Comm & Hom

Yuxuan Sun

November 20, 2023

Abstract

This note is written from the course Commutative Algebra and Homological Algebra taught by Prof. Tyler Lawson in University of Minnesota Twin Cities. This note is not guaranteed to be correct and is meant to be used as a dictionary.

Contents

1 Intro

Theorem 1.0.1. *radical ideal is generated by a polynomial f with no multiple roots.*

Suppose $J \subset \mathbb{C}[x_1, \dots, x_n]$ is an ideal. Then $I(Z(J)) = rad(J) = \{f \mid f^n \subset J\}$

Definition 1.0.2. radical ideal is generated by a polynomial f with no multiple roots. cokernel: take the image of f and mod out by image of f.

1.1 Modules

Let R be a commutative ring. An R-module M is an abelian group $(+)$ with a map $R \times M \to M$ written $(r, m) \mapsto rm$. Satisfying

1. associativity: $r(sm) = (rs)m$ for all $r, s \in R, m \in M$.
2. distributivity: $r(m + m') = rm + rm'$ and $(r + r')m = rm + r'm$ for all $r, r' \in R, m, m' \in M$.
3. unitality: $1m = m$ for all $m \in M$.

Several things you could derive from the definition: $0m = 0, (-1)m = -m$, etc.

Example 1.1.1. *Let $R = k[x]$. A $k[x]$-module is*

- *a k-vector space M*
- *with a map $xM \to M$, where $m \mapsto xm$, a k linear transformation.*

Example 1.1.2. *What is an R-submodule of R? It's*

1. *$J \subseteq R$;*
2. *closed under addition, 0, negatives;*
3. *for any $r \in R, j \in J, r, j \in J$.*

an ideal.

Definition 1.1.3. Let M be an R-module, N a sbugroup of M. N is a *submodule* if for any $n \in N$ and $r \in R$, the product rn is in N.

Definition 1.1.4. If M is an R-module, we shall write $\operatorname{ann} M$ for the annihilator of M; that is,

$$\operatorname{ann} M = \{r \in R \mid rM = 0\},$$

which is an ideal.

Definition 1.1.5. Let $I \subseteq R$ an ideal, M an R-module. We denote

$$IM = \left\{ \sum a_i m_i \mid a_i \in I, m_i \in M \right\} \subseteq M$$

the smallest R-submodule of M containing all elements of the form am, where $a \in I, m \in M$.

Example 1.1.6. *Suppose M is an R-module. FOr $N, N' \subseteq M$ submodules,*

$$[N : N'] \subseteq R \quad x \in [N : N'] \iff xN' \subseteq N.$$

For N a submodule, I an ideal

$$[N : I] \subseteq M. \quad y \in [N : I] \iff Iy \subseteq N.$$

The point of having the above is to generalize the annihilator.

Example 1.1.7. *ann* $M = [O : M]$.

Some operations we could do. Given a sequence of modules $M_1, M_2, \ldots$.

Definition 1.1.8. We denote

$$\prod_{i \in I} M_i = \{(m_1, m_2, \ldots) \mid m_i \in M_i\}.$$

$\prod M_i$ is an R-module with componentwise addition and scalar multiplication.

Note that $\oplus M_i \subseteq \prod M_i$, a sub-$R$-module.

Also, $\oplus M_i = \{(m_i)_{i \in I} \mid \text{ only finitely many } m_i \text{ are zero }\}$

Suppose we have an R-module homomorphism

$$f : M \to N.$$

We could construct 3 modules: $ker(f) \subseteq M, Im(f) \subseteq N, coker(f) = N/Im(f)$

Definition 1.1.9. Suppose we have R-module homomorphism

$$f : m \to N \quad g : N \to P.$$

This is exact if $\operatorname{Im} f = \ker g$.

Definition 1.1.10. If we have a sequence of maps

$$\cdots \to M_1 \to M_2 \to M_3 \to \cdots.$$

then we say it's exact iff each 2-term sequence is exact.

Saying $0 \to M \to N$ is exact is saying f is injective. And $M \to N \to 0$ is exact is saying f is surjective.

Definition 1.1.11. A short exact sequence is an exact sequence

$$0 \to M \to N \to P \to 0 \quad f : M \to N, g : N \to P.$$

This tells us that

1. M iso to $Im(f)$
2. P iso to $N/ker(g)$
3. $ker(g) = Im(f)$, P iso $coker(f)$

Definition 1.1.12. A free R-module is an R-module isomorphic to $\oplus_{i \in I} R$. In particular, R^n are the finitely generated free modules.

Definition 1.1.13. A module M is finitely generated if there exists $m_1, \ldots, m_n \in M$ such that every element of M is of the form $\sum_{i=1}^{n} a_i m_i$ for some $a_i \in R$.

