = b_1 \cdots b_m$, $c = c_1 \cdots c_k$ with u_i is unit and a_i, b_j, c_l are irreducible, with $1 \leq i \leq n, 1 \leq j \leq m, 1 \leq l \leq k$. Thus,

$$p \cdot c_1 \cdot c_2 \cdots c_k = a_1 \cdot a_2 \cdots a_n \cdot b_1 \cdots b_m.$$

Then by the uniqueness of product of irreducibles, we get $n + m = k$. Thus, p is an associate of a_i for some i or b_j for some j. If p is an associate of a_i, then $p|a$, or if p is an associate of b_j, then $p|b$. Therefore, $p \in R$ is prime. □

Corollary 5.2. *Let R be an integral domain. R is a UFD if and only if every non-zero and non-unit element in R is a product of prime elements.*

Proof. ($\Rightarrow$) Follows from Definition 5.2 and Theorem 5.1.

($\Leftarrow$) Suppose an element $a \in R$ is a product of prime elements, say $a = p_1 p_2 \cdots p_n$, where p_i is prime. Since R is an integral domain, by the proof of Theorem 5.1, each p_i is irreducible. Next, we want to show that if $b_1, \ldots, b_n, c_1, \ldots, c_m$ are prime elements in R such that

$$b_1 \cdots b_n = c_1 \cdots c_m,$$

then $n = m$ and after rearrangement, we have b_i and c_i are associates.

We prove by inducting on n. If $n = 1$, then we have $b_1 = c_1 \cdots c_m$. Since b_1 is irreducible, $m = 1$, so $b_1 = c_1$. Assume the uniqueness property holds for some n and then we have

$$b_1 \cdots b_n \cdot b_{n+1} = c_1 \cdots c_m,$$

so $b_{n+1} \mid (c_1 \cdots c_m)$. Since b_i is a prime element for $1 \leq i \leq n+1$, it follows that $b_{n+1} \mid c_j$ for $1 \leq j \leq m$, say $b_{n+1} \mid c_m$. Then there exists some $a \in R$ such that $c_m = ab_{n+1}$. Since c_m, b_{n+1} are irreducible, a must be a unit. So b_{n+1} and c_m are associates. Then we obtain that

$$b_1 \cdots b_n \cdot b_{n+1} = c_1 \cdots c_{m-1} \cdot ab_{n+1}.$$

Since R is an integral domain, we get

$$b_1 \cdots b_n = c_1 \cdots c_{m-1} \cdot a.$$

Since c_{m-1} is irreducible and a is a unit, the product $c_{m-1}a$ is an irreducible element. Therefore, by the inductive assumption, $n = m - 1$ and after rearrangement, we have b_i and c_i are associates. So R is a UFD. □

Theorem 5.3. *If R is a Noetherian integral domain, then R satisfies UFD 1.*

Proof. Suppose R is a Noetherian integral domain and a non-zero and non-unit element a in R can not be written as a product of finitely many irreducibles, then a is not irreducible. So $a = a_1 \cdot b_1$, where a_1, b_1 are not units and at least one of a_1 or b_1 can not be written as a product of finitely many irreducibles. Without loss of generality, assume that it is a_1, then $a_1 = a_2 \cdot b_2$. We can continue the same process. In this way, we get the chain $\langle a \rangle \subsetneq \langle a_1 \rangle \subsetneq \langle a_2 \rangle \subsetneq \cdots$, which contradicting ACC condition. Thus, R satisfies UFD 1. □

The first example of unique factorization domain we want to show is GCD domains and LCM domains as the following proposition:

Proposition 5.4. *Suppose R be a UFD. Then R is also a GCD domain and an LCM domain, i.e., every pair of non-zero, non-unit elements in R has a greatest common divisor and a least common multiple.*

Proof. Suppose R is a UFD and non-zero, non-unit elements $a, b \in R$, then we can write

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$$

and

$$b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$$

where p_i is irreducible and prime in R and $a_i, b_i \geq 0$.

Let c_i =min$\{a_i, b_i\}$, consider

$$c = p_1^{c_1} p_2^{c_2} \cdots p_n^{c_n}$$

then $c \mid a$ and $c \mid b$, so c is a common divisor of a and b. Let $d \mid a$ and $d \mid b$ where $d \in R$. If d is a unit, $d \mid c$, so gcd(a, b)=c. If d is not a unit, we can write

$$d = p_1^{d_1} p_2^{d_2} \cdots p_n^{d_n}$$

then $d \mid a$ for $d_i \leq a_i$ $\forall i$ and $d \mid b$ for $d_i \leq b_i$ $\forall i$. Also $d_i \leq$min$\{a_i, b_i\} \implies d_i \leq c_i \implies d \mid c$. Thus, gcd$(a, b)$=c.

Similarly, let e_i=max$\{a_, b_i\}$, consider

$$e = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$$

then $a \mid e$ and $b \mid e$, so e is a common multiple of a and b. Let $a \mid f$ and $b \mid f$ where $f \in R$. If f is a unit, $e \mid f$, so lcm(a, b)=e. If f is not a unit, we can write

$$f = p_1^{f_1} p_2^{f_2} \cdots p_n^{f_n}$$

then $a \mid f$ for $f_i \geq a_i$ $\forall i$ and $b \mid f$ for $f_i \geq b_i$ $\forall i$. Also $f_i \geq$max$\{a_i, b_i\} \implies f_i \geq e_i \implies e \mid f$. Thus, lcm$(a, b)$=e. Therefore, R is also a GCD domain and LCM domain. □

However, the following proposition shows that a GCD domain is not necessary to be a UFD.

Proposition 5.5. *Suppose $A = \mathbb{Z} + X\mathbb{Q}[X]$, then A is a GCD domain, but not a UFD.*

Proof. Since $\langle X \rangle \subsetneq \langle \frac{X}{2} \rangle \subsetneq \langle \frac{X}{4} \rangle \subsetneq \cdots$ is an ascending chain of principal ideals that does not terminate, A does not satisfy the ascending condition on principal ideals, so A is not a UFD.

To see that A is a GCD domain, let $f, g \in A$ be non-zero, non-unit elements. We will use the fact that f and g have a GCD in $\mathbb{Q}[X]$ and that GCDs in $\mathbb{Q}[X]$ are unique only up to units.

We write $f = nf_0$ and $g = mg_0$, where $n, m \in \mathbb{Z}$ are such that both f_0 and g_0 have constant terms equal to 1. Let $d_0 \in \mathbb{Q}[X]$ be the GCD of f_0 and g_0 so that d_0 also has constant term equal to 1. In $\mathbb{Q}[X]$ we have equations $f_0 = d_0 \cdot u$ and $g_0 = d_0 \cdot v$. Then u and

v must have constant term equal to 1, and so belong to A. In other words, d_0 is a common divisor of f_0 and g_0 in A.

Suppose $h \mid f_0$ and $h \mid g_0$ for some $h \in A$. Since the constant term of h is an integer, it must be ± 1. Since h is also a common divisor of f_0 and g_0 in $\mathbb{Q}[X]$, h divides d_0 in $\mathbb{Q}[X]$, say $d_0 = h \cdot q$, for $q \in \mathbb{Q}[X]$. Since the constant term of h is ± 1, it follows that the constant term of q is ± 1, so $q \in A$. In other words, d_0 is a GCD of f_0 and g_0 in A.

Suppose $z \in \mathbb{Z}$ is the GCD of n and m, since d_0 is a GCD of f_0 and g_0 in A, and $f = nf_0$ and $g = mg_0$, then $z \cdot d_0$ is a GCD of f and g in A. Thus, A is a GCD domain. □

Theorem 5.6. *An integral domain is a UFD if and only if every non-zero prime ideal in R contains a principal prime.*

Proof. ($\Rightarrow$) Assume R is a UFD and P a non-zero prime ideal in R. Unless P is a field, P will contain an element a that is neither 0 or a unit. When a is written as a product of principal primes, $a = p_1 p_2 ... p_r$, one of the factors p_i must be contained in P.

($\Leftarrow$)Assume that every non-zero prime ideal in R contains a principal prime. As in Theorem 2.5, denote by S, the set of all products of principal primes. It is to show that S contains every element in R that is neither 0 nor a unit. We want to prove by contradiction. Suppose c is an element of R that is not 0, not a unit, and not in S. Since S is saturated, the principal ideal (c) is disjoint from S. Again, using the Zorn's Lemma, we can expand (c) to a prime ideal P disjoint from S, by Theorem 2.1 and Theorem 2.2. By hypothesis, P contains a principal prime in S, which is a contradiction. Thus, R is a UFD. □

Corollary 5.7. *Suppose S is multiplicatively closed in a UFD R, then R_S is a UFD.*

Proof. Suppose R is a UFD and $Q \subseteq R_S$ is prime, then $Q = P_S$ where $P \subseteq R$ is prime. So there exists a prime element $p \in P$, such that $p/1 \in R_S$ is prime. Thus, $p/1 \in Q$. Then we can conclude that Q contains a principal prime. By theorem 5.6, R_S is a UFD. □

Theorem 5.8 (Nagata's Lemma)**.** *Let R be an integral domain, $\mathcal{P} := \{p_i\}_{i \in I}$ be a collection of prime elements, and let S be the multiplicatively closed set generated by the p_i. Assume that no element in R is divisible by infinitely many $p \in \mathcal{P}$ (e.g., R satisfies ACC on principal ideals) and R_S is a UFD, then R is a UFD.*

Proof. By Theorem 5.6, it suffices to show every prime ideal contains a principal prime. Suppose R_S is a UFD. Let $P \subseteq R$ be a prime ideal. If $P \cap S \neq \emptyset$, then $\exists s \in P$, such that $s = p_1 \cdots p_r$. Since P is prime, some $p_i \in P$. If $P \cap S = \emptyset$, then $P_S \subseteq R_S$ is a prime ideal, so $\exists\ p/s \in R_S$ is a principal prime in P_S with $p \in P$. Take $p \in P$ such that $p/1 \in P_S$. Since no element in R is divisible by infinitely many $p \in \mathcal{P}$, we write $p = p_0 \cdot p_1 \cdots p_t$, where $p_1 \cdots p_t \in S$ and p_0 is not divisible by a prime in S. Then $p_0 \notin S$. So we have $p/1 \cdot R_S = p_0/1 \cdot R_S$.

We claim that p_0 is prime. Indeed, suppose $p_0 \mid ab$, then $\exists\ c$ such that $p_0 c = ab$ and so $\frac{p_0}{1} \cdot \frac{c}{1} = \frac{a}{1} \cdot \frac{b}{1}$ in $R_S \implies \frac{p_0}{1} \mid \frac{a}{1}$ or $\frac{p_0}{1} \mid \frac{b}{1}$ in R_S. Without loss of generality, assume $\frac{p_0}{1} \mid \frac{a}{1}$ in R_S, then there exists $s \in S$ and $r \in R$ such that $sa = p_0 r$. Since $s \in S$, we can write $s = q_1 \cdots q_k$. Then we have $q_1 \cdots q_k \cdot a = p_0 \cdot r$, which implies $q_1 \mid p_0 r$. So by the choice of p_0, we have $q_1 \mid r$. Thus, we get $q_2 \cdots q_k \cdot a = p_0 r'$, where $r' \in R$. By induction, we have $a = p_0 r_0$, where $r_0 \in R$, so $p_0 \mid a$. Thus, p_0 is prime. Then $p \in P$ is a principal prime.

So we have every prime ideal in R contains a principal prime, thus by Theorem 5.6, R is a UFD. $\square$

Definition 5.3. An ideal I of a commutative ring R with identity 1_R is principal if $I = \langle a \rangle$ for some $a \in R$, i.e.

$$I = \{ra : r \in R\}.$$

An integral domain R is a *principal ideal domain* (PID) if all the ideals of R are principal.

Theorem 5.9. *Every PID is a UFD.*

Proof. Let R be a PID and take P be prime in R. Then $p \in P$ is principal, so P contains a principal prime. Thus, by Theorem 5.6, R is a UFD. $\square$

Theorem 5.10. *R is a UFD if and only if $R[X]$ is a UFD.*

Proof. ($\Rightarrow$) Suppose R is a UFD, S is the set of all products of primes, and K is the field of fractions. Then $R_S[X] = (R[X])_S = K[X]$. Since $K[X]$ is a PID, then it is a UFD. So $R_S[X]$ is a UFD. Thus, by Nagata's Lemma, $R[X]$ is a UFD.

($\Leftarrow$) Suppose $R[X]$ is a UFD. Let a be a non-zero, non-unit element in R, so also in $R[X]$, then by Corollary 5.2, a has a factorization

$$a = p_1 \cdots p_n$$

where p_i is a prime element in $R[X]$. And we have $\deg(a) = \deg(p_1) + \cdots + \deg(p_n) = 0$, which implies each p_i is in R and is prime. Again by Corollary 5.2, R is a UFD. $\square$

We would like to show more examples of unique factorization domains as following:

Proposition 5.11. *Suppose $X_1, Y_1, \ldots, X_n, Y_n$ are indeterminates over R. If R is a UFD and $n \geq 3$, then*

$$R[X_1, Y_1, \ldots, X_n, Y_n]/(X_1Y_1 + \cdots + X_nY_n)$$

is also a UFD.

Proof. The proof will require a couple of claims. Let

$$A := R[X_1, Y_1, \ldots, X_n, Y_n]/(X_1Y_1 + \cdots + X_nY_n).$$

First we want to show that A is an integral domain when $n \geq 2$. We claim that if A' is a commutative ring, x in A' is a non-zerodivisor, and A'_x is an integral domain, then A' is an integral domain.

We first prove the claim. Suppose $u \cdot v = 0$ in A', then we get $\frac{u}{1} \cdot \frac{v}{1} = 0$ in A'_x. Since A'_x is an integral domain, $\frac{u}{1} = 0$ or $\frac{v}{1} = 0$. Without loss of generality, assume $\frac{u}{1} = 0 = \frac{0}{1}$, then there exists x^n such that $x^n(1 \cdot u - 0 \cdot 1) = 0$, which is $x^n \cdot u = 0$. Since x is a non-zerodivisor, $x(x^{n-1} \cdot u) = 0$ implies $x^{n-1} \cdot u = 0$. Then by induction, $u = 0$. Thus, A' is an integral domain.

We want to apply the claim to A, so we need to show that X_1 is a non-zerodivisor in A and show A_{X_1} is an integral domain.

To see X_1 is a non-zerodivisor in A. Suppose $X_1 f = 0$ in A, then

$$X_1 f = g(X_1Y_1 + \cdots + X_nY_n),$$

for some g in $R[X_1, Y_1, \ldots, X_n, Y_n]$. Thus, $X_1(f - gY_1) = g(X_2Y_2 + \cdots + X_nY_n)$. Since X_1 does not divide $X_2Y_2 + \cdots + X_nY_n$, it divides g. Therefore, f is a multiple of $X_1Y_1 + \cdots + X_nY_n$, so $f = 0$ in A.