Definition 1.1.14. A module M if finitely presented if there exists an exact sequence

$$R^n \to R^m \to M \to 0.$$

2 Localization

2.1 Fractions

Suppose R is a ring, $U \subseteq R$ is a subset thatis closed under multiplication, and contains the unit $1 \in R$.

Definition 2.1.1. We can form the localization $R[U^{-1}]$, whose elements are

$$\{(r, s) \mid r \in R, s \in U\}.$$

We also put an equivalence relation on the elements.

$$(r, s) \equiv (r', s') \iff \exists u, v \in U, (ur, us) = (vr', vs').$$

Note that the equivalence relation is different from cross-multication as what we do in fractions.

Example 2.1.2. *Let $R = \mathbb{Z}, U = \{1, 2, 4, 6, 16, \ldots\}$. Then*

$$R[U^{-1}] = \mathbb{Z}\left[\frac{1}{2}\right] = \left\{\frac{p}{q} \mid p \in \mathbb{Z}, q = 2^k\right\}.$$

Definition 2.1.3. In $R[U^{-1}]$, we have a ring.

$$\begin{aligned}(r, s) + (r', s') &= (rs' + r's, ss')\\ (r, s) \cdot (r', s') &= (rr', ss')\\ 0 &= (0, 1)\\ 1 &= (1, 1)\end{aligned}$$

Example 2.1.4. *Let $R = \mathbb{Z}/6, U = \{1, 3\}$. Then localization is smaller:*

$$R[U^{-1}] = \mathbb{Z}/2.$$

Example 2.1.5. *Let $R = \mathbb{C}[x], U = \{1, x, x^2, x^3, \ldots\}$. Then*

$$R[U^{-1}] = \mathbb{C}[x, x^{-1}] = \{f(x)/x^n | f(x) \text{ poly }, n \in \mathbb{N}\} = \left\{\sum_{n\in\mathbb{Z}} a_n x^n \mid a_n \in \mathbb{C}\right\}.$$

Note that in the summation there should only be finitely many n. The ring is also called Laurent polynomials.

This ring is isomorphic to

$$\mathbb{C}[x, y]/(yx - 1).$$

Note that there is always a ring homomorphism

$$\phi : R \to R[U^{-1}] \quad \phi(r) = \frac{r}{1}.$$

Example 2.1.6. *$R = \mathbb{C}[x_1, \ldots, x_n], U = R - \{0\}$. Note U is closed under multiplication because R is an integral domain.*

$$R[U^{-1}] = \{f(\vec{x})/g(\vec{x}) \mid f, g \in \mathbb{C}[x_1, \ldots, x_n], g \neq 0\}.$$

Proposition 2.1.7. *The theory of ideals in $R[U^{-1}]$ is closely related to the theory of ideals in R. Given an ideal J in R, we could have $J \cdot R[U^{-1}]$, which is an ideal in $R[U^{-1}]$.*

The map from ideals of $R[U^{-1}]$ to ideals of R is an injection. They are sort of "ideals that don't meet the set U".

An ieal J is of the form $\phi^{-1}(L)$ iff for any a, b s.t. $a \in R, b \in U$, $ab \in J \implies a \in J$.

There is a correspondance between prime ideals of $R[U^{-1}]$ and prime ideals of R that don't contain any elements of U.

Example 2.1.8. *prime ideals of $\mathbb{Q}$; prime ideals of $\mathbb{Z}$ that don't contain any elements of the set $\{1, 2, 3, 4, 5, \ldots\}$; $\{(0)\}$.*

Definition 2.1.9. Supose R is a ring. $P \subseteq R$ is a prime ideal. We define R_P to be the localization of the set $U = R - P$.

Note that U is closed under multiplication because P is prime.

Also, R_P has one maximal ideal: PR_P.

There is a correspondance between prime ideals of R_P; prime ideals of R that don't contain any elements of U; prime ideals of R contained in P.

Example 2.1.10.

$$\mathbb{Z}_{(2)} = \left\{ \frac{n}{m} \mid m \textit{ odd} \right\}.$$

This has 2 ideals: $(0), (2)$.

Definition 2.1.11. A ring R is *local* if it has a unique maximal ideal.

R_P is always local if P is prime.

If R is a ring, M is an R-module, $U \subseteq R$ is a subset closed under multiplication and 1. We can construct

$$M[U^{-1}] = \left\{ \frac{m}{s} \mid m \in M, s \in U \right\}.$$

$M[U^{-1}]$ is an abelian group and a module on $R[U^{-1}]$.

Example 2.1.12. *$R = \mathbb{Z}, U = \{1, 3, 9, 27, \ldots\}, M = \mathbb{Z}/10$. Check that $M[U^{-1}] \cong \{0\}$.*

2.2 Hom

For R-modules M, N. There is a new R-module $\mathrm{Hom}_R(M, N)$

$$\mathrm{Hom}_R(M, N) \subseteq \{f : M \to N\}.$$

Functions that are

1. group homomorphisms
2. R-linear: $f(rx) = rf(x)$

Definition 2.2.1. $\mathrm{Hom}_R(M, N)$ is an R-module in the following way.

- $f + g : (f + g)(m) = f(m) + g(m)$
- $rf : (rf)(m) = rf(m)$

There are some properties of Hom.

1. $\mathrm{Hom}_R(R, N) \cong N$, where $f \mapsto f(1), n \in N \mapsto f(r) = rn$. Basically the same as picking an element from N.
2. $$\mathrm{Hom}_R(\oplus_{i\in I} M_i, N) \cong \prod_{i\in I} \mathrm{Hom}_R(M_i, N).$$
   The RHS is choosing for each $i \in I$, a homomorphism $M_i \to N$. There's also
   $$\mathrm{Hom}_R(M, \prod N_i) \cong \prod_{i\in I} \mathrm{Hom}_R(M, N_i).$$
3. If I have R-module homomorphisms
   $$\alpha : M \to M' \quad \beta : N \to N'.$$
   I get a map
   $$\mathrm{Hom}_R(\alpha, \beta) : \mathrm{Hom}_R(M', N) \to \mathrm{Hom}_R(M, N') \quad \text{where} \quad f \mapsto \beta f \alpha.$$
   Thi respects identity functions and function composition. Functorial.
4. Exactness. Hom_R is *left-exact*:
   (a) If $M' \to M \to M'' \to 0$ is an exact sequence, then for any N,
   $$0 \to \mathrm{Hom}_R(M'', N) \to \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M', N)$$
   is also exact.
   (b) If $0 \to N' \to N \to N''$ is exact then
   $$0 \to \mathrm{Hom}_R(M, N') \to \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M, N'')$$
   is exact.

For R-module M, N there is a tensor product $M \otimes_R N$, which we get by taking all formal sums of symbols $m \otimes n, m \in M, n \in N$, mod out by subgroup generated by elements of the form

- $(m + m') \otimes n - m \otimes n - m' \otimes n$;
- $m \otimes (n + n') - m \otimes n - m \otimes n'$;
- $(rm) \otimes n - m \otimes (rn)$.

Example 2.2.2.

$$R[x_1,\dots,x_n]\otimes_R R[y_1,\dots,y_n]\cong R[x_1,\dots,x_n,y_1,\dots,y_n].$$

Properties of $\otimes_R$.

1.
$$R\otimes_R M\cong M\quad \sum r_i\otimes m_i\mapsto \sum r_i m\quad 1\otimes m<-m.$$

2.
$$(\oplus M_i)\otimes_R N\cong \oplus\left(M_i\otimes_R N\right).$$

3. Functornality. For R-module homomorphisms $\alpha: M\to M'$, $\beta: N\to N'$, we get an R-module homomorphism
$$\alpha\otimes\beta: M\otimes_R N\to M'\otimes_R N'\quad \sum m_i\otimes n_i\mapsto \sum \alpha(m_i)\otimes\beta(n_i).$$

4. Right exactness. If $M'\to M\to M''$ is exact, then
$$M'\otimes_R N\to M\otimes_R N\to M''\otimes_R N\to 0.$$
is exact.

5. Symmetry.
$$M\otimes_R N\cong N\otimes_R M\quad \sum m_i\otimes n_i\mapsto n_i\otimes m_i.$$

Proposition 2.2.3.
$$M[U^{-1}]\cong R[U^{-1}]\otimes_R M.$$

Proof sketch. The procedure we could do is
$$\frac{m}{u}\mapsto\frac{1}{u}\otimes m\quad \frac{rm}{u}\leftarrow\!\shortmid\ \frac{r}{u}\otimes m.$$
$\square$

Definition 2.2.4. An R-module F is *flat* whenever
$$f: M\to N\quad\text{is injective,}$$
and the map
$$F\otimes_R M\to F\otimes_R N\quad\text{is injective.}$$
Alternatively,
$$0\to M\to N\text{ exact}\implies 0\to F\otimes_R M\to F\otimes_R N\text{ exact }.$$

Theorem 2.2.5. *$R[U^{-1}]$ is always a flat module over R.*

Proof. Suppose $f : M \to N$ is injective. We need to check $M[U^{-1}] \to N[U^{-1}]$ is also injective.

Suppose $\frac{m}{u} \in M[U^{-1}]$ which goes to 0 in $N[U^{-1}]$, then $\frac{f(m)}{u} = \frac{0}{1}$ in $N[U^{-1}]$. This means there exists $v \in U$ s.t. $vf(m) = 0$, which leads to $vf(m) = f(vm) = 0$. Since f is injective, $vm = 0$ in M. Then $\frac{m}{u} = \frac{vm}{vu} = \frac{0}{m} = \frac{0}{1}$. ☐

Example 2.2.6. *$\mathbb{Q}$ is a flat module over $\mathbb{Z}$. $\mathbb{Z}/2$ is a falt module over $\mathbb{Z}/6$. Both $\mathbb{C}(x)$ and $\mathbb{C}[x, x^{-1}]$ are flat over $\mathbb{C}[x]$.*

Theorem 2.2.7. *A module M over R is zero iff for every maximal ideal m, the localization M_m is zero.*

Definition 2.2.8. An R-module M is *Noetherian* is every submodule of M is finitely genereated.