To show A_{X_1} is an integral domain, our second claim is that if $A^{'}$ be a commutative ring, and $W_1, \ldots, W_n$ are indeterminates over $A^{'}$ and consider $F = uW_1 + a_2W_2 + \cdots + a_nW_n$, where u is a unit in $A^{'}$, and $a_2, \ldots, a_n$ are arbitrary elements in $A^{'}$. Then

$$A^{'}[W_1, \ldots, W_n]/(F) \cong A^{'}[W_2, \ldots, W_n].$$

The proof of the claim: we first define

$$\phi : A^{'}[W_1, \ldots, W_r] \to A^{'}[W_2, \ldots, W_r]$$

by sending W_1 to $(-va_2W_2 - \cdots - va_nW_n)$, where $v = u^{-1}$ and W_i to W_i, for $i \geq 2$ and extending it to all polynomial in $W_1, \ldots, W_n$. Then ϕ is a surjective ring homomorphism, and F is in the kernel of ϕ.

To see that F generates the kernel of ϕ, let H belong to the kernel of ϕ, and write H as a polynomial in W_1 with coefficients in $A^{'}[W_2, \ldots, W_n]$. We induct on the degree of W_1 in H. If it equals zero, then H has to be zero, since ϕ takes H to H in this case. Suppose the degree of W_1 in H is greater than zero. Since F is a monic polynomial in W_1, we can use the division algorithm and write $H = FG + R$, where the W_1-degree of R is less than the W_1-degree of H. Since $R = H - FG$, R is in the kernel of ϕ. By induction, R is a multiple of F, and thus H is a multiple of F, so we complete the proof of the claim.

We then apply the second claim to show A_{X_1} is an integral domain by taking

$$A^{'} = R[X_1^{-1}, X_1, X_2, \ldots, X_n],$$

and $u = X_1^{-1}, a_i = X_i, W_1 = Y_1, \ldots, W_n = Y_n$, and $F = X_1Y_1 + \cdots + X_nY_n$.

Thus, by the first claim above, we get A is an integral domain when $n \geq 2$.

Now we can give the proof of the Theorem. We have $A/(X_1) = R[Y_1]/(X_2Y_2 + \cdots + X_nY_n)$. Since $n \geq 3, A/(X_1)$ is an integral domain by the second claim above. Therefore, X_1 is a prime element in A. On the other hand, A_{X_1} is a polynomial ring over R, with one of the variables inverted, so then A_{X_1} is a UFD by Theorem 5.10 and Corollary 5.7. Therefore, A is a UFD by Nagata's Lemma. □

The next examples consider the UFD property of coordinate rings over the complex and real numbers.

Proposition 5.12. *Suppose X, Y are indeterminates over $\mathbb{C}$ and set*

$$A_2 = \mathbb{C}[X, Y]/(X^2 + Y^2 - 1),$$

then A_2 is a UFD.

Proof. Since $\mathbb{C}[X,Y] = \mathbb{C}[X+iY, X-iY]$ and $X^2+Y^2-1 = (X+iY)(X-iY)-1$. We can set $U = X+iY$ and $V = X-iY$, then $A_2 = \mathbb{C}[U,V]/(UV-1)$, which is $\mathbb{C}[U]_S$ with $S = \{1, U, U^2, \ldots\}$. We know that $\mathbb{C}[U]$ is a UFD, then by Corollary 5.7, the ring A_2 is a UFD. $\square$

We would have a different conclusion if we change the field from $\mathbb{C}$ to $\mathbb{R}$.

Proposition 5.13. *Suppose X, Y are indeterminates over $\mathbb{R}$ and set*

$$B_2 = \mathbb{R}[X,Y]/(X^2+Y^2-1),$$

then B_2 is not a UFD.

Proof. To see that B_2 is not a UFD, we show that the image of X in B_2 is an irreducible element that is not a prime element.

Since B_2/XB_2 is isomorphic to $\mathbb{R}[Y]/(Y^2-1)$, which is not an integral domain, the image of X in B_2 is not a prime element.

Next, suppose we could factor $X \equiv f \cdot g$ in B_2 with $f, g \in \mathbb{R}[X,Y]$. Thus in $\mathbb{R}[X,Y]$, we can write $X = f \cdot g + h \cdot (X^2+Y^2-1)$. Write f and g as a sum of their homogeneous components, i.e., $f = f_0 + \cdots + f_n$ and $g = g_0 + \cdots + g_m$, where each f_i is a homogeneous polynomial degree i and each g_j is a homogeneous polynomial degree j. Then suppose f_n were divisible by X^2+Y^2, so $f_n = (X^2+Y^2) \cdot f'_{n-2}$. If we set

$$f' = f_0 + \cdots + (f_{n-2} + f'_{n-2} + f_{n-1}),$$

then it follows that $f \equiv f'$ in B_2. Similarly, we may reduce g if g_m were divisible by X^2+Y^2. In other words, without loss of generality, we may write $X \equiv f \cdot g$ in B_2 so that when we express f and g as a sum of their homogeneous components as above, X^2+Y^2 divides neither f_n nor g_m.

We claim that under this additional assumption, $n+m \leq 1$. Indeed, suppose $n+m \geq 2$. From the equation $X \equiv f \cdot g + h \cdot (X^2+Y^2-1)$, we obtain $0 = f_n \cdot g_m + h_{n+m-2} \cdot (X^2+Y^2)$. But then this implies X^2+Y^2 divides either f_n or g_m, which is a contradiction. Thus, we have $n+m \leq 1$. So we get either $n = 0$ or $m = 0$,i.e., either f or g is a unit in $\mathbb{R}[X,Y]$. Therefore, the image of f or g in B_2 is a unit in B_2, which implies that the image of X in B_2 is irreducible. $\square$

From Proposition 5.11 to Proposition 5.13, we notice that the UFD property is a subtle one. To have a deeper view on that, we consider the following proposition:

Proposition 5.14. *If X, Y, Z are indeterminates over $\mathbb{C}$, then for*

$$A_3 = \mathbb{C}[X,Y,Z]/(X^2+Y^2+Z^2-1) \quad \textit{and} \quad B_3 = \mathbb{R}[X,Y,Z]/(X^2+Y^2+Z^2-1)$$

A_3 is not a UFD and B_3 is a UFD.

Sketch of Proof. Since

$$X^2+Y^2+Z^2-1 = (X+iY)(X-iY) + (Z-1)(Z+1),$$

we have $(\overline{X+iY})(\overline{X-iY})+(\overline{Z-1})(\overline{Z+1})=0$ in A_3.

And so $(\overline{X+iY})(\overline{X-iY})=(\overline{1-Z})(\overline{Z+1})$. Since each expression is irreducible in A_3, there are two different factorizations in A_3, which means A_3 is not a UFD.

The example B_3 is a coordinate ring of the real 2-sphere, which is a UFD. We are giving a sketch of the proof and this sketch is based upon a proof given in [5].

Let $\mathbb{R}$ denote the real numbers, and upper case X, Y, Z, U, V, W, T denote indeterminates over $\mathbb{R}$ and lower case x, y, z, u, v, w, t denote homomorphic images of the variables. So, we start with the polynomial ring $\mathbb{R}[X, Y, Z]$ and mod out the principal ideal generated by $X^2+y^2+Z^2-1$, to get the ring B_3, which we want to show is a UFD. Taking T an indeterminate over B_3, it is enough to show $B_3[T]$ is a UFD by Theorem 5.10, and then by Nagata's Lemma, it is enough to show that $B_3[T, T^{-1}]$ is a UFD.

Now let S denote the ring $\mathbb{R}[U, V, W, T]/(U^2+V^2+W^2-T^2)$. Note that t in S is a prime element, since $S/(t)$ is isomorphic to $\mathbb{R}[U, V, W]/(U^2+V^2+W^2)$, an integral domain. If we show S is a UFD, then $S[t^{-1}]$ is a UFD. However, this latter ring is isomorphic to $B_3[T, T^{-1}]$ by the map from $\mathbb{R}[U, V, W, T, T^{-1}]$ that takes U to xT, V to yT, W to zT, T to T in $B_3[T, T^{-1}]$.

Thus, it remains to see S is a UFD. However, $S=\mathbb{R}[U, V, C, D]/(U^2+V^2-CD)$ by setting $C=T-W$ and $D=T+W$. Note that $S/(c)$ is isomorphic to $\mathbb{R}[U, V]/(U^2+V^2)$, so c is prime in S. By the second claim on the proof of Proposition 5.11, $S[c^{-1}]=\mathbb{R}[U, V, C, C^{-1}]$, which is a UFD. Thus, by Nagata's Lemma, S is a UFD, and the sketch of the proof is complete.

6 Complexes and Homology

The goal of this section is to prove the theorem: a short exact sequence of chain complexes implies a long exact sequence on homology. We should first learn about chain complexes and cochain complexes.

Definition 6.1. (1) A *chain complex* is a collection $\mathcal{C}$ of R-modules and R-module maps

$$\mathcal{C}: \cdots \longrightarrow C_{n+1} \xrightarrow{d_{n+1}} C_n \xrightarrow{d_n} C_{n-1} \longrightarrow \cdots$$

satisfying $d_n \circ d_{n+1}=0$, for all n. The d_n are called "*boundary maps*" or "*differentials*".

(1′) A *cochain complex* is a collection $\mathcal{C}'$ of R-module and R-module maps

$$\mathcal{C}': \cdots \longrightarrow C'_{n-1} \xrightarrow{\delta_n} C'_n \xrightarrow{\delta_{n+1}} C'_{n+1} \longrightarrow \cdots$$

satisfying $\delta_{n+1} \circ \delta_n=0$, for all n.

(2) Let $\mathcal{C}$ be a chain complex. For each n we define $Z_n(\mathcal{C}) := ker(d_n)$, $B_n(\mathcal{C}) := im(d_{n+1})$ and $H_n(\mathcal{C}) := Z_n(\mathcal{C})/B_n(\mathcal{C})$. These modules are, respectively, the module of "*n-cycles*", the module of "*n-boundaries*" and the n^{th} "*homology*" module associated to $\mathcal{C}$. Note that

$B_n(\mathcal{C}) \subseteq Z_n(\mathcal{C})$, since $d_n \circ d_{n+1} = 0$.

(2′) Let $\mathcal{C}'$ be a cochain complex. We define $Z^n(\mathcal{C}') := ker(\delta_{n+1})$, $B^n(\mathcal{C}') := im(\delta_n)$ and $H^n(\mathcal{C}') := Z^n(\mathcal{C}')/B^n(\mathcal{C}')$ for each n. These modules are, respectively, the module of "*n-cocycles*", the module of "*n-coboundaries*" and the n^{th} "*cohomology*" module associated to $\mathcal{C}'$. Note that $B^n(\mathcal{C}') \subseteq Z^n(\mathcal{C}')$, since $\delta_{n+1} \circ \delta_n = 0$.

(3) A *chain map* $f : \mathcal{C} \to \mathcal{D}$ between chain complexes $\mathcal{C}$ and $\mathcal{D}$ is a collection of homomorphisms $f_n : C_n \to D_n$ such that the diagram

$$\begin{tikzcd}
\cdots \arrow[r] & C_{n+1} \arrow[r, "d_{n+1}"] \arrow[d, "f_{n+1}"'] & C_n \arrow[r, "d_n"] \arrow[d, "f_n"'] & C_{n-1} \arrow[r] \arrow[d, "f_{n-1}"'] & \cdots \\
\cdots \arrow[r] & D_{n+1} \arrow[r, "\delta_{n+1}"'] & D_n \arrow[r, "\delta_n"'] & D_{n-1} \arrow[r] & \cdots
\end{tikzcd}$$

commutes for all n. It follows that $f_n(Z_n(\mathcal{C})) \subseteq Z_n(\mathcal{D})$ and $f_n(B_n(\mathcal{C})) \subseteq B_n(\mathcal{D})$, So we obtain induced maps on homology $f_* : H_n(\mathcal{C}) \to H_n(\mathcal{D})$.

(3′) A *cochain map* between cochain complexes is defined analogously and induces maps on cohomology. If $f : \mathcal{C}' \to \mathcal{D}'$ is a cochain map, we denote the induced map on cohomology by $f^* : H^n(\mathcal{C}') \to H^n(\mathcal{D}')$.

(4) A sequence $\mathcal{A} \xrightarrow{f} \mathcal{B} \xrightarrow{g} \mathcal{C}$ of chain complexes and chain maps is said to be exact, if for each n, the sequence $A_n \xrightarrow{f_n} B_n \xrightarrow{g_n} C_n$ is exact. A short exact sequence of complexes is an exact sequence of complexes $0 \longrightarrow \mathcal{A} \xrightarrow{f} \mathcal{B} \xrightarrow{g} \mathcal{C} \longrightarrow 0$.
Thus, a short exact sequence of complexes is a commutative diagram

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
\cdots \arrow[r] & A_{n+1} \arrow[r] \arrow[d, "f_{n+1}"'] & A_n \arrow[r] \arrow[d, "f_n"'] & A_{n-1} \arrow[r] \arrow[d, "f_{n-1}"'] & \cdots \\
\cdots \arrow[r] & B_{n+1} \arrow[r] \arrow[d, "g_{n+1}"'] & B_n \arrow[r] \arrow[d, "g_n"'] & B_{n-1} \arrow[r] \arrow[d, "g_{n-1}"'] & \cdots \\
\cdots \arrow[r] & C_{n+1} \arrow[r] \arrow[d] & C_n \arrow[r] \arrow[d] & C_{n-1} \arrow[r] \arrow[d] & \cdots \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

To prove the theorem of this section, we need the Snake Lemma.

Lemma 6.1 (Snake Lemma)**.** *Consider the commutative diagram with exact rows*

$$\begin{tikzcd}
 & C' \arrow[r, "i'"] \arrow[d, "f"] & D' \arrow[r, "\pi'"] \arrow[d, "g"] & E' \arrow[r] \arrow[d, "h"] & 0 \\
0 \arrow[r] & C \arrow[r, "i"'] & D \arrow[r, "\pi"'] & E. &
\end{tikzcd}$$

Then we have an exact sequence

$$ker(f) \longrightarrow ker(g) \longrightarrow ker(h) \xrightarrow{\partial} coker(f) \longrightarrow coker(g) \longrightarrow coker(h).$$

Theorem 6.2. *Let* $0 \longrightarrow \mathcal{C} \xrightarrow{f} \mathcal{D} \xrightarrow{g} \mathcal{E} \longrightarrow 0$ *be a short exact sequence of chain complexes. Then we have a long exact sequence on homology*

$$\cdots \longrightarrow H_{n+1}(\mathcal{E}) \xrightarrow{\partial_{n+1}} H_n(\mathcal{C}) \xrightarrow{f_*} H_n(\mathcal{D}) \xrightarrow{g_*} H_n(\mathcal{E}) \xrightarrow{\partial_n} H_{n-1}(\mathcal{C}) \longrightarrow \cdots .$$

Proof. Consider the following snake diagram

$$\begin{tikzcd}
 & C_n/B_n(\mathcal{C}) \arrow[r] \arrow[d, "d_{\mathcal{C}}"] & D_n/B_n(\mathcal{D}) \arrow[r] \arrow[d, "d_{\mathcal{D}}"] & E_n/B_n(\mathcal{E}) \arrow[r] \arrow[d, "d_{\mathcal{E}}"] & 0 \\
0 \arrow[r] & Z_{n-1}(\mathcal{C}) \arrow[r] & Z_{n-1}(\mathcal{D}) \arrow[r] & Z_{n-1}(\mathcal{E}). &
\end{tikzcd}$$

The horizontal maps are derived from the chain maps f and g, and the vertical maps are given by $d(x_n + B_n) = dx_n$. The kernel of a vertical map is $\{x_n + B_n : x_n \in Z_n\} = H_n$, the cokernel is $Z_{n-1}/B_{n-1} = H_{n-1}$. The diagram is commutative by the definition of a chain map. But in order to apply the Snake Lemma, we must verify that the rows are exact, and this involves another application of the snake lemma.