Theorem 2.2.9. *If*

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$$

is exact, then M is Noetherian (resp. Artinian) iff M' and M'' are both Noetherian (resp. Artinian).

2.3 Rings and Modules of Finite Length

Definition 2.3.1. An R-module M is *simple* iff M has exactly 2 R-submodule: 0 and M.

Definition 2.3.2. A *composition series* for a module M is a chain

$$0 = M_0 < M_1 < M_2 < \cdots < M_{n-1} < M_n = M$$

of submodules (with strict inclusion) such that for all $1 \leq i \leq n$, M_i/M_{i-1} is simple.

Proposition 2.3.3. *A $\mathbb{Z}$-module M is simple iff it's of the form $\mathbb{Z}/p$ where p is prime.*

Proposition 2.3.4. *Let R be an R-module, J be an ideal. R/J is simple iff J is maximal.*

Example 2.3.5. *Let $R = \mathbb{C}[x, y]$, $M = C_z[x, y]/(x^2, xy, y^2)$.*

Proposition 2.3.6. *If k is a field, a compositions series for a vectors space V exists iff V is finite dimensional, the sequence always goes from 0 dimension to 1, 2, and grows to the entire thing V.*

Definition 2.3.7. The *length* of an R-module M is the minimal length of a compositions series, if one exists, or ∞. We denote it as $l(M)$.

Theorem 2.3.8. *Every composition series for M has the same length.*

Throughout the following, we assume all modules we work with have finite length.

Proposition 2.3.9. *If $N < M \implies l(N) < l(M)$.*

Proof. Choose a composition series for N:

$$0 < N_1 < N_2 < \cdots < N.$$

We start with a composition series for M of minimal length:

$$0 < M_0 < M_1 < \cdots < M_n = M.$$

We intersect it with N: $N_k = M_k \cap N$. Then we don't necessarily have strict containment.

$$0 = N_0 \leq N_1 \leq N_2 \leq \cdots \leq N_n = N.$$

□

Theorem 2.3.10. *Every composition series of M has the same length.*

Proof. Suppose we have a composition series

$$0 = M_0 < M_1 < \cdots < M_n = M,$$

with the assumption that M_k/M_{k-1} simple. Then

$$0 \leq l(M_0) < l(M_1) < \cdots < l(M_n) = l(M).$$

Thus $n \leq l(M)$. From the definition of length, we know $n = l(M)$. □

Proposition 2.3.11. *$l(M) < \infty$ iff M satisfies ACC and DCC.*

Definition 2.3.12. A *finite filtration* of a module M is a sequence

$$0 = M_0 \leq M_1 \leq M_2 \cdots \leq M_n = M.$$

Associated to a filtration, we have *subquotients*

$$M_k/M_{k-1} = gr^k(M) \quad \text{grading } k.$$

Proposition 2.3.13. *Suppose M, N are modules with filtrations $\{M_k\}, \{N_k\}$ and a function $f : M \to N$ s.t. $f(M_k) \subseteq N_k$. Then we get induced module maps*

$$gr^k(M) \to gr^k(N) \quad \textit{where} \quad [x] \mapsto [f(x)].$$

Also, if all of these are isomorphisms, then so is f.

Example 2.3.14. $gr^k(M) \cong 0 \iff M_k/M_{k-1} = 0 \iff M_{k-1} = M_k$.

Theorem 2.3.15 (Snake Lemma)**.** *If (DO THE TIKZ)*

Proposition 2.3.16. *Suppose M has a composition series and N is a submodule with quotient M/N. We have*

$$l(M) = l(N) + l(M/N).$$

Suppose M has a filtration, we could take the entire sequence and localize it.

Proposition 2.3.17. *If R is Noetherian, then so is any quotient R/J and any localization $S^{-1}R$.*

Subrings of Noetherian ring are not necessarily Noetherian.

Theorem 2.3.18. *If R is Noetherian, then so is $R[x]$.*

Definition 2.3.19. If we have a polynomial $a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n, a_n \neq 0, a_i \in R$, we say f has *degree* n and a_n is its *lead coefficient*

Theorem 2.3.20 (Hilbert basis theorem)**.** *If R is Noetherian, then so is $R[x]$.*

A natural proposition of the theorem will be the following.