Then consider the diagram

$$\begin{tikzcd}
0 \arrow[r] & C_n \arrow[r, "f_n"] \arrow[d, "c"] & D_n \arrow[r, "g_n"] \arrow[d, "d"] & E_n \arrow[r] \arrow[d, "e"] & 0 \\
0 \arrow[r] & C_{n-1} \arrow[r, "f_{n-1}"'] & D_{n-1} \arrow[r, "g_{n-1}"'] & E_{n-1} \arrow[r] & 0
\end{tikzcd}$$

where the horizontal maps are again derived from f and g. Since $0 \longrightarrow \mathcal{C} \xrightarrow{f} \mathcal{D} \xrightarrow{g} \mathcal{E} \longrightarrow 0$ is a short exact sequence, each row of the second diagram is exact, then by Snake Lemma, we have an exact sequence

$$ker(c) \longrightarrow ker(d) \longrightarrow ker(e) \xrightarrow{\partial} coker(c) \longrightarrow coker(d) \longrightarrow coker(e).$$

Now let us denote

$$A' = ker(c), B' = ker(d), C' = ker(e), D' = coker(c), E' = coker(d), F' = coker(e).$$

Then we have the diagram

$$\begin{tikzcd}
 & A' \arrow[r] \arrow[d] & B' \arrow[r] \arrow[d] & C' \arrow[d] & \\
0 \arrow[r] & C_n \arrow[r, "f_n"] \arrow[d, "c"'] & D_n \arrow[r, "g_n"] \arrow[d, "d"'] & E_n \arrow[r] \arrow[d, "e"'] & 0 \\
0 \arrow[r] & C_{n-1} \arrow[r, "f_{n-1}"'] \arrow[d] & D_{n-1} \arrow[r, "g_{n-1}"'] \arrow[d] & E_{n-1} \arrow[r] \arrow[d] & 0 \\
 & D' \arrow[r] & E' \arrow[r] & F' &
\end{tikzcd}$$

We claim that the first and forth sequences are exact. Indeed. We denote induced maps by an overbar. Let $x \in A' = ker(c)$ and $y = \overline{f}_n x = f_n x$, then $g_n y = g_n f_n x = 0$, so $y \in ker(\overline{g}_n)$. On the other hand, if $y \in B' \subseteq D_n$ and $\overline{g}_n y = g_n y = 0$, then $y = f_n x$ for some $x \in C_n$. Thus $0 = dy = df_n x = f_{n-1}cx$, and since f_{n-1} is injective, $cx = 0$. Therefore $y = f_n x$ with $x \in A'$, and $y \in im(\overline{f}_n)$. So $A' \to B' \to C'$ is exact.

Next, let $x \in C_{n-1}$, then $\overline{g}_{n-1}(f_{n-1}x + im(d)) = g_{n-1}f_{n-1}x + im(e) = 0$ by the exactness of the sequence $0 \to C_{n-1} \to D_{n-1} \to E_{n-1} \to 0$, so $im(\overline{f}_{n-1}) \subseteq ker(\overline{g}_{n-1})$. Conversely, if $y \in D_{n-1}$ and $\overline{g}_{n-1}(y + im(d)) = g_{n-1}y + im(e) = 0$, then $g_{n-1}y = ez$ for some $z \in E_n$. Since g_n is surjective, $z = g_n x$ for some $x \in D_n$. So we have $g_{n-1}y = ez = eg_n x = g_{n-1}dx$, so $y - dx \in ker(g_{n-1}) = im(f_{n-1})$. Let $y - dx = f_{n-1}w$ with $w \in C_{n-1}$. Therefore, $y + im(d) = \overline{f}_{n-1}(w + im(c))$ and $y + im(d) \in im(\overline{f}_{n-1})$. So $D' \to E' \to F'$ is exact.

Moreover, we know that if f_n is injective, so is the map induced by f_n and if f_{n-1} is surjective, so is the map induced by f_{n-1}. Then we can show each row of the first snake diagram is exact by shifting indices from n to $n \pm 1$. Then by the Snake Lemma, it yields the exact sequence

$$H_n(\mathcal{C}) \xrightarrow{f_*} H_n(\mathcal{D}) \xrightarrow{g_*} H_n(\mathcal{E}) \xrightarrow{\partial_n} H_{n-1}(\mathcal{C}) \xrightarrow{f_*} H_{n-1}(\mathcal{D}) \xrightarrow{g_*} H_{n-1}(\mathcal{E}).$$

Doing this for each n, we can get a long exact sequence on homology

$$\cdots \longrightarrow H_{n+1}(\mathcal{E}) \xrightarrow{\partial_{n+1}} H_n(\mathcal{C}) \xrightarrow{f_*} H_n(\mathcal{D}) \xrightarrow{g_*} H_n(\mathcal{E}) \xrightarrow{\partial_n} H_{n-1}(\mathcal{C}) \longrightarrow \cdots .$$

□

By Theorem 6.2, we know that every short exact sequence of chain complexes implies a long exact sequence on homology. Here, we show that a long exact sequence on homology arising from mapping cone.

Definition 6.2. The mapping cone $\mathcal{C}.(f)$ of a morphism of chain complexes $f : \mathcal{A} \to \mathcal{B}$ is the complex $\mathcal{C}.(f)$ given by $C(f)_n = A_{n-1} \oplus B_n$ and differential $\partial : C(f)_n \to C(f)_{n-1}$, with

$$\partial = \begin{pmatrix} d & 0 \\ (-1)^{n-1}f & \delta \end{pmatrix}$$

where $d : A_n \to A_{n-1}$ and $\delta : B_n \to B_{n-1}$ are maps in the complexes, and $f_{n-1}d = \delta f_n$.

With the definition above, we can show that the differential ∂ is complex as following: Since

$$\begin{aligned}\partial\begin{pmatrix}A_{n-1}\\ B_n\end{pmatrix} &= \begin{pmatrix}d & 0\\ (-1)^{n-1}f & \delta\end{pmatrix}\begin{pmatrix}A_{n-1}\\ B_n\end{pmatrix}\\ &= \begin{pmatrix}dA_{n-1}\\ (-1)^{n-1}f(A_{n-1})+\delta(B_n)\end{pmatrix},\end{aligned}$$

then

$$\begin{aligned}\partial^2\begin{pmatrix}A_{n-1}\\ B_n\end{pmatrix} &= \begin{pmatrix}d & 0\\ (-1)^{n-1}f & \delta\end{pmatrix}\begin{pmatrix}dA_{n-1}\\ (-1)^{n-1}f(A_{n-1})+\delta(B_n)\end{pmatrix}\\ &= \begin{pmatrix}0\\ (-1)^{n-2}f(d(A_{n-1}))+(-1)^{n-1}\delta f(A_{n-1})\end{pmatrix}\\ &= \begin{pmatrix}0\\ 0\end{pmatrix}.\end{aligned}$$

We have a short sequence of complexes of the form

$$0\to\mathcal{B}\to\mathcal{C}.(f)\to\mathcal{A}[-1]\to 0$$

where $\mathcal{A}[-1]$ means $A[-1]_n = A_{n-1}$. The injection map $\mathcal{B}\to\mathcal{C}.(f)$ and the projection map $\mathcal{C}.(f)\to\mathcal{A}[-1]$ are given by the direct summands.

Then by Theorem 6.2, we get a long exact sequence

$$\cdots\to H_{n+1}(\mathcal{A}[-1])\to H_n(\mathcal{B})\to H_n(\mathcal{C}.(f))\to H_n(\mathcal{A}[-1])\to H_{n-1}(\mathcal{B})\to\cdots$$

where $H_n(\mathcal{A}[-1]) = H_{n-1}(\mathcal{A})$. Then we can rewrite the long exact sequence on homology as:

$$\cdots\to H_n(\mathcal{A})\to H_n(\mathcal{B})\to H_n(\mathcal{C}.(f))\to H_{n-1}(\mathcal{A})\to H_{n-1}(\mathcal{B})\to\cdots$$

7 Regular Sequences and Koszul Complex

Definition 7.1. An element a in R-module A is called a *zero divisor* on A, if there exists a nonzero element x in R such that $rx = xr = 0$. We write the zero divisors on A as $\mathcal{Z}(A)$.

Definition 7.2. Let R be any commutative ring, A be any R-module. The (ordered sequence of) elements $x_1,\ldots,x_n$ of R is said to be an *regular sequence* or an R-sequence on A if
(1) $(x_1,\ldots,x_n)A \neq A$
(2) For $i = 1,\ldots,n$, $x_i \notin \mathcal{Z}(A/(x_1,\ldots,x_{i-1})A)$.

Part (b) of the definition says that x_1 is not a zero-divisor on A, x_2 is not a zero-divisor on A/x_1A,..., x_n is not a zero-divisor on $A/(x_1,\ldots,x_{n-1})A$. Moreover, the case $A = R$ is of special importance. We then simply say that the sequence $x_1,\ldots,x_n$ is an R-sequence.

Theorem 7.1. *Let $x, y \in R$ be an regular sequence on the R, then $x \notin \mathcal{Z}(R/(y))$.*

Proof. Since x, y is a regular sequence on R, $x \notin \mathcal{Z}(R)$ and $y \notin \mathcal{Z}(R/(x))$. We suppose $t' \in R/(y)$ and $xt' = 0$ and want to show $t' = 0$. Pick any t in R mapping on t', then $xt \in yR$, say $xt = yu$. Since $y \notin \mathcal{Z}(R/(x))$, $u \in xR$, say $u = xu' \implies xt = xyu'$. Since $x \notin \mathcal{Z}(R)$, we can cancel x in the equation $xt = xyu'$ to get $t = yu' \in yR$. So $t' = 0$, which means $x \notin \mathcal{Z}(R/(y))$. □

Note that in general, if x, y, z is a regular sequence on R, z, y, x need not be a regular sequence on R. However, the statement holds in a local ring.

Definition 7.3. (R, m) is called a *local ring* if R is Noetherian and m is unique maximal ideal, that is m is all non-units in R.

Lemma 7.2. *Let (R, m) be a local ring. If x, y is regular on R, then y, x is regular on R.*

Proof. From Theorem 7.1, we know that $x \notin \mathcal{Z}(R/(x))$. Then we want to show $y \notin \mathcal{Z}(R)$. Suppose $ya = 0$ in R, want to show $a = 0$. Then $ya \equiv 0$ in $R/(x)$, which implies $a \equiv 0$ mod xR. Thus, $a \in xR$, say $a = xa_0$, we have $y(xa_0) = 0$, which is $x(ya_0) = 0$. Since $x \notin \mathcal{Z}(R)$, we get $ya_0 = 0$. We can repeat to get $a_0 = xa_1$, then $a = xa_0 = x^2a_1$, and so on. Thus inductively, for all n, there exists a_{n-1} such that $a = x^n a_{n-1} \in x^n R$, then by Krull Intersection Theorem, $a \in \bigcap_{n \geq 1} a^n R = 0$. Therefore, y, x is regular on R. □

Next, we want to introduce associated primes of R-module M and show $\operatorname{Ass}(M)$ is finite.

Definition 7.4. Let R be Noetherian, A be a finitely generated R-module and P be prime. P is called an *associated prime* if $P = (0 :_R a) = \{r \in R \mid ra = 0\} = Ann_R(a)$, for some non-zero $a \in A$. We say $P \in Ass(A)$ if and only if $P = (0 :_R a)$ for some $a \in R$-module A.

Proposition 7.3. *Suppose R is Noetherian and A is a R-module. Then any zero divisor on A is contained in an associated prime.*

Proof. Suppose $r \in R$ is a zero divisor on A, then $\exists\ a \neq 0$ such that $ra = 0$, which means $r \in (0 :_R a)$. Let $\mathcal{C} = \{(0 : ta) \mid t \in R\}$. Since R is Noetherian, let $P = (0 : t_0 a)$ be a maximal element in $\mathcal{C}$. If P is prime, it is an associated prime and $r \in (0 : a) \subseteq (0 : t_0 a) = P$. If not, suppose $x, y \in R$, $xy \in P$. If $x \notin P$, i.e. $xt_0 a \neq 0$, then $(0 : xt_0 a) \neq R$, then $P \subseteq (0 : xt_0 a)$. However, since P is maximal, $P = (0, xt_0 a)$, so $y \in P$, whcih means P is prime. Therefore, $r \in P$. □

Lemma 7.4. *Given a short exact sequence of R-modules*

$$0 \to M' \to M \to M'' \to 0$$

where M' is a submodule of M and $M'' = M/M'$, we have

$$Ass(M) \subseteq Ass(M') \cup Ass(M'').$$

Proof. Suppose $P \in Ass(M)$ and let $P = Ann_R(x)$ for some nonzero $x \in M$. If $x \in M'$, then $P \in Ass(M')$. Otherwise, the image $\overline{x}$ of x in M'' is nonzero and it is clear that $P \subseteq Ann_R(\overline{x})$. If this is an equality, then $P \in Ass(M'')$. So assume there is $a \in Ann_R(\overline{x}) \backslash P$. In this case, $ax \in M' \backslash \{0\}$, and the fact that P is prime implies the inclusion $Ann_R(x) \subseteq Ann_R(ax)$ is an equality. Thus, $P \in Ass(M')$. □

Proposition 7.5. *Suppose R is a Noetherian ring, M is a finitely generated R-module, then the following hold:*

(1) The set $Ass(M)$ is finite.

(2) If $M \neq 0$, then $Ass(M)$ is non-empty.

(3) The set of zero divisors of M equals to

$$\bigcup_{P \in Ass(M)} P$$

.

Proof. Let us consider the set $\mathcal{P}$ consisting of the ideals of R of the form $Ann_R(x)$ for some $x \in M \backslash \{0\}$. Since R is Noetherian, there is a maximal element $P \in \mathcal{P}$. We want to show P is a prime ideal so that $P \in Ass(M)$.

By assumption, let $P = Ann_R(x)$ for some $x \in M \backslash \{0\}$. Since $x \neq 0$, we have $P \neq R$. Suppose $b \in R \backslash P$, then $bx \neq 0$ and we have $Ann_R(x) \subseteq Ann_R(bx)$. By the maximality of P, we conclude that this is an equality, so for every $a \in R$ such that $ab \in P$, we have $a \in P$. Thus, $Ass(M)$ is non-empty. Moreover, we now know if M is nonzero, then we can find $x \in M \backslash \{0\}$ such that $Ann_R(x) = P_1$ is a prime ideal.

The map $R \to M$ with $a \to ax$ induces, thus we have an injection $R/P \to M$, so then we have a short exact sequence

$$0 \to M_1 \to M \to M/M_1 \to 0,$$

where $M_1 \cong R/p_1$. Since P_1 is a prime ideal in R, we have $Ass(R/P_1) = \{P_1\}$, and Lemma 7.4 implies

$$Ass(M) \subseteq Ass(M/M_1) \cup \{P_1\},$$

then it suffices to show $Ass(M/M_1)$ is finite.