Proposition 2.3.21. *If R is Noetherian, so is $R[x_1, \ldots, x_n]$.*

Theorem 2.3.22. *If R is Noetherian, so is the power series ring $R[\![x]\!]$.*

3 Primary Decomposition

3.1 Associated Primes

Definition 3.1.1. Suppose M is an R-module. The set of *associated primes* is the collection

$$\mathrm{Ass}(M) = \{P \mid P \leq R \text{ is prime } P = a_n(x) \mid x \in M\}.$$

Proposition 3.1.2. *If $M \neq 0$, then $\mathrm{Ass}(M)$ is not empty. In fact, any ideal which is maximal in the set $\{\mathrm{ann}(x) \mid x \in M, x \neq 0\}$ is prime.*

If R is Noetherian and $M \neq 0$, then $\mathrm{Ass}(M) \neq \emptyset$.

Proposition 3.1.3. *$P \in \mathrm{Ass}(M)$ iff there exists an injective map of R-modules $R/P \to M$.*

Proposition 3.1.4. *Suppose R is Noetherian and M finitely generated R-module. Then there exists a filtration*

$$0 = M_0 \subseteq M_1 \subseteq .. \subseteq M_k = M$$

such that the subquotients $gr^i(M) = M_i/M_{i-1}$ are isomorphic to R/P_i where P_i are prime.

Proposition 3.1.5. *Suppose M is an R-module and $N \subseteq M$ is a submodule. Then*

$$\mathrm{Ass}(N) \subseteq \mathrm{Ass}(M) \subseteq \mathrm{Ass}(N) \cup \mathrm{Ass}(M/N).$$

Proof. First containment.

$$P \in \mathrm{Ass}(N) \implies P = \mathrm{ann}(x) \quad x \in N \subseteq M \implies P \in \mathrm{Ass}(M).$$

Second containment.

Take $P \in \mathrm{Ass}(M)$, then $P = \mathrm{ann}(y)$ where $y \in M$. Consider $\overline{y} \in M/N$.

First case is that $\mathrm{ann}(\overline{y}) = P$, then $P \in \mathrm{Ass}(M/N)$.

Second is that $\mathrm{ann}(\overline{y}) > \mathrm{ann}(y) = P$. Then there exists $s \in R$ such that $s \in \mathrm{ann}(\overline{y})$ but $s \notin P$. Then $sy \in M, \overline{sy} = s\overline{y} = 0 \in M/N$, which tells us that $sy \in N$.

We know that $r \in \mathrm{ann}(sy) \iff rs \in \mathrm{ann}(y)$. Note that $\mathrm{ann}(sy) = P$. □

Example 3.1.6. *Consider* $\mathbb{C}[x, y]/(x^2, xy) = M$*. Then*

$$\mathrm{Ass}_{\mathbb{C}[x,y]}(M) = \{(x), (x, y)\}.$$

We know this from observing $\mathrm{ann}(y) = (x), \mathrm{ann}(x) = (x, y)$.

3.2 Prime Avoidance

Theorem 3.2.1. *Suppose* $I_1, I_2, \ldots, I_n, J$ *are ideals such that* $J \subseteq \cup_{i=1}^{n} I_j$*. If either*

1. *the ambient ring* R *contains an infinite field, or*
2. *at most two of the ideals* $I_1, I_2, \ldots, I_n$ *are not prime,*

then $J \subseteq I_j$ *for some* j.

Proposition 3.2.2.

$$\bigcup_{P \in \mathrm{Ass}(M)} P = \{0\} \cup \{x \in R \mid x \textit{ is a zero-divisor on } M\}.$$

Proposition 3.2.3. *Suppose* M *is a finitely generated module over a Noetherian ring* R*. Then* $\mathrm{Ass}(M)$ *automatically contains any minimal elements in the set*

$$\{P \subseteq R \mid P \textit{ prime}, P \supseteq \mathrm{ann}(M)\}.$$

Definition 3.2.4. An idea $I \subseteq R$ is *primary* iff $|\mathrm{Ass}(R/I)| = 1$. Specifically, say $\mathrm{Ass}(R/I) = \{P\}$, then we say I is P-primary.

Proposition 3.2.5. *An ideal* I *is* P*-primary iff*

1. *Every element* $x \notin P$ *is not a zero divisor in* R/I.
2. *Every element* $x \in P$ *has a power* $x^n \in I$.

Proposition 3.2.6. *An ideal* $I \subseteq R$ *is* P*-primary iff any of the following criteria are true.*

1. *If* $xy \in I$*, and* $x \notin P$*, then* $y \in I$.

Proposition 3.2.7. *An ideal* $I \subseteq R$ *is primary iff*

1. *if* $xy \in I$ *and* $x \notin I$*, then* $y^n \in I$ *for some* $n > 0$.

2. *if $xy \in I$, $x \notin I, y \notin I$, then $x^n \in I$ and $y^m \in I$ for some $n, m > 0$.*

Proposition 3.2.8. *In a Noetherian ring R, every ideal is a finite intersection of irreducible ideals.*

The above could be proven by looking at the maximal counterexample.

Proposition 3.2.9. *If $I \subsetneq R$ is an irreducible ideal, then I is primary.*

Combine them together we have the following.

Proposition 3.2.10. *Any ideal of R is a finite intersection of primary ideals.*

Note that we proved irreducible implies primary, but the converse is false.

Also we showed that if I is P-primary, then $P^n \subseteq I \subseteq P$. The converse is not true either.

Proposition 3.2.11. *If M is maximal and $M^n \subseteq I \subseteq M$, then I is M-primary.*

Minimal primes in the primary decomposition are unique.

If R is a UFD, so is $R[x]$. How do we check whether a polynomial $P = a_0 + a_1 x + \cdots + a_n x^n$ is irreducible?

1. $\gcd(a_0, \ldots, a_n) = 1$
2. P is irreducible in $Q[x]$ where Q is the fraction field.

If M is an R-module. (R Noetherian, M finitely generated).

Definition 3.2.12. A submodule $N \subseteq M$ is *P-primary* in M if $\mathrm{Ass}_R(M/N) = \{P\}$.

3.3 Nakayama's Lemma

Proposition 3.3.1. *Suppose R is a ring, M a finitely generated module over R, $I \subseteq R$ an ideal. If $IM = M$, then there exists $a \in R$ such that $a \cong 1 \mod I$ and $aM = 0$.*

Definition 3.3.2. The *Jacobson radical* of a ring R is the intersection of all maximal ideals of R, called the *Jacobson radical*.

Proposition 3.3.3 (Nakeyama's lemma)**.** *$x \in R$ is an element of the Jacobson radical iff $1 + rx$ is a unit for any $r \in R$.*

Proposition 3.3.4 (Nakayama's Lemma)**.** *If N is a finitely generated R-module and $mN = N$ then $N = 0$.*

local rings have unique maximal ideal.

Nakeyama's lemma has other different forms, for example the following.

Theorem 3.3.5. *Suppose R is a local ring, M is a finitely generated R-module, $x_1, \ldots, x_n \in M$ are generators of M mod the maximal ideal, then $x_1, \ldots, x_n$ generate M.*

If you throw out "finitely generated", the above theorem is false.

Definition 3.3.6. An *idempotent* in R is an element $e \in R, e^2 = e$.

Proposition 3.3.7. *If $e \in R$ is idempotent, then $R \cong R/(e) \times R/(1-e)$.*

Proposition 3.3.8. *If R is a ring, $I \subseteq R$ a finitely generated ideal satisfying $I^2 = I$, then there exists an idempotent $e \in R$ s.t. $(e) = I$. (implies $R \cong S \times I$).*

Proposition 3.3.9 (Cayley Hamilton Theorem)**.** *Suppose M is a module over a ring R that can be generated by n elements, and $\phi : M \to M$ is a module homomorphism $\phi(M) \subseteq IM$, then there exists a polynomial*

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n, \quad a_j \in I^j.$$

such that for all $m \in M$,

$$0 = \phi^n m + a_1 \phi^{n-1} m + \cdots + a_n m.$$

Definition 3.3.10. Suppose R is a ring and S is an *R-algebra* (there's a ring homomorphism ϕ from R to S). An element in $s \in S$ is *integral over R* if there exists a monic polynomial $p(x) = x^n + a_1 x^{n-1} + \cdots + a_n \in R[x]$ such that $p(s) = 0$, which means

$$s^n + \phi(a_1)s^{n-1} + \cdots + \phi(a_n) = 0.$$

Recall

Theorem 3.3.11 (Rational zeros theorem)**.** *If*

$$x^n + a_1 x^{n-1} + \cdots + a_n$$

is a polynomial with integer coefficients and $p/q \in \mathbb{Q}$, then $p/q \in \mathbb{Z}$.

SEARCH

Remark that if $Im(\phi)$ is a subring of S, then s is integral over R iff s is integral over $Im(\phi)$.

WLOG we often assume $R \subseteq S$ when discussing integrality.

Definition 3.3.12. For $R \subseteq S$ a subring, define $\overline{R}$, the *integral closure of R*, to be

$$\{s \in S \mid s \text{ is integral over } r\}.$$

Theorem 3.3.13. *$\overline{R}$ is a ring containing R.*

Proof. To show $R \subseteq \overline{R}$, we know $r \in R$ satisfies $x - r$. □

Definition 3.3.14. If $R \subseteq S$ and $s \in S$, we define

$$R[s] := \text{ subring of } S \text{ generated by } R \text{ and } s = \left\{ \sum_i^r a_i s^i \mid a_i \in R \right\}.$$

Proposition 3.3.15. *TFAE*

1. *s is an integral over R*
2. *The set $R[s] \subseteq S$ is a finitely-generated R-module*
3. *there exists a subring $R \subseteq T \subseteq S$ s.t. T is a finitely generated R-module and $s \in T$.*

Proof. $2 \implies 3$ is immediate when $T = R[s]$.