If $M_1 \neq 0$, we can repeat this argument and find $M_1 \subseteq M_2$ such that $M_2/M_1 \cong R/P_2$ for some prime ideal P_2 in R. Since M is finitely generated as a Noetherian module, this process must terminate. So after finitely many steps, we conclude that $Ass(M)$ is finite. By definition, for every $P \in Ass(M)$, the ideal P is contained in the set of zero divisors of M.

On the other hand, if $a \in R$ is a zero divisor, then $a \in I$ for some $I \in \mathcal{P}$. If we choose a maximal P in $\mathcal{P}$ that contains I, then we have $P \in Ass(M)$. So a lies in the union of the associated primes of M. Thus, the set of zero divisors of M equals to

$$\bigcup_{P \in Ass(M)} P$$

□

Then we can give a definition of Koszul complex.

Definition 7.5. Given a ring R and $x_1, \ldots, x_n \in R$, we define a complex $\mathcal{K}.$ as follows: set $\mathcal{K}_0 = R$ and $\mathcal{K}_p = 0$ if p is not in the range $0 \leq p \leq n$.

We write for standard basis, using the symbols: $e_{i_1} \wedge e_{i_2} \wedge \cdots \wedge e_{i_p}$, for $1 \leq i_1 < \ldots < i_p \leq n$. For $1 \leq p \leq n$, we let $\mathcal{K}_p = \oplus R_{e_{i_1} \wedge e_{i_2} \wedge \cdots \wedge e_{i_p}}$ be the free R-module of rank $\binom{n}{p}$ with basis $e_{i_1} \wedge e_{i_2} \wedge \cdots \wedge e_{i_p}$.

The differential $f_p : \mathcal{K}_p \to \mathcal{K}_{p-1}$ is defined by setting

$$f_p(e_{i_1} \wedge e_{i_2} \wedge \cdots \wedge e_{i_p}) = \sum_{j=1}^{p} (-1)^{j-1} x_{i_j} e_{i_1} \wedge e_{i_2} \wedge \cdots \wedge \overline{e_{i_j}} \wedge \cdots \wedge e_{i_p}$$

where the superscript $\overline{e_{i_j}}$ means the term is omitted and for $p = 1$, set $f_p(e_i) = x_i$. This complex is called the Koszul complex, written as $\mathcal{K}.(x_1, \ldots, x_n)$ or $\mathcal{K}.(\underline{x})$.

To show f_p is indeed complex, we let

$$\begin{aligned}
&f_p \circ f_{p+1}(e_{i_1} \wedge e_{i_2} \wedge \cdots \wedge e_{i_{p+1}}) \\
=&f_p(\sum_{j=1}^{p+1} (-1)^{j-1} x_{i_j} e_{i_1} \wedge e_{i_2} \wedge \cdots \wedge \overline{e_{i_j}} \wedge \cdots \wedge e_{i_{p+1}}) \\
=&\sum_{j=1}^{p+1} (-1)^{j-1} x_{i_j} f_p(e_{i_1} \wedge e_{i_2} \wedge \cdots \wedge \overline{e_{i_j}} \wedge \cdots \wedge e_{i_{p+1}}) \\
=&\sum_{j=1}^{p+1} (-1)^{j-1} x_{i_j} (\sum_{k=1}^{j-1} (-1)^{k-1} x_{i_k} e_{i_1} \wedge \cdots \wedge \overline{e_{i_k}} \wedge \cdots \wedge \overline{e_{i_j}} \wedge \cdots \wedge e_{i_{p+1}} \\
+&\sum_{k=j+1}^{p+1} (-1)^{k} x_{i_k} e_{i_1} \wedge \cdots \wedge \overline{e_{i_j}} \wedge \cdots \wedge \overline{e_{i_k}} \wedge \cdots \wedge e_{i_{p+1}}) \\
=&\sum_{j=1}^{p+1} \sum_{k=1}^{j-1} (-1)^{k+j-2} x_{i_j} x_{i_k} e_{i_1} \wedge \cdots \wedge \overline{e_{i_k}} \wedge \cdots \wedge \overline{e_{i_j}} \wedge \cdots \wedge e_{i_{p+1}} \\
+&\sum_{j=1}^{p+1} \sum_{k=j+1}^{p+1} (-1)^{k+j-1} x_{i_j} x_{i_k} e_{i_1} \wedge \cdots \wedge \overline{e_{i_j}} \wedge \cdots \wedge \overline{e_{i_k}} \wedge \cdots \wedge e_{i_{p+1}}
\end{aligned}$$

Without loss of generality, assume $1 \le k_0 < j_0 \le p+1$, then we have

$$\begin{aligned}
&(-1)^{k_0+j_0-2} x_{i_{j_0}} x_{i_{k_0}} e_{i_1} \wedge \cdots \wedge \overline{e_{i_{k_0}}} \wedge \cdots \wedge \overline{e_{i_{j_0}}} \wedge \cdots \wedge e_{i_{p+1}} \\
+&(-1)^{k_0+j_0-1} x_{i_{j_0}} x_{i_{k_0}} e_{i_1} \wedge \cdots \wedge \overline{e_{i_{k_0}}} \wedge \cdots \wedge \overline{e_{i_{j_0}}} \wedge \cdots \wedge e_{i_{p+1}} = 0,
\end{aligned}$$

then by induction, we have $f_p \circ f_{p+1} = 0$.

Suppose we have the Koszul complex

$$0 \to \mathcal{K}_n \to \cdots \to \mathcal{K}_p \to \mathcal{K}_{p-1} \to \cdots \to \mathcal{K}_1 \to \mathcal{K}_0 \to 0$$

then $\mathcal{K}_p \cong R^{\binom{n}{p}}$, where a commutative ring R and elements $x_1, x_2, \ldots, x_n$ in R with the canonical basis $(e_{i_1}, e_{i_2}, \ldots, e_{i_n}) \in \mathbb{R}^n$.

For example, when $n = 3$, we have x_1, x_2, x_3 in R. Then $\mathcal{K}_1$ has the basis $\{e_1, e_2, e_3\}$, $\mathcal{K}_2$ has the basis $\left\{\begin{matrix} e_1 \wedge e_2 \\ e_1 \wedge e_3 \\ e_2 \wedge e_3 \end{matrix}\right\}$, and $\mathcal{K}_3$ has the basis $\{e_1 \wedge e_2 \wedge e_3\}$. In fact, for the basis of $\mathcal{K}_2$, we can have $e_1 \wedge e_2, e_1 \wedge e_3, e_2 \wedge e_3$ on different rows to get different basis. So

$f_1(e_1) = x_1, f_1(e_2) = x_2,\ f_1(e_3) = x_3 \implies A = (x_1 \quad x_2 \quad x_3)$.

$f_2(e_1 \wedge e_2) = x_1e_2 - x_2e_1 \implies \begin{pmatrix} -x_2 \\ x_1 \\ 0 \end{pmatrix}$

$f_2(e_1 \wedge e_3) = x_1e_3 - x_3e_1 \implies \begin{pmatrix} -x_3 \\ 0 \\ x_1 \end{pmatrix}$

$f_2(e_2 \wedge e_3) = x_2e_3 - x_3e_2 \implies \begin{pmatrix} 0 \\ -x_3 \\ x_2 \end{pmatrix}$

Thus the matrix we have is $B=\begin{pmatrix} -x_2 & -x_3 & 0 \\ x_1 & 0 & -x_3 \\ 0 & x_1 & x_2 \end{pmatrix}$.

$f_3(e_1 \wedge e_2 \wedge e_3) = x_1e_2 \wedge e_3 - x_2e_1 \wedge e_3 + x_3e_1 \wedge e_2 = \begin{pmatrix} x_3 \\ -x_2 \\ x_1 \end{pmatrix}$. Then we have the diagram:

$$\begin{tikzcd}
0 \arrow[r] & R \arrow[r, "\begin{pmatrix} x_3 \\ -x_2 \\ x_1 \end{pmatrix}"] \arrow[d] & R^3 \arrow[r, "B"] \arrow[d] & R^3 \arrow[r, "A"] \arrow[d] & R \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathcal{K}_3 \arrow[r, "f_3"'] & \mathcal{K}_2 \arrow[r, "f_2"'] & \mathcal{K}_1 \arrow[r, "f_1"'] & \mathcal{K}_0 \arrow[r] & 0
\end{tikzcd}$$

Since $f_1f_2 = (x_1 \quad x_2 \quad x_3)\begin{pmatrix} -x_2 & -x_3 & 0 \\ x_1 & 0 & -x_3 \\ 0 & x_1 & x_2 \end{pmatrix}=(0 \quad 0 \quad 0)$
and $f_2f_3 = \begin{pmatrix} -x_2 & -x_3 & 0 \\ x_1 & 0 & -x_3 \\ 0 & x_1 & x_2 \end{pmatrix}\begin{pmatrix} x_3 \\ -x_2 \\ x_1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$. Thus, this sequence is complex.

Theorem 7.6. *Let $\mathcal{K}.(x_1, \dots, x_n)$ be Koszul complex on a regular sequence $x_1, \dots, x_n$, then $\mathcal{K}.(x_1, \dots, x_n)$ is isomorphic to mapping cone of*

$$f : \mathcal{K}.(x_1, \dots, x_{n-1}) \xrightarrow{\cdot x_n} \mathcal{K}.(x_1, \dots, x_{n-1})$$

Proof. By definition of cone, we have $C(f)_n = K_{n-1}(x_1, \dots, x_{n-1}) \oplus K_n(x_1, \dots, x_{n-1})$. On one hand,

$$\partial_{C(f)}(0, e_1 \wedge \cdots \wedge e_{n-1}) = fe_1 \wedge \cdots \wedge e_{n-1} - \partial_{\mathcal{K}.(x_1,\dots,x_{n-1})}(e_1 \wedge \cdots \wedge e_{n-1})$$

On the other hand,

$$
\begin{aligned}
&\partial_{\mathcal{K}.(x_1,\ldots,x_n)}(0, e_1 \wedge \cdots \wedge e_{n-1}) \\
=&\sum_{i=0}^{n-1}(-1)^i x_i e_0 \wedge \cdots \wedge \overline{e_i} \wedge \cdots \wedge e_{n-1} \\
=&f e_1 \wedge \cdots \wedge e_{n-1} + \sum_{i=1}^{n-1}(-1)^i x_i e_0 \wedge \cdots \wedge \overline{e_i} \wedge \cdots \wedge e_{n-1} \\
=&f e_1 \wedge \cdots \wedge e_{n-1} - e_0(\sum_{i=1}^{n-1}(-1)^{i+1} x_i e_1 \wedge \cdots \wedge \overline{e_i} \wedge \cdots \wedge e_{n-1})
\end{aligned}
$$

which is the image of the result of the previous computation. □

With a long exact sequence on homology arising from mapping cone and Theorem 7.6, we want to show that the Koszul complex on a regular sequence is acyclic. Before showing the theorem, we need to know the definition of acyclic.

Definition 7.6. A chain complex $\mathcal{M}$ of the form

$$\mathcal{M} : 0 \to M_n \to \cdots \to M_p \to M_{p-1} \to \cdots \to M_1 \to M_0 \to 0$$

is called *acyclic* if $H_i(\mathcal{M}) = 0$ for each $i \neq 0$. In other words, $\mathcal{M}$ is acyclic if and only if it is exact everywhere except possibly at M_0.

Theorem 7.7. *Suppose $x_1, x_2, \ldots, x_n$ in a ring R is a regular sequence, then the Koszul complex on this regular sequence is acyclic.*

Proof. Suppose in a ring R, $x_1, \ldots, x_n$ is a regular sequence. We use induction on n. When $n = 1$, then we have $x_1 \in R$ be regular, so we have the map

$$f : \mathcal{K}. \xrightarrow{\cdot x_1} \mathcal{K}.$$

and the Koszul complex is

$$0 \to \mathcal{K}_1 \xrightarrow{\cdot x_1} \mathcal{K}_0 \to 0$$

Since x_1 is regular, the kernel of $\mathcal{K}_1$ is 0, which implies the Koszul complex is exact at $\mathcal{K}_1$, but not at $\mathcal{K}_0$.

When $n > 1$, assume the theorem holds for the case $n-1$. Suppose $x_1, \ldots, x_n$ is a regular sequence in R, let $\underline{x} = x_1, x_2, \ldots, x_{n-1}$ and $\underline{x}' = x_1, \ldots, x_n$, then we have the map

$$f : \mathcal{K}.(\underline{x}) \xrightarrow{\cdot x_n} \mathcal{K}.(\underline{x})$$

So by Theorem 7.6, $\mathcal{K}.(\underline{x}') \cong \mathcal{C}.(f)$. Thus, we have a long exact sequence on homology for $\mathcal{K}.(\underline{x}')$ and $\mathcal{K}.(\underline{x})$:

$$\cdots \to H_i(\mathcal{K}.(\underline{x})) \xrightarrow{\cdot x_n} H_i(\mathcal{K}.(\underline{x})) \to H_i(\mathcal{K}.(\underline{x}')) \to H_{i-1}(\mathcal{K}.(\underline{x})) \xrightarrow{\cdot x_n} H_{i-1}(\mathcal{K}.(\underline{x})) \to \cdots$$

By the assumption the theorem is true for the case $n-1$, we get $H_i(\mathcal{K}.) = 0$ for $0 < i \leq n-1$. And so in the long exact sequence above, we get $H_i(\mathcal{K}.) = 0$ for $0 < i \leq n$ by the exactness. Thus, Koszul complex on a regular sequence is acyclic. □

By Theorem 7.7, we know that if the Koszul complex is acyclic, then

$$\cdots \to \mathcal{K}_2 \to \mathcal{K}_1 \to R/I \to 0$$

gives a free resolution of R/I, and we will talk about free resolution on section 9.

8 Height and Dimension

Definition 8.1. In commutative algebra, the *Krull dimension* of a commutative ring R is the supremum of the lengths of all chains of prime ideals.

Definition 8.2. The dimension of a ring R, denoted by $\dim R$, is the maximum length n of a chain $P_0 \subset P_1 \subset \cdots \subset P_n$ of prime ideals of R.

Definition 8.3. The notion of height is defined for proper ideals in a commutative Noetherian ring R. The height of a proper prime ideal P, denoted by $\mathrm{ht}(P)$, of R is the maximum of the lengths n of the chains of prime ideals contained in P, i.e., $P_0 \subset P_1 \subset \cdots \subset P_n = P$. The height of any proper ideal I, denoted by $\mathrm{ht}(I)$, is the minimum of the heights of the prime ideals containing I.

To prove Kull's Principal Ideal Theorem, we need to define Artinian rings and state a theorem about the relation between Artinian and Noetherian.

Definition 8.4. An Artinian ring A is a ring that satisfies the descending chain condition on ideals.

Theorem 8.1. *Suppose (A, m) is Quasi-local, A is Artinian if and only if A is Noetherian and* $\dim A = 0$.

Theorem 8.2 (Krull's Principal Ideal Theorem)**.** *Suppose R is a Noetherian ring, $0 \neq a \in R$ and a is not a unit. If P is a minimal prime over aR, then* $\mathrm{ht}(P) \leq 1$.

Proof. Consider localize R at P, R_P is a local ring, then $\mathrm{ht}(P) = \mathrm{ht}(P_S)$, where $S = R \backslash P$. We can assume (R, P) is local.

If $\mathrm{ht}(P) = 0$, then we are done.

If $\mathrm{ht}(P) = 1$, then we are done.

Suppose $\mathrm{ht}(P) \geq 2$ and we want to find a contradiction. Assume there is $Q_0 \subset Q_1 \subset P$, a chain of prime ideals with $aR \subseteq P$. Then we can mod out Q_0 to get the chain $\overline{0} \subset \overline{Q_1} \subset \overline{P}$, which means $\mathrm{ht}(\overline{P}) \geq 2$. So we can assume R is an integral domain and have the chain of prime ideals $0 \subset Q \subset P$ with $aR \subseteq P$, and P is the only prime containing a.

Define $Q^{(n)} = \{r \in R | s \cdot r \in Q^n$, for some $s \notin Q\}$. Since R/aR has just one prime P/aR, $\dim(R/aR) = 0$ and R/aR is Noetherian. Then by Theorem 8.1, R/aR is Artinian. Therefore it follows that

$$\cdots \subseteq \frac{Q^{(n+1)} + aR}{aR} \subseteq \frac{Q^{(n)} + aR}{aR} \subseteq \cdots,$$

then there exists s such that $\dfrac{Q^{(s+1)}+aR}{aR}=\dfrac{Q^{(s)}+aR}{aR}$, so $Q^{(s+1)}+aR=Q^{(s)}+aR$, which means $Q^{(s)}\subseteq Q^{(s+1)}+aR$.

Let $x\in Q^{(s)}, y\in Q^{(s+1)}$, then $x=y+a\cdot r$, for $r\in R$. So $x-y=a\cdot r$, where $(x-y)\in Q^{(s)}$. There exists $t\notin Q$ with $t(x-y)\in Q^s$ and $a\notin Q$, so $r\in Q^{(s)}$. We have

$$\begin{aligned}
&x\in Q^{(s+1)}+a\cdot Q^{(s)}\\
\Rightarrow& Q^{(s)}\subseteq Q^{(s+1)}+a\cdot Q^{(s)}\\
\Rightarrow& Q^{(s)}= Q^{(s+1)}+a\cdot Q^{(s)}\\
\Rightarrow& \frac{Q^{(s)}}{Q^{(s+1)}}=\frac{Q^{(s+1)}+a\cdot Q^{(s)}}{Q^{(s+1)}}=a\cdot(\frac{Q^{(s)}}{Q^{(s+1)}})\\
\Rightarrow& \frac{Q^{(s)}}{Q^{(s+1)}}=0\quad\text{(Nakayama's Lemma)}\\
\Rightarrow& Q^{(s)}=Q^{(s+1)}
\end{aligned}$$

Then we want to find a contradiction. To see this, let $x\in Q^{(s)}$, then $\exists\ t\notin Q$ such that $t\cdot x\in Q^s$. Let $x_0\in Q^s$ such that $t\cdot x=x_0$, so we have $x=x_0/t$ in R_Q, which implies $Q^{(s)}\subset Q^s\cdot R_Q$. Then $Q^{(s+1)}\cdot R_Q=Q^{s+1}\cdot R_Q$, so $\forall\ n\geq s$, $Q^n\cdot R_Q=Q^s\cdot R_Q$, which implies that $\bigcap(Q^n\cdot R_Q)=Q^s\cdot R_Q\neq 0$. However, by the Kull's intersection theorem, in this local ring (R,Q), $\bigcap_{n\geq 1}Q^n=0$. Thus, $Q=0$, which is a contradiction. Therefore, $\mathrm{ht}(P)\leq 1$. □

9 Projective Modules, Projective Resolutions and Projective Dimension

Definition 9.1. An R-module P is *projective* if for every R-linear map $f:P\to N$ and every surjective R-linear map $g:M\to N$, there is a unique R-linear map $h:P\to M$ such that $f=g\circ h$, i.e. the following diagram commutes:

$$\begin{tikzcd} & P \arrow[dl, "h"'] \arrow[d, "f"] \\ M \arrow[r, "g"] & N \end{tikzcd}$$

Proposition 9.1. *Suppose R-module P is a projective module, then there exists an R-module Q such that $P\oplus Q$ is a free R-module, which also means P is the direct summand of a free R-module.*

Proof. Suppose P is a projective module and choose a surjection $\pi:F\to P$, where F is a free R-module. By the definition of a projective module, there is a map $i:P\to F$ satisfying $\pi\circ i=id_P$. So we have $F=ker(\pi)\oplus i(P)$. We name $Q=ker(\pi)$ and we have $i(P)=P$, then we can conclude that there exists an R-module Q such that $P\oplus Q$ is a free R-module. □

We need to note that if M' is a submodule of M, then we have a short exact sequence

$$0\to M'\to M\to M/M'\to 0$$

Moreover, up to an isomorphism, every short exact sequence is of the form:

$$\begin{tikzcd}
0 \arrow[r] & N \arrow[r, "f"] \arrow[d, "\cong"'] & M \arrow[r, "g"] \arrow[d, "="'] & K \arrow[r] \arrow[d, "\cong"'] & 0 \\
0 \arrow[r] & ker(g) \arrow[r] & M \arrow[r] & M/ker(g) \arrow[r] & 0
\end{tikzcd}$$

Proposition 9.2. *Let R be a ring and let*

$$0 \longrightarrow N \xrightarrow{f} M \xrightarrow{g} K \longrightarrow 0$$

be a short exact sequence of R-modules. The following conditions are equivalent:

(1)There exists a homomorphism $h : K \to M$ such that $g \circ h = id_K$.

(2)There exists a homomorphism $k : M \to N$ such that $k \circ f = id_N$.

If either condition holds, we say that the short exact sequence splits.

Proof. (1) $\Rightarrow$ (2) Let $h : K \to M$ such that $g \circ h = id_K$, then define a homomorphism $\phi : M \to M$ by $\phi = id_M - h \circ g$. We can think of ϕ as a projection onto N, in that ϕ maps M into the submodule N and it is the identity on N.

We claim that ϕ is a projection. Indeed, we have $g \circ \phi = g - g \circ h \circ g = g - id_K \circ g = 0$. Thus, by the universal property of the kernel, ϕ factors through the kernel $f : N \to M$, which means there is a unique map $k : M \to N$ such that $f \circ k = \phi$, i.e. the image of ϕ is contained in the image of f.

In addition, since $g \circ f = 0$, $f \circ k \circ f = \phi \circ f = f - h \circ g \circ f = f$. Thus, for all $n \in N$, $f(n) = f(k(f(n)))$. Since f is injective, $n = k(f(n))$, which means $k \circ f = id_N$.

(2) $\Rightarrow$ (1) Similarly, let $k : M \to N$ such that $k \circ f = id_N$, then define a homomorphism $\psi : M \to M$ by $\psi = id_M - f \circ k$. So $\psi \circ f = f - f \circ k \circ f = f - f \circ id_N = 0$, then ψ is also a projection. Thus, by the universal property of the kernel, ψ factors through the kernel $g : M \to K$, which means there is a unique map $h : K \to M$ such that $h \circ g = \psi$.

Since $g \circ f = 0$, $g \circ h \circ g = g \circ \psi = g - g \circ f \circ k = g$. Thus, for all $m \in M$, $g(m) = g(h(g(m)))$. Since g is surjective, for all $k \in K$, there exists $m \in M$ such that $g(m) = k$. Thus, we have $k = g(h(k))$, which means $g \circ h = id_K$. □

As a result of Proposition 9.2, suppose a short exact sequence $0 \to N \to M \to K \to 0$ splits, we have $M \cong N \oplus K$.

The following theorem tells us the relation between projective modules and short split exact sequences, and we are going to use the result of Proposition 9.2 for the proof of the theorem.

Theorem 9.3. *Let R be a ring with identity and let P be an R-module. P is a projective module if and only if every short exact sequence $0 \to N \to M \to P \to 0$ splits.*

Proof. ($\Rightarrow$) Let f denote the map from M to P in the given exact sequence. Since P is projective, there exists $h : P \to M$ such that $f \circ h : P \to P$ is the identity. This shows that h is injective and $im(h) \cap ker(f) = 0$. Also, every m in M can be written as

$$m = h(f(m)) + (m - h(f(m))) \in im(h) + ker(f)$$

so $M = im(h) \oplus ker(f) \cong P \oplus N$.

($\Leftarrow$) Suppose every short exact sequence $0 \to N \to M \to P \to 0$ splits. We claim that if P is a R-module, then there exists a projective module M such that $M \to P \to 0$. Indeed, let S be a set of generators of P. Let F_S be the free module generated by elements e_s for s in S. Then F_S is projective and $f : F_S \to P$ given by

$$f(\sum r_s e_s) = \sum r_s s$$

is surjective. Name $M = F_S$, so such a projective module Q exists. Let N be the kernel of the projection $M \to P \to 0$. Then the hypothesis implies that $M \cong P \oplus N$. Moreover, the diagram

$$\begin{array}{ccccc} & & P & & \\ & & \downarrow & & \\ M & \longrightarrow & L & \longrightarrow & 0 \end{array}$$

can be extended to a diagram

$$\begin{array}{ccccc} & & P \oplus N & & \\ & & \downarrow & & \\ M & \longrightarrow & L & \longrightarrow & 0 \end{array}$$

so N maps trivially to L. Since $M \cong P \oplus N$ is projective by the claim, there exists a map $h' : P \oplus N \to M$ making the diagram commutative. Now put h to be the restriction of h' to P. Thus, P is projective. $\square$

Corollary 9.4. *If R is a ring with identity, P is a projective R-module and $f : M \to P$ is a surjective map of R-modules, then $M \cong P \oplus ker(f)$.*

Proof. Suppose P is projective. We have a short exact sequence

$$0 \longrightarrow ker(f) \longrightarrow M \xrightarrow{f} P \longrightarrow 0$$

which splits by Theorem 9.3. So $M \cong P \oplus ker(f)$. $\square$

Proposition 9.5. *Suppose (R, m) is local, P is finitely generated and projective, then P is free.*

Proof. Suppose P is a finitely generated R-module, then let $\{p_1, \dots, p_n\}$ be a minimal system of generators of P. Then define a surjective map $\psi : R^n \to P$ by $(x_1, \dots, x_n) \to \sum_{i=1}^n x_i p_i$, where $x_i \in R^n$. Since P is projective, by Corollary 9.4, we get $R^n \cong P \oplus ker(\psi)$. Let $ker(\psi) = O$, we have $R^n \cong P \oplus O$.

Then we want to show $O = 0$. We first multiply m to $R^n \cong P \oplus O$, then we get $mR^n \cong mP \oplus mO$. We can mod out $R^n \cong P \oplus O$ by $mR^n \cong mP \oplus mO$ to get

$$R^n/mR^n \cong P/mP \oplus O/mO$$

Moreover, $P/mP, O/mO$ are vector spaces over the field R/m and the dimension of P is n, so by comparing the dimension, we get $O/mO = 0$. Then by Nakayama's Lemma, we get $O = 0$. Thus, $P \cong R^n$, which means P is free. $\square$

Proposition 9.6. *Suppose R is a Noetherian ring and P is a finitely generated R-module. P is a projective R-module if and only if P_Q is a free R_Q-module for all primes ideals $Q \subseteq R$.*

Proof. Suppose P is projective, then P_Q is projective over the local ring R_Q and so is free by Proposition 9.5.

For the converse, we use the fact that when R is Noetherian, and M, N are finitely generated R-modules, then $Hom_R(M,N)_S \cong Hom_{R_S}(M_S, N_S)$ for all multiplicatively closed sets S. Take a short exact sequence

$$0 \longrightarrow K \longrightarrow F \xrightarrow{\pi} P \longrightarrow 0$$

of R-modules, with F finitely generated and free. Since R is Noetherian, K is also finitely generated. We have an induced exact sequence

$$0 \longrightarrow Hom_R(P,K) \longrightarrow Hom_R(P,F) \xrightarrow{\pi^*} Hom_R(P,P)$$

If we show that π^* is surjective, then there exists $h \in Hom(P,F)$ such that $\pi^*(h) = id_P$. This means $h \circ \pi = id_P$, so the sequence splits, and therefore P is a summand of F, by Proposition 9.2. Thus, P is projective.

To see that π^* is surjective, it suffices to show that $(\pi^*)_Q$ is surjective for all prime ideals Q. Then we take Q a prime ideal in R. By hypothesis, P_Q is projective, so the sequence

$$0 \longrightarrow K_Q \longrightarrow F_Q \xrightarrow{\pi} P_Q \longrightarrow 0$$

splits. Thus,

$$0 \longrightarrow Hom_{R_Q}(P_Q,K_Q) \longrightarrow Hom_{R_Q}(P_Q,F_Q) \xrightarrow{\pi_Q^*} Hom_{R_Q}(P_Q,P_Q) \longrightarrow 0$$

is exact. Therefore,

$$0 \longrightarrow Hom_R(P,K)_Q \longrightarrow Hom_R(P,F)_Q \xrightarrow{\pi_Q^*} Hom_R(P,P)_Q \longrightarrow 0$$

is exact. Thus, π_Q^* is surjective. □

Let R be a Noetherian local ring with maximal ideal m, then we will give the definition of projective resolution and projective dimension.

Definition 9.2. Given an R-module M, an exact sequence

$$\mathcal{F} : \cdots \longrightarrow F_n \xrightarrow{\phi_n} \cdots \longrightarrow F_2 \xrightarrow{\phi_2} F_1 \xrightarrow{\phi_1} F_0 \xrightarrow{\pi} M \longrightarrow 0$$

is called a *projective resolution* if all of the F_i are projective.

Definition 9.3. Suppose M has a finite projective resolution, the minimal length among all finite projective resolutions of M is called its *projective dimension* and denoted $\mathrm{pd}_R(M)$. If M does not admit a finite projective resolution, then by convention the projective dimension is said to be infinite.

To prove the following proposition, we need to know the definition of free resolutions, and then minimal free resolution.

Definition 9.4. A *free resolution* of a R-module M is a complex

$$\mathcal{F} : \cdots \longrightarrow F_i \longrightarrow F_{i-1} \longrightarrow \cdots \longrightarrow F_1 \longrightarrow F_0 \longrightarrow M \longrightarrow 0$$

with trivial homology such that coker$(F_1 \to F_0 \cong M)$ and such F_i is a free R-module.

Definition 9.5. A complex

$$\mathcal{F} : \cdots \longrightarrow F_i \longrightarrow F_{i-1} \longrightarrow \cdots$$

over a local ring (R, m) is *minimal* if $im(F_i \to F_{i-1}) \subset (mF_{i-1})$.

In addition, to prove the following proposition we need the fact that *if two out of three modules in a short exact sequence have finite projective dimension, the third does as well.*

Proposition 9.7. *Let R be local with maximal ideal m, and let x be a non-zero-divisor in R that is not contained in m^2. Write $\overline{R} = R/(x)$. Let A be a finitely generated R-module annihilated by x (thereby an $\overline{R}$-module). If $pd_R(A) < \infty$, then $pd_{\overline{R}}(A) < \infty$.*

Proof. Let

$$0 \longrightarrow K^* \longrightarrow F^* \longrightarrow A \longrightarrow 0$$

be the start of a minimal free resolution of A over $\overline{R}$. Since $F^* = F/xF$, for an appropriate free R-module F, $pd_R(F^*) = 1$, and in particular, it is finite. Since $pd_R(A)$ is finite, this forces $pd_R(K^*)$ to be finite, since if two out of three modules in a short exact sequence have finite projective dimension, the third does as well. By induction of projective dimension over R, K^* has finite projective dimension over $\overline{R}$. Thus, A has finite projective dimension over $\overline{R}$, by the reasoning just employed. So, this reduces the problem to the case that $pd_R(A) = 1$.