$3 \implies 1$ uses Cayley-Hamilton Theorem. □

In geometry, we are taking out singularities by taking integral closures.

Proposition 3.3.16. *If R is a UFD, then R is integrally closed in its field of fractions K.*

Proof. Suppose $\frac{r}{s} \in K$, $\gcd(r, s) = 1$, and $\frac{r}{s}$ is integral over R. We multiply $f(\frac{r}{s})$ by s^n, then

$$0 = r^n + a_1 s^{n-1} + \cdots + a_n s^n \implies r^n = s(-a_1 r^{n-1} - \cdots - a_n s^{n-1}).$$

This means s divides r but $\gcd(r, s) = 1$. Thus it has to be s is a unit in R. Thus $rs^{-1} \in R$. □

Proposition 3.3.17. *Suppose $R \subseteq S$ is a subring, $U \subseteq R$ is a multiplicatively closed subset.*

$$\overline{R}^S[U^{-1}] = \overline{R[U^{-1}]}^{S[U^{-1}]}.$$

Proof. 1. If $\frac{r}{s} \in \overline{R}[U^{-1}]$, then $\frac{r}{s}$ is integral over $R[U^{-1}]$. Since $\frac{r}{s} \in \overline{R}[U^{-1}]$, we know $r \in \overline{R}$.

□

Definition 3.3.18. Suppose $R \subseteq S$. We say that this inclusion satisfies

1. *lying over* if for any prime $p \in R$, there exists a prime $q \in S$ such that $p = R \cap q$.
2. *going up* if for any inclusion of primes $p_0 \subseteq p_1$ of R, and prime q_0 of S s.t. $q_0 \cap R = p_0$, there exists $q_1$of S s.t. $q_0 \subseteq q_1$ and $q_1 \cap R = p_1$.
3. *going down*: for any inclusion of primes $p_0 \supseteq p_1$ of R and q_0 in S with $q_0 \cap R = p_0$, there exists prime $q_1 \in S$ s.t. $q_0 \supseteq q_1$ and $q_1 \cap R = p_1$.

Example 3.3.19. *Consider $\mathbb{Z} \subseteq \mathbb{Q}$. lying over No, going up No, going down Yes.*

Example 3.3.20. *Consider $\mathbb{C}[x] \subseteq \mathbb{C}[x, y]$. The only prime ideal of $\mathbb{C}[x]$ is $x - \alpha$ where $\alpha \in \mathbb{C}$.*

lying over Yes, going up

Show that if $R \subseteq S$ is an *integral extension* $S = \overline{R}$, then some of these properties are automatically satisfied.

Proposition 3.3.21. *Suppose $R \subseteq S$ and S is integral over R. Then*

1. *This satisfies lying over*
2. *This satisfies going up*

Trick: we are going to use certain quotients and localizations to reduce this to an easiest case.

Proof. Say we want to prove going up.

Suppose we have prime of S, q_0, and primes of R, $p_0 \subseteq p_1$, and $p_0 = q_0 \cap R$. Then define

$$R' = R/p_0 \quad S' = S/q_0.$$

There is a map from $R' \to S'$. (check it's well-defined). (omitted)

Moreover, if S is integral over R, then S' is integral over R'. □

Proof. Say $P \subseteq R$ is a prime ideal.

Define $U = R - P$, consider

$$R_P = R[U^{-1}] \subseteq S[U^{-1}] = S_P.$$

The idea is to find a prime ideal Q of S_P that contains $P[U^{-1}]$. If we can do that, then $q = Q \cap S$ is a prime of S that doesn't contain any elements of $U = R - P$, which is equivalent to saying that $q \cap R \subseteq P$. And $q = Q \cap S \supseteq P$ and so $q \cap R \supseteq P$.

So this reduces us to the case $R \subseteq S$, R is local, and we want to find an ideal of S that is prime and contains the maximal $m \subseteq R$.

Idea:

There is an ideal of S, which is mS, m the maximal in R. If we can find a maximal ideal of S containing mS, then it's prime and contains m. This is impossible iff $mS = S$.

From Nakayama's lemma, if S was finitely generated, we are done. However we don't know that.

If $mS = S$, then $\sum a_i x_i = 1$, where $a_i \in m$ and $x_i \in S$. Let $T_c S$ be the subring of S generated by $x_1 \cdots x_n$, as $T = R[x_1 \cdots x_n]$.

The claim is that T is a finitely-generated R-module and $mT = T$. Now we could use Nakayama's lemma, to get a contradiction saying that $T = 0$.