So if $pd_R(A) = 1$, we take a minimal free resolution

$$0 \longrightarrow K \longrightarrow F \longrightarrow A \longrightarrow 0$$

over R, where K and F are free R-modules, and the column vectors in F generating K have entries in m. Note that if we invert(localize) x, then $A_x = 0$, which means $K_x = F_x$, and this implies that K and F are free R-modules of the same rank.

Assume $F = R^n$. We take $v_1, \ldots, v_n$ in F that form a basis for K. Since the resolution is minimal, the entries of the v_i are in m. Let $e_1, \ldots, e_n$ denote the standard basis for R^n. Then since x annihilates A, each xe_i is in K. Thus, we can write $xe_1 = r_1v_1 + \cdots + r_nv_n$ for all $r_i \in R$. Now some r_i is not in m, otherwise, x is in m^2, contrary to the assumption. Without loss of generality, let r_1 be a unit. Then we can write v_1 in terms of $xe_1, v_2, \ldots, v_n$, so that $xe_1, v_2, \ldots, v_n$ generate K, and hence for a basis for K.

Now write $xe_2 = s_1(xe_1) + s_2v_2 + \cdots + s_nv_n$, where $s_i \in R$. Then since x is not in m^2, one of $s_2, \ldots, s_n$ must not be in m. Also note that we do not need to consider s_1. Then without loss of generality, let s_2 be a unit. This will give that $xe_1, xe_2, v_3, \ldots, v_n$ generate K. Continuing on this process, we end up with $xe_1, \ldots, xe_n$ is a basis for K, and

$$A = F/K = F/(xF),$$

showing that A is free over $\overline{R}$. Thus, $pd_{\overline{R}}(A) < \infty$. $\square$

10 Tensor product, Tor and Torsion

Definition 10.1. Let M, N and L be R-modules.
1. A function $f : M \times N \to L$ is said to be *bilinear* if it satisfies the following conditions:
(a) $f(m_1 + m_2, n) = f(m_1, n) + f(m_2, n)$, $\forall\ m_1, m_2 \in M$ and $n \in N$.
(b) $f(m, n_1 + n_2) = f(m, n_1) + f(m, n_2)$, $\forall\ m \in M$ and $n_1, n_2 \in N$.
(c) $r \cdot f(m, n) = f(rm, n) = f(m, rn)$, $\forall\ m \in M$ and $n \in N$.

2. We say that a *tensor product* for M and N is an R-module P together with a bilinear function $h : M \times N \to P$ satisfying the following condition:

Given an R-module L and a bilinear function $f : M \times N \to L$, there exists unique R-module homomorphism $\phi : P \to L$ such that $\phi \circ h = f$. In other words, any diagram

$$\begin{tikzcd} M \times N \arrow[r, "h"] \arrow[d, "f"] & P \arrow[dl, "\phi"] \\ L & \end{tikzcd}$$

with f bilinear, can be completed with a unique R-module map $\phi : P \to L$.

Proposition 10.1. *Let M and N be R-modules. Then the tensor product of M and N exists and is unique (up to isomorphism).*

Proof. Let $\mathcal{F}$ denote the free-module on the set $\{(m,n)\}_{(m,n) \in M \times N}$. Let $\mathcal{K}$ denote the submodule of $\mathcal{F}$ generated by all expressions of the form:
(1) $(m_1 + m_2, n) - (m_1, n) - (m_2, n)$
(2) $(m, n_1 + n_2) - (m, n_1) - (m, n_2)$
(3) $r \cdot (m, n) - (rm, n)$
(4) $r \cdot (m, n) - (m, rn)$

We set $P := \mathcal{F}/\mathcal{K}$ and let $h : M \times N \to P$ be the function taking (m, n) to $(m, n) + \mathcal{K}$, for all $(m, n) \in M \times N$. In other words, h is just the inclusion of the basis for $\mathcal{F}$ into $\mathcal{F}$ followed by the canonical projection onto the quotient $\mathcal{F}/\mathcal{K}$. The function h is bilinear, by definition. Let L be any R-module and $f : M \times N \to L$ any bilinear function. Since $\mathcal{F}$ is a free module, we can define a map $\psi : \mathcal{F} \to L$ by sending each basis element $(m, n) \in \mathcal{F}$ to $f((m, n))$ and extending linearly to all of $\mathcal{F}$.

Since f is bilinear, $\mathcal{K} \subseteq ker(\psi)$. Thus, we obtain an induced map $\psi : \mathcal{F}/\mathcal{K} \to L$ which sends each $(m, n) + \mathcal{K}$ to $f((m, n))$. In other words, ϕ is an $R-$module homomorphism satisfying $\phi \circ h = f$. Clearly, ϕ is the only R-module homomorphism having this property. Now suppose that T is an R-module and $\zeta : M \times N \to T$ is a bilinear function satisfying the requirement of a tensor product. Then, first thinking of P as a tensor product, we may complete the diagram.

$$\begin{tikzcd} M \times N \arrow[r, "h"] \arrow[d, "k"] & P \arrow[dl, "\phi"] \\ T & \end{tikzcd}$$

with an R-module map $\phi : P \to T$ satisfying $\phi \circ h = k$. Interchanging the roles of P and T, we get an R-module map $\psi : T \to P$ satisfying $\psi \circ k = h$, then we get a diagram

$$\begin{tikzcd} M \times N \arrow[r, "h"] \arrow[d, "h"] & P \\ P \arrow[ur, "\psi"] & \end{tikzcd}$$

which can be completed by $\psi \circ \phi$. But 1_P also completes the diagram, so $\psi \circ \phi = 1_P$. Similarly, $\phi \circ \psi = 1_T$, so ϕ is an isomorphism with inverse ψ. In particular, P is unique up to isomorphism and h is unique, up to composition with an isomorphism. □

Now that the tensor product of modules M and N exists and is unique, we write $M \otimes_R N$ for tensor product. We also write $m \otimes n$ for the coset $(m, n) + \mathcal{K}$, $\forall\ (m, n) \in M \times N$. Every element in the tensor product can be written in the form $r_1(m_1 \otimes n_1) + \cdots + r_k(m_k \otimes n_k)$, for some $r_i \in R, m_i \in M, n_i \in N$.

Proposition 10.2. *The tensor product satisfies the following properties with regard to R-modules:*
1. $M \otimes_R N \cong N \otimes_R M$.
2. *If F is free with basis $\{v_\alpha\}$ and G is free with basis $\{w_\beta\}$, then $F \otimes_R G$ is free with basis $\{v_\alpha \otimes w_\beta\}$.*
3. *If $f : M \to M'$ and $g : N \to N'$ are R-module maps, then $\exists!$ R-module map*

$$f \otimes g : M \otimes_R N \to M' \otimes_R N'$$

satisfying $(f \otimes g)(m \otimes n) = f(m) \otimes g(n)$, $\forall\ m \otimes n \in M \otimes_R N$.

Proof. **1.** Let $h : M \times N \to M \otimes_R N$ be the bilinear map given in the definition of tensor product and $f : M \times N \to N \otimes M$ be the bilinear map taking the pair (m, n) to $n \otimes m$. Then we may complete the diagram

$$\begin{tikzcd} M \times N \arrow[r, "h"] \arrow[d, "f"] & M \otimes_R N \arrow[dl, "\phi"] \\ N \otimes_R M & \end{tikzcd}$$

with a unique R-module map $\phi : M \otimes_R N \to N \otimes_R M$ satisfying $\phi \circ h = f$. In particular, $\phi(m \otimes N) = n \otimes m$, $\forall\ m \otimes n \in M \otimes_R N$.

Similarly, $\exists!\ \psi : N \otimes_R M \to M \otimes_R N$ satisfying $\psi(n \otimes m) = m \otimes n$, $\forall\ n \otimes m \in N \otimes_R M$. Thus, $\psi \circ \phi$ completes the diagram

$$\begin{tikzcd} M \times N \arrow[r, "h"] \arrow[d, "h"] & M \otimes_R N \arrow[dl, "\psi\circ\phi"] \\ M \otimes_R N & \end{tikzcd}$$

Since $1_{M\otimes_R N}$ also completes the diagram, $\psi \circ \phi = 1_{M\otimes_R N}$. Similarly, $\phi \circ \psi = 1_{N\otimes_R M}$, so $M \otimes_R N \cong N \otimes_R M$.

2. We note that the elements $\{v_\alpha \otimes w_\beta\}$ clearly span $F \otimes_R G$. Suppose we have a dependence relation

$$r_1(v_{\alpha_1} \otimes w_{\beta_1}) + \cdots + r_n(v_{\alpha_n} \otimes w_{\beta_n}) = 0$$

Let $\mathcal{F}$ be the free module on the elements $(v_\alpha, w_\beta) \in F \times G$ and let $f : F \times G \to \mathcal{F}$ be the map extending the canonical inclusion of the basis (v_α, w_β) into $\mathcal{F}$. Then f is bilinear, so there exists $\phi : F \otimes_R G \to \mathcal{F}$ satisfying $\phi \circ h = f$. If we apply ϕ to the dependence relation above, since ϕ applied to the element $v_\alpha \otimes w_\beta$ are basis elements in $\mathcal{F}$, we deduce that each $r_i = 0$. Thus, $\{v_\alpha \otimes w_\beta\}$ forms a basis for $F \otimes_R G$.

3. Let $h : M \times N \to M \otimes_R N$ be the given map and $k : M \times N \to M' \otimes_R N'$ be the bilinear function which takes (m, n) to $f(m) \otimes g(n)$. Then there exists unique R-linear map $f \otimes g : M \otimes_R N \to M' \otimes_R N'$, satisfying $(f \otimes g) \circ h = k$.

In other words, $(f \otimes g)(m \otimes n) = f(m) \otimes g(n)$, $\forall\ m \otimes n \in M \otimes_R N$. □

Proposition 10.3. *Let*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

be a short exact sequence of R-modules. For any R-modules D:

$$A \otimes_R D \xrightarrow{f\otimes 1_D} B \otimes_R D \xrightarrow{g\otimes 1_D} C \otimes_R D \longrightarrow 0$$

is exact.

Proof. We note that $g\otimes 1_D$ is clearly onto and $g\otimes 1_D \circ f\otimes 1_D = (g\circ f)\otimes 1_D = 0$, since $g\circ f = 0$. We need to see that $ker(g\otimes 1_D) \subseteq im(f\otimes 1_D)$. For this, let $\phi : B\otimes_R D/im(f\otimes 1_D) \to C\otimes_R D$ be the map induced by $g \otimes 1_D$.

If we show ϕ is one-to-one, then $ker(f \otimes 1_D) = im(f \otimes 1_D)$, since $ker(g \otimes 1_D)/im(g \otimes 1_D)$ clearly belongs to the kernel of ϕ. For this, we let $h : C \times D \to C \otimes_R D$ be the given map and $k : C \times D \to B \otimes D/im(f \otimes 1_D)$ be the bilinear map, which takes (c, d) to the class of $b \otimes d \in B \otimes_R D/im(f \otimes 1_D)$, where $b \in B$ is any element satisfying $g(b) = c$.

If we show k is well-defined, then $\exists$ an R-linear map $\psi : C \otimes_R D \to B \otimes_R D/im(f \otimes 1_D)$ which satisfies $\psi \circ h = k$. In other words, $\psi(c \otimes d) = [b \otimes d]$.

But if we start with $[b\otimes d] \in B\otimes_R D/im(f\otimes 1_D)$, and apply $\psi\circ\phi$, we get back to $[b\otimes d]$, since $\psi(c \otimes d) = [b \otimes d]$. This implies that ϕ is one-to-one.

To see k is well-defined, suppose $g(b') = c$. Then $b - b' \in ker(g) = im(f)$, so $b - b' = f(a)$ for some $a \in A$. Thus, $[b \otimes d] = [(b' + f(a)) \otimes d] = [b' \otimes d] + [f(a) \otimes d] = [b' \otimes d]$ in $B \otimes_R D/im(f \otimes 1_D)$, so k is well-defined. □

Definition 10.2. (1) A commutative diagram $\mathcal{A}$

$$\begin{tikzcd}
 & \vdots & \vdots & \vdots & \\
\cdots \arrow[r] & A_{i,j} \arrow[u] \arrow[r, "\delta"] & A_{i,j-1} \arrow[u] \arrow[r, "\delta"] & A_{i,j-2} \arrow[u] \arrow[r] & \cdots \\
\cdots \arrow[r] & A_{i+1,j} \arrow[u, "d"'] \arrow[r, "\delta"'] & A_{i+1,j-1} \arrow[u, "d"'] \arrow[r, "\delta"'] & A_{i+1,j-2} \arrow[u, "d"'] \arrow[r] & \cdots \\
 & \vdots \arrow[u] & \vdots \arrow[u] & \vdots \arrow[u] &
\end{tikzcd}$$

of R-modules and R-module maps is a *double complex* if each row and column form a complex.

(2) Let $\mathcal{A}$ as above be a double complex. Associated to $\mathcal{A}$ is a complex $\mathcal{T}$, the so-called *total complex* of $\mathcal{A}$. For $n \in \mathbb{Z}$, the n^{th} module in $\mathcal{T}$ is the module $T_n = \oplus_{i+j=n} A_{ij}$ and the n^{th} *boundary map* (*differential*) $\partial : T_n \to T_{n-1}$ is the R-module map defined by the equation $\partial(a_{ij}) = \delta(a_{ij}) + (-1)^j d(a_{ij})$, $\forall\ a_{ij} \in A_{ij}$ satisfying $i + j = n$. Note that $\delta(a_{ij}) \in A_{i,j-1}$ and $d(a_{ij}) \in A_{i-1,j}$, so ∂ indeed takes values in T_{n-1}.

Also, since $\partial(a_{ij}) = \delta(a_{ij}) + (-1)^j d(a_{ij})$,

$$\begin{aligned}
\partial^2(a_{ij}) &= \partial(\delta(a_{ij}) + (-1)^j d(a_{ij})) \\
&= \delta(\partial(a_{ij})) + (-1)^j d(\partial(a_{ij})) \\
&= \delta(\delta(a_{ij}) + (-1)^j d(a_{ij})) + (-1)^j d(\delta(a_{ij}) + (-1)^j d(a_{ij})) \\
&= \delta^2(a_{ij}) + (-1)^j \delta d(a_{ij}) + (-1)^j d\delta(a_{ij}) + d^2(a_{ij}) \\
&= 0
\end{aligned}$$

so $\mathcal{T}$ is a complex.

We can give an example about double complex: let $\mathcal{A}$: $\cdots \longrightarrow A_n \xrightarrow{d} A_{n-1} \longrightarrow \cdots$ and $\mathcal{B}$: $\cdots \longrightarrow B_m \xrightarrow{\delta} B_{m-1} \longrightarrow \cdots$ be complexes. We obtain a double complex:

$$\begin{tikzcd}
 & \vdots & \vdots & \\
\cdots \arrow[r] & A_n \otimes_R B_{m+1} \arrow[u] \arrow[r, "1_{\mathcal{A}}\otimes\delta"] & A_n \otimes_R B_m \arrow[u] \arrow[r] & \cdots \\
\cdots \arrow[r] & A_{n+1} \otimes_R B_{m+1} \arrow[u, "d\otimes 1_{\mathcal{B}}"'] \arrow[r, "1_{\mathcal{A}}\otimes\delta"'] & A_{n+1} \otimes_R B_m \arrow[u, "d\otimes 1_{\mathcal{B}}"'] \arrow[r] & \cdots \\
 & \vdots \arrow[u] & \vdots \arrow[u] &
\end{tikzcd}$$

whose total complex is by definition $\mathcal{A} \otimes_R \mathcal{B}$. In other words, $\mathcal{A} \otimes_R \mathcal{B}$ is the complex whose k^{th} module is $\oplus_{i+j=k} A_i \otimes_R B_j$ and whose k^{th} differential satisfies

$$\partial(a_i \otimes b_j) = a_i \otimes \delta(b_j) + (-1)^j d(a_i) \otimes b_j$$

We note that following from the previous proposition for R-modules A and B, we calculate $Tor_n^R(A, B)$ as follows: Let $\mathcal{P}_A$ denote a projective resolution of A, with A deleted. Tensor $\mathcal{P}_A$ with B and take homology as following:

Definition-Theorem If A and B are R-modules with deleted projective resolutions $\mathcal{P}_A$ and $\mathcal{P}_B$, then $Tor_n^R(A, B)$ is the n^{th} homology of the complex $\mathcal{P}_A \otimes_R \mathcal{P}_B$, $\forall\ n \geq 0$.

Proposition 10.4. *Let A and B be R-modules. Write $\mathcal{P}_A$ for a deleted projective resolution of A, $\mathcal{P}_B$ for a deleted projective resolution of B. Then*

$$H_n(\mathcal{P}_A \otimes_R B) \cong H_n(\mathcal{P}_A \otimes_R \mathcal{P}_B) \cong H_n(A \otimes_R \mathcal{P}_B),$$

for all $n \geq 0$. In particular, $Tor_n^R(A, B) \cong H_n(\mathcal{P}_A \otimes_R \mathcal{P}_B)$.

Proof. Let $\mathcal{D}$ denote the double complex whose $(i, j)^{th}$ module is $P_i \otimes_R P'_j$, where P_i is the i^{th} term in $\mathcal{P}_A$ and P'_j is the j^{th} term in $\mathcal{P}_B$. Thus, $\mathcal{P}_A \otimes_R \mathcal{P}_B$ is the total complex associated to $\mathcal{D}$. Let $\mathcal{C}$ denote the double complex obtained from $\mathcal{D}$ by adding the complex $A \otimes_R \mathcal{P}_B$ above the 0^{th} row. Thus, $A \otimes_R \mathcal{P}_B$ is the -1^{st} row of $\mathcal{C}$. Note that this is consistent with the view that A is the -1^{st} term in the complex $\mathcal{P}_A \to A \to 0$. Thus, $\mathcal{C}$ is the double complex

$$\begin{tikzcd}
 & 0 & 0 & 0 & \\
\cdots \arrow[r] & A \otimes_R P'_2 \arrow[r] \arrow[u] & A \otimes_R P'_1 \arrow[r] \arrow[u] & A \otimes_R P'_0 \arrow[r] \arrow[u] & \cdots \\
\cdots \arrow[r] & P_0 \otimes_R P'_2 \arrow[r, "\delta"'] \arrow[u, "d"'] & P_0 \otimes_R P'_1 \arrow[r, "\delta"'] \arrow[u, "d"'] & P_0 \otimes_R P'_0 \arrow[r] \arrow[u, "d"'] & \cdots \\
\cdots \arrow[r] & P_1 \otimes_R P'_2 \arrow[r, "\delta"'] \arrow[u, "d"'] & P_1 \otimes_R P'_1 \arrow[r, "\delta"'] \arrow[u, "d"'] & P_1 \otimes_R P'_0 \arrow[r] \arrow[u, "d"'] & \cdots \\
 & \vdots \arrow[u] & \vdots \arrow[u] & \vdots \arrow[u] &
\end{tikzcd}$$

Write $\mathcal{T}$ for the total complex associated to $\mathcal{C}$. $\forall\ n \geq -1$, we have short exact sequences

$$0 \longrightarrow A \otimes_R P'_{n+1} \longrightarrow T_n \longrightarrow (\mathcal{P}_A \otimes_R \mathcal{P}_B)_n \longrightarrow 0$$

whose maps are given by inclusion and projection. It is straight forward to check that the inclusion and projection maps commute with the appropriate boundary maps, so these sequences fit together into an exact sequence of complexes

$$0 \longrightarrow (A \otimes_R \mathcal{P}_B)(1) \longrightarrow \mathcal{T} \longrightarrow \mathcal{P}_A \otimes_R \mathcal{P}_B \longrightarrow 0$$

We therefore get a long exact sequence on homology

$$\cdots \longrightarrow H_n(\mathcal{T}) \longrightarrow H_n(\mathcal{P}_A \otimes_R \mathcal{P}_B) \longrightarrow H_{n-1}((A \otimes_R \mathcal{P}_B)(1)) \longrightarrow H_{n-1}(\mathcal{T}) \longrightarrow \cdots .$$

However, all columns of $\mathcal{C}$ are exact, so $H_n(\mathcal{T}) = 0$, $\forall\ n \geq 0$. Thus,

$$H_n(\mathcal{P}_A \otimes_R \mathcal{P}_B) \cong H_{n-1}((A \otimes_R \mathcal{P}_B)(1)) = H_n(A \otimes_R \mathcal{P}_B) \quad \forall n \geq 0.$$

Similarly, we can prove $H_n(\mathcal{P}_A \otimes_R \mathcal{P}_B) \cong H_{n-1}((\mathcal{P}_A \otimes_R B)(1)) = H_n(\mathcal{P}_A \otimes_R B) \quad \forall n \geq 0$. Therefore, $H_n(A \otimes_R \mathcal{P}_B) \cong H_n(\mathcal{P}_A \otimes_R \mathcal{P}_B) \cong H_n(\mathcal{P}_A \otimes_R B)$, $\forall\ n \geq 0$. □

From Proposition 10.4, we may calculate $Tor_n^R(A, B)$ by taking the homology of the complex $\mathcal{P}_A \otimes_R B$ or the homology of the complex $A \otimes_R \mathcal{P}_B$.

Theorem 10.5. *$Tor_n^R(A, B) \cong Tor_n^R(B, A)$, for R-modules A and B with all $n \geq 0$.*

Proof. Follow from the previous proposition. □

We can use Tor to show that a finitely generated R-module M has a finite minimal free resolution in a local ring R.

Proposition 10.6. *Suppose (R, m) is local, M is finitely generated, $pd_R(M) < \infty$, then M has a finite minimal free resolution.*

Proof. Since $pd_R(M) < \infty$, $\mathrm{Tor}_i(k, M) = 0$, for all $i > n$ with $\mathrm{pd}_R(M) = n$. Now compute $\mathrm{Tor}_i(k, M)$, using a minimal free resolution

$$\cdots \longrightarrow F_{i+1} \xrightarrow{\phi_{i+1}} F_i \xrightarrow{\phi_i} F_{i-1} \xrightarrow{\phi_{i-1}} \cdots \longrightarrow F_n \longrightarrow \cdots \longrightarrow F_0 \longrightarrow M \longrightarrow 0$$

Tensor with $k = R/m$ to get an exact sequence

$$\cdots \longrightarrow F_{i+1}/mF_{i+1} \xrightarrow{\overline{\phi}_{i+1}} F_i/mF_i \xrightarrow{\overline{\phi}_i} F_{i-1}/mF_{i-1} \longrightarrow \cdots$$

Since ϕ_i and ϕ_{i+1} have entries in m, $\overline{\phi}_i = \overline{\phi}_{i+1} = 0$, for $i > n$. We have $ker(\overline{\phi}_i) = F_i/mF_i$ and $im(\overline{\phi}_{i+1}) = 0$. $0 = \mathrm{Tor}_i(k, M) = ker(\overline{\phi}_i)/im(\overline{\phi}_{i+1})$ for $i > n$, which implies $F_i/(mF_i) = 0$, then $F_i = mF_i$, which implies $F_i = 0$ by Nakayama's lemma. Therefore, the minimal free resolution is finite. □

11 Regular Local Rings

Recall that (Kull's Principal Ideal Theorem) Suppose R is Noetherian, if I is an ideal of R with $I = (x_1, \ldots, x_n)R$ and P is a minimal prime over I, then $\mathrm{ht}(P) \leq n$.

Consider R is a Noetherian local ring with the maximal ideal m, written as (R, m), and $\dim(R) = d$, then by the Kull's Principal Ideal Theorem, we have that the number of generators of m is greater than or equal to $d = \mathrm{ht}(m)$.

Definition 11.1. R is a regular local ring if d is the minimal number of generators of m.

Recall that (Nakayama's Lemma) If M is a finitely-generated R-module and the images of $m_1, \ldots, m_n$ of M in $M/J(R)M$ generate $M/J(R)M$ as an R-module, then $m_1, \ldots, m_n$ also generate M as an R-module.

For any local ring (R, m), $x_1, \ldots, x_n$ is a minimal generating set for m if and only if $\overline{x}_1, \ldots, \overline{x}_n$ is a basis in a vector space m/m^2 over the field R/m, by Nakayama's Lemma.

In general, if $x \in m/m^2$, then:
(1) x is part of a minimal generating set for m since $\overline{x}$ is part of a basis for m/m^2.
(2) The minimal number of generators of m/xR is one less than the minimal number of generators for m, since if $\{x, x_2, \ldots, x_n\}$ is the minimal generating set for m, then $\{\overline{x}, \overline{x}_2, \ldots, \overline{x}_n\}$ is a basis for m/m^2.

To prove the following proposition, we need to use the fact of *The Prime Avoidance Lemma*, which says that *If an ideal I in a commutative ring R is contained in a union of finitely many prime ideals P_i's, then it is contained in P_i for some i.*

Proposition 11.1. *If (R, m) is a regular local ring, then R is an integral domain with* $\dim(R) = d$.

Proof. If I is an ideal, let $\mu(I)$ be the number of minimal generators of I.

Suppose $d = 0$, then $\mu(m) = 0$. We have $m = \langle 0 \rangle \in R$, so R is a field, then also a domain.

Suppose $d = 1$, then $m = (x)$. Suppose $ab = 0$ and neither $a, b = 0$. By the intersection theorem, we can write $a = \alpha x^n$, $b = \beta x^m$ with α, β are units. Then

$$0 = ab = \alpha x^n \beta x^m = \alpha\beta x^{n+m},$$

so $x^{n+m} = 0$. Thus, x is in the minimal prime, which implies m contained in a minimal prime, so we have $\mathrm{ht}(m) = 0$, which is a contradiction. Then either $a = 0$ or $b = 0$. Therefore, R is a domain.

Suppose the result is true for dimension up to $d - 1$. We need to prove that the result is true for R of dimension d. Suppose m was contained in the union of m^2 and the finitely many minimal prime ideals. Then by Prime Avoidance Lemma, m must be contained either in m^2 or in one of the minimal prime ideals. However, by Nakayama's Lemma, $m \neq m^2$, so m is a minimal prime ideal, which makes the dimension to be zero. This is a contradiction to the assumption. Thus, there exists an element $x \in m \backslash m^2$ is not in any minimal prime, which means $x \in m$ with $m \not\subseteq P_1 \cup \cdots \cup P_r \cup m^2$, where P_i are minimal primes.

Let $A = m/(x)$, then A is the unique maximal ideal in $R/(x)$. By the choice of $R/(x)$, we have $\dim(R/(x)) = d - 1$. Now A/A^2 is a proper homomorphic image of m/m^2, so it can be generated by $(d-1)$ elements. By Nakayama's Lemma, A can also be generated by $(d-1)$ elements. So $R/(x)$ is a regular local ring, and by the induction assumption, $R/(x)$ is an integral domain. Thus x is a prime ideal of R. Since x is not in any minimal prime ideal, there is a minimal prime ideal properly contained inside (x) and we call this minimal prime ideal Q. Suppose $y \in Q$, then we write $y = rx$ for some $r \in R$. But since $x \notin Q, a \in Q$, we have $Q = xQ$. Then by Nakayama's lemma, $Q = 0$. Thus R is an integral domain. $\square$

From the prove of Proposition 11.1, in a regular local ring, there exists an element $x \in m \backslash m^2$ is not in any minimal prime, which means $x \in m$ with $m \not\subseteq P_1 \cup \cdots \cup P_r \cup m^2$, where P_i are minimal primes.

Corollary 11.2. *Let (R, m) be a local ring. Suppose x is not in m^2, then R is a regular local ring if and only if $R/(x)$ is a regular local ring.*

Proof. ($\Leftarrow$) Suppose $R/(xR)$ is a regular local ring, so $\dim(R/(xR)) = \mu(R/(xR))$. We also have $\dim(R/xR) = \dim(R) - 1$. Since $x \notin m^2$, $\mu(m/(xR)) = \mu(R) - 1$. Thus, $\dim(R) = \mu(R)$, which implies R is a regular local ring.

($\Rightarrow$) Suppose R is a regular local ring, so $\dim(R) = \mu(R)$, then $\dim(R/xR) = \dim(R) - 1$. Since $x \notin m^2$, $\mu(m/(xR)) = \mu(R) - 1$. Thus, $\dim(R/xR) = \mu(R/xR)$, which implies R/xR is a regular local ring. $\square$

Proposition 11.3. *If R is a regular local ring with $\dim(R) = d$ and $m = (x_1, \ldots, x_d)$. Then $x_1, \ldots, x_d$ is a regular sequence.*

Proof. Suppose R is a regular local ring. We want to prove by inducting on d.

When $d = 1$, then $x_1 \neq 0$. Since R is a domain, x_1 is regular.

When $d > 1$, $x_1 \notin m^2$, x_1 is nonzero divisor since R is a domain. Again, $R/(x_1R)$ is a regular local ring, so $\overline{x}_2, \ldots, \overline{x}_d$ is a regular sequence in $R/(x_1R)$ by induction. Thus, $x_1, \ldots, x_d$ is a regular sequence. $\square$

Theorem 11.4. *Suppose (R, m) is local, $\dim(R) = d$, then the following are equivalent:*

(1) R is a regular local ring.

(2) $\mathrm{pd}_R(k)$ is finite where $k = R/m$, i.e. R/m has a finite free resolution.

(3) $\mathrm{pd}_R(M)$ is finite for all finitely generated R-modules M, i.e. all finitely generated R-modules have a finite free resolution.

Proof. (1) $\Rightarrow$ (2): Suppose R is a regular local ring and $m = (x_1, \ldots, x_d)$, consider the Koszul complex on $x_1, \ldots, x_d$:

$$0 \longrightarrow \mathcal{K}_d \longrightarrow \cdots \longrightarrow \mathcal{K}_1 \longrightarrow \mathcal{K}_0 \longrightarrow R/m \longrightarrow 0$$

which is exact, since R is regular local, and thus $x_1, \ldots, x_d$ form a regular sequence. Then we have the diagram

$$0 \longrightarrow R^{\binom{d}{d}} \longrightarrow \cdots \longrightarrow R^{\binom{d}{2}} \longrightarrow R^{\binom{d}{1}} \longrightarrow R^{\binom{d}{0}} \longrightarrow R/m \longrightarrow 0$$

so $pd_R(k) < \infty$.

(2) $\Rightarrow$ (3): Let M be a finitely generated R-module and suppose $pd_R(k) < \infty$, then there exists n such that $\mathrm{Tor}_i(k, M) = 0$, for all $i > n$ and M. Take a minimal free resolution

$$\mathcal{F} : \cdots \longrightarrow F_{i+1} \xrightarrow{\phi_{i+1}} F_i \xrightarrow{\phi_i} F_{i-1} \xrightarrow{\phi_{i-1}} \cdots \longrightarrow F_n \longrightarrow \cdots \longrightarrow F_0 \longrightarrow M \longrightarrow 0$$

$\mathrm{Tor}_i(k, M) = 0$, for all $i > n$. Tensor with $k = R/m$ to get an exact sequence

$$\cdots \longrightarrow F_{i+1}/mF_{i+1} \xrightarrow{\overline{\phi}_{i+1}} F_i/mF_i \xrightarrow{\overline{\phi}_i} F_{i-1}/mF_{i-1} \longrightarrow \cdots$$

Since ϕ_i and ϕ_{i+1} have entries in m, $\overline{\phi}_i = \overline{\phi}_{i+1} = 0$, for $i > n$. We have $ker(\overline{\phi}_i) = F_i/mF_i$ and $im(\overline{\phi}_{i+1}) = 0$. $0 = \mathrm{Tor}_i(k, M) = ker(\overline{\phi}_i)/im(\overline{\phi}_{i+1})$ for $i > n$, which implies $F_i/(mF_i) = 0$, then $F_i = mF_i$, which implies $F_i = 0$ by Nakayama's lemma. Thus, we have $pd_R(M) < \infty$.

(3) $\Rightarrow$ (1): Consider the case $M = k$. Suppose $pd_R(k) < \infty$, take $x \in m \backslash m^2$ such that x is non-zero-divisor and $x \cdot k = 0$. Then by the proposition 9.7, $pd_{R/(xR)}(k) < \infty$. Then by induction, we can show that $R/(xR)$ is a regular local ring. So by Corollary 11.2, R is a regular local ring. □

Corollary 11.5. *If R is a regular local ring and Q is a prime ideal of R, then R_Q is regular.*

Proof. Since R is regular, R/Q has a finite R-free resolution by R-modules. We then localize at Q to obtain a finite R_Q-free resolution of $R_Q/QR_Q \cong (R/Q)_Q$. Thus, R_Q is regular by Theorem 11.4. □

12 Stably-free Modules

In this section, we introduce the definition and some propositions of stably-free modules that we need to use for the proof of the main theorem. The goal for this section is to show that if R-module P is stably-free with rank 1, then P is free.

Definition 12.1. R-module P is *stably free* if there exists free modules F, G such that $F = G \oplus P$.

The following proposition connects projective modules and finite free resolutions that we learned on section 9 to stably-free modules.

Proposition 12.1. *Suppose P is projective and there exists finite free resolution*

$$(*) : 0 \longrightarrow F_n \xrightarrow{\phi_n} F_{n-1} \xrightarrow{\phi_{n-1}} \cdots \longrightarrow F_1 \xrightarrow{\phi_1} F_0 \xrightarrow{\pi} P \longrightarrow 0$$

then P is stably free.

Proof. We prove by inducting on n. When $n = 1$, we have an exact sequence

$$0 \longrightarrow F_1 \longrightarrow F_0 \xrightarrow{\pi} P \longrightarrow 0$$

By Corollary 9.4, we have $F_0 \cong F_1 \oplus P$. Since F_0 and F_1 are free, P is stably free.

When $n > 1$, we have

$$0 \longrightarrow F_n \longrightarrow \cdots \longrightarrow F_1 \xrightarrow{\varphi_1} K \longrightarrow 0$$

with $K = ker(\pi)$, is a finite free resolution. If K is projective, then stably free by induction. Consider the exact sequence

$$0 \longrightarrow K \longrightarrow F_0 \longrightarrow P \longrightarrow 0.$$

So $F_0 \cong K \oplus P$. Since F_0 is free, so is $K \oplus P$, which implies K is projective, then K is stably free. So there exists F, G free modules such that $F = G \oplus K$, then $F_0 \oplus G = G \oplus K \oplus P = F \oplus P$. Since F_0, F, G are free, P is stably free. □

Lemma 12.2. *Suppose there are column vectors $v_1, \dots, v_n \in R^n$, $A = [v_1, \dots, v_n]$ as a matrix. Then $\{v_1, \dots, v_n\}$ is a basis for R^n if and only if $\det(A)$ is a unit in R.*

Proof. ($\Rightarrow$) Suppose $v_1, \dots, v_n$ is a basis for R^n. Let $e_1, \dots, e_n$ be the standard basis, then

$$e_1 = b_{11}v_1 + \cdots + b_{n1}v_n \Rightarrow e_1 = A \begin{bmatrix} b_{11} \\ b_{21} \\ \vdots \\ b_{n1} \end{bmatrix}$$

$$e_2 = b_{12}v_1 + \cdots + b_{n2}v_n \Rightarrow e_2 = A \begin{bmatrix} b_{12} \\ b_{22} \\ \vdots \\ b_{n2} \end{bmatrix}$$

$$\vdots$$

$$e_n = b_{1n}v_1 + \cdots + b_{nn}v_n \Rightarrow e_n = A \begin{bmatrix} b_{1n} \\ b_{2n} \\ \vdots \\ b_{nn} \end{bmatrix}$$

Then $B = (b_{ij}) = [e_1, \dots, e_n] = A \cdot B$, where $I_n = [e_1, \dots, e_n]$. Thus, $1 = \det(A) \cdot \det(B)$, which means $\det(A)$ is a unit in R.

($\Leftarrow$) Suppose $v_1, \dots, v_n \in R^n$ and $\det(A)$ is a unit in R, then there exists C such that $I_n = A \cdot C$. So $R^n = \langle e_1, \dots, e_n \rangle \subseteq \langle v_1, \dots, v_n \rangle$. Thus, $\{v_1, \dots, v_n\}$ spans R^n.

Let $r_1 v_1 + \cdots + r_n v_n = 0$, then $A \begin{bmatrix} r_1 \\ r_2 \\ \vdots \\ r_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$

Since A is nonzero and invertible, $\begin{bmatrix} r_1 \\ r_2 \\ \vdots \\ r_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$

Thus, $v_1, \dots, v_n$ are linearly independent. Therefore, $\{v_1, \dots, v_n\}$ is a basis for R^n. □

Theorem 12.3. *Suppose $R^n = G \oplus K$, where G is free of rank $(n-r)$ and $\{v_1, \dots, v_{n-r}\} \subseteq R^n$ is a basis for G. Then K is free of rank r if and only if the columns $v_1, \dots, v_{n-r}$ can be extended to an invertible matrix, in other words, can be extended to a basis of R^n.*

Proof. ($\Rightarrow$) Suppose K is free of rank r, then there exists $u_1, \dots, u_r \in K$ is a basis for K. Since $R^n = G \oplus K$, $\{v_1, \dots, v_{n-r}, u_1, \dots, u_r\}$ is a basis for R^n. By Lemma 12.2, $\det([v_1, \dots, v_{n-r}, u_1, \dots, u_r])$ is a unit. Thus, $v_1, \dots, v_{n-r}$ can be extended to a basis for R^n.

($\Leftarrow$) Suppose $v_1, \dots, v_{n-r}, w_1, \dots, w_r$ are such that $[v_1, \dots, v_{n-r}, w_1, \dots, w_r]$ is invertible, then $\{v_1, \dots, v_{n-r}, w_1, \dots, w_r\}$ is a basis for R^n. We write $w_i = u_i + k_i$, where $u_i \in G, k_i \in K$. Take $k \in K$, then

$$k = a_1 v_1 + \cdots + a_{n-r} v_{n-r} + b_1(u_1 + k_1) + \cdots + b_r(u_r + k_r).$$

So we have $k - (b_1k_1 + \cdots + b_rk_r) = a_1v_1 + \cdots + a_{n-r}v_{n-r} + b_1u_1 + \cdots + b_ru_r$.

Since $G \cap F = 0$, $k-(b_1k_1+\cdots+b_rk_r) = 0$. So $k = (b_1k_1+\cdots+b_rk_r)$, then $K = \langle k_1, \ldots, k_r\rangle$. Thus, $\langle v_1, \ldots, v_{n-r}, k_1, \ldots, k_r\rangle = R^n$, let $A = \{v_1, \ldots, v_{n-r}, k_1, \ldots, k_r\}$.

Again, let $e_1, \ldots, e_n$ be the standard basis, then

$$e_1 = A\begin{bmatrix} c_{11} \\ c_{21} \\ \vdots \\ c_{n1} \end{bmatrix}$$

$$e_2 = A\begin{bmatrix} c_{12} \\ c_{22} \\ \vdots \\ c_{n2} \end{bmatrix}$$

$\vdots$

$$e_n = A\begin{bmatrix} c_{1n} \\ c_{2n} \\ \vdots \\ c_{nn} \end{bmatrix}$$

So we have $I_n = A \cdot C$. By Lemma 12.2, A is invertible. So the columns are basis for R^n, which means $k_1, \ldots, k_r$ are linearly independent. Thus, $\{k_1, \ldots, k_r\}$ is a basis for K. $\square$

Lemma 12.4. *If P is stably free with rank 1, then P is free.*

Proof. Suppose P is stably free with rank 1, then we can write $R^n = R^{n-1} \oplus P$. Let $v_1, \ldots, v_{n-1} \in R^n$ is a basis for R^{n-1}. We want to show that $v_1, \ldots, v_{n-1}$ can be extended to a basis for R^n. Let m be any maximal ideal. Since $R^n = R^{n-1} \oplus P$, we have

$$k^n = R^n/(mR^n) = R^{n-1}/(mR^{n-1}) \oplus P/(mP),$$

where $k = R/m$.

We then let $\overline{v}_1, \ldots, \overline{v}_{n-1}$ be a basis for $R^{n-1}/(mR^{n-1})$ as column vector in k^n, then rank $\overline{C} = [\overline{v}_1, \ldots, \overline{v}_{n-1}]$ is $n-1$. So some $(n-1)\times(n-1)$ submatrix of $\overline{C}$ has non-zero determinant, then some $(n-1) \times (n-1)$ submatrix of $[v_1, \ldots, v_{n-1}]$ is not in m.

Let Δ_i be the $(n-1) \times (n-1)$ minor obtained by deleting the i^{th} row of $[v_1, \ldots, v_{n-1}]$. Then we have $I = (\Delta_1, \ldots, \Delta_n)R = R$, so there exists $a_1, \ldots, a_n \in R$, such that

$$a_1\Delta_1 - a_2\Delta_2 + \cdots + (-1)^n a_n\Delta_n = 1,$$

which means $A = \begin{vmatrix} a_1 & v_1 & \cdots & v_{n-1} \\ a_2 & & & \\ \vdots & \vdots & \vdots & \vdots \\ a_n & & & \end{vmatrix}$.

Thus, $\det(A) = a_1\Delta_1 - a_2\Delta_2 + \cdots + (-1)^n a_n\Delta_n = 1$. So we know that A is invertible. Therefore, $v_1, \ldots, v_{n-1}$ can be extended to a basis for R^n $\square$

13 Main Theorem

Theorem 13.1. *Suppose R is a Noetherian ring. If R is a regular local ring, then R is a unique factorization domain.*

Before the proof, let us learn some history about the theorem. This theorem is called Auslander-Buchsbaum theorem. And it was first proved by Maurice Auslander and David Buchsbaum in 1959.

Prior to the result, Zariski proved that if every complete regular local ring of dimension 3 is a unique factorization domain, then every complete regular local ring is a unique factorization domain. In addition, Mori and Krull proved that a local ring is a unique factorization domain if it's completion is a unique factorization domain.

In 1958, Nagata proved in [3] that if every regular local ring of dimension 3 is a UFD, then every regular local ring is a UFD. And then in 1959, Auslander and Buchsbaum proved in [4] that every regular local ring of dimension 3 is a UFD.

Proof. Since R is a regular local ring, R is an integral domain. Assume $\dim R = d$, then we can induct on d.

If $d = 0$, R is a field, so is a UFD.

If $d = 1$, the maximal ideal $m = \langle a \rangle$ where $a \in R$ is prime. Then every prime ideal contains a principal prime, by Theorem 5.6, R is a UFD.

If $d > 1$, R is Noetherian. Let us take $x \in m \backslash m^2$, so x is prime. By Nagata's Lemma, it suffices to show that R_x is a UFD. Now, let us choose a height one prime P_x in R_x. We then want to show P_x is principal.

We claim that P_x is a stably-free R_x-module of rank 1. Indeed, first take a finite free resolution of P over R

$$0 \longrightarrow F_n \longrightarrow F_{n-1} \longrightarrow \cdots \longrightarrow F_1 \longrightarrow F_0 \longrightarrow P \longrightarrow 0,$$

then localize the resolution at x to get

$$0 \longrightarrow (F_n)_x \longrightarrow (F_{n-1})_x \longrightarrow \cdots \longrightarrow (F_1)_x \longrightarrow (F_0)_x \longrightarrow P_x \longrightarrow 0$$

For the claim, we first want to show P_x is projective using Proposition 9.6. Take $Q \subseteq R_x$ be prime, then $Q = Q'_x$ for some prime $Q' \subseteq R$ with $x \notin Q'$, and $R_{Q'} = (R_x)_Q$ is a regular local ring by Corollary 11.5.

If $P_x \nsubseteq Q$, then $(P_x)_Q = (R_x)_Q = R_Q$ is a free R_Q-module, which implies P_x is projective.

If $P_x \subseteq Q$, then $(P_x)_Q = P_Q \subseteq R_Q$ is a height 1 prime in R_Q, where R_Q has dimension less than d. By induction on d, $(P_x)_Q = P_Q$ is principal, i.e. free of rank 1 over R_Q, so P_x is locally free over R_x, which implies P_x is projective by Proposition 9.6. Thus, P_x is projective and there is a finite free resolution of P_x. Since $P \subseteq R$ with $\text{rank}(P) = 1$, then by Proposition 12.1, P_x is a stably free R_x-module of rank 1.

Therefore, by Lemma 12.4, P_x is free of rank 1, which implies P_x is principal. So by Theorem 5.6, R_x is a UFD. Then by Nagata's Lemma, R is a UFD. $\square$

References

[1] Kaplansky, Irving. *Commutative Rings*. Dillon's Q.M.C. Bookshop, 1968.

[2] Matsumura, Hideyuki. *Commutative Ring Theory*. 1st pbk. ed., with corrections. ed., Cambridge University Press, 1989.

[3] Nagata, Masayoshi. "A General Theory of Algebraic Geometry Over Dedekind Domains, II: Separably Generated Extensions and Regular Local Rings." American Journal of Mathematics, vol. 80, no. 2, 1958, pp. 382–420.

[4] Auslander, M, and Buchsbaum, D A. "UNIQUE FACTORIZATION IN REGULAR LOCAL RINGS." Proceedings of the National Academy of Sciences of the United States of America, vol. 45, no. 5, 1959, pp. 733–734.

[5] Richard G. Swan. *Vector Bundles and Projective Modules*. Transactions of the American Mathematical Society, vol. 105, no. 2, 1962, pp. 264–277.