□

Example 3.3.22. *We show $R \to S$ which is integral but not finitely generated. Consider $\mathbb{Q} \subseteq \overline{\mathbb{Q}} \subseteq \mathbb{C}$. Note that $\overline{\mathbb{Q}}$ is not finitely generated.*

3.4 Nullstellensatz

If $I \subseteq \mathbb{C}[x_1 \cdots x_n]$ ideal, then $I(V(I)) = \sqrt{I}$.

Proposition 3.4.1. *Suppose R, S are domains K the fraction field of R, and that the fraction field of S, L, is integral over K. Then any prime ideal $P \subseteq S$ is either 0 or it has nontrivial intersection with R.*

Proof. P is a prime ideal of S that's not trivial, which implies that P contains some nonzero element, denoted by b. Since $b \in S$, the image $b/1 \in L$ is integral over K. Thus there exist elements

$$\frac{a_1}{u_1}, \frac{a_2}{u_2}, \ldots, \frac{a_n}{u_n}$$

such that

$$0 = b^n + \frac{a_1}{u_1} b^{n-1} + \cdots + \frac{a_n}{b_n} \in L.$$

Then we could have $\frac{a_n}{b_n} = -b$ times something in L. Multiply by some large element to clear all denominators $u_1 u_2 \cdots u_n$.

Then

$$(u_1 u_2 \cdots u_n) a_n = -b \text{ something in } S \in P.$$

Since the LHS is in R, if LHS $\neq 0$, we are done.

Since R was a domain and u_i's were in denominators, we could only have $a_n = 0$. Then the original polynomial will be

$$0 = b^n + \cdots + \frac{a_{n-1}}{u_{n-1}} b.$$

Since $b \neq 0$ by assumption and S is a domain, we could divide both sides by b and just do so iteratively.

Therefore, every prime ideal os S intersects R nontrivally. $\square$

Corrallary 3.4.2. *If S is integral over R, and $q_0 \subsetneq q_1$ proper containment of prime ideals, then*

$$q_0 \cap R \subsetneq q_1 \cap R$$

still proper.

The idea behind this is that integrality preserves dimensions.

Proof. Define $p_0 = q_0 \cap R, p_1 = q_1 \cap R$, we know $p_0 \subseteq p_1$. We still get an injective map

$$R/p_0 \to S/q_0.$$

We each have ideals p_1/p_0 and q_1/q_0, this map also preserves integrality. The fact that q_1 properly contains q_0 implies that $q_1/q_0 \neq (0)$. Since $R/p_0 \subseteq S/q_0$ are domains since they are moded out by prime ideals.

Then

$$\begin{aligned} R/p_0 \cap q_1/q_0 &= (R/R \cap q_0) \cap (q_1/q_0) \\ &= (R \cap q_1)/R \cap q_0 \\ &= (R \cap q_1) \neq R \cap q_0, \end{aligned}$$

as desired. □

Proposition 3.4.3. *Suppose $R \subseteq S$ and S is integral over R. Then S is a field iff R is a field. (Also S needs to be an integral domain).*

Proof. Suppose R is a field, $x \in S$. Since S is integral over R, we have

$$0 = x^n + a_1 x^{n-1} + \cdots + a_n, \quad a_i \in \mathbb{R}.$$

We claim that WLOG we can assume $a_n \neq 0$ because S is an integral domain. Because R is a field, a_n has an inverse.

$$\begin{aligned} a_n &= x(-x^{n-1} - a_1 x^{n-2} - \cdots - a_{n-1}) \\ 1 &= x \left(\frac{-x^{n-1} - a_1 x^{n-2} - \cdots - a_{n-1}}{a_n} \right) \end{aligned}$$

Thus x is a unit, which implies S is a field.

Other direction: Suppose S is a field. If R is not a field, then there exists some nontrivial maximal ideal of R: $(0) \subsetneq m$. By going up we get $(0) \subseteq P$, and $P \cap R = m$, which implies $P = (0)$. □

Nullstellensatz

1. maximal ideals of $\mathbb{C}[x_1, \ldots, x_n]$ are of the form $(x_1 - a_1, \ldots, x_n - a_n)$ where $a_i \in \mathbb{C}$.
2. For any ideal J, $I(V(J)) = \sqrt{J}$.

where $V(J)$ consists of all n-tuples $x = (x_1, \ldots, x_n) \in \mathbb{C}^n$ such that $f(x) = 0$ for all $f \in J$, and $I(U)$ is the ideal of all polynomials that vanish on the set U. Also $\sqrt{J}$ denotes the radical of J, which means all $r \in \mathbb{C}[x_1, \ldots, x_n]$ such that $r^n \in J$ for some $n \in \mathbb{Z}^+$.

Definition 3.4.4. A *Jacobson ring* is a ring R satisfying: any prime ideal P is an intersection of maximal ideals

$$P = \bigcap_{\alpha \in A} m_\alpha.$$

Example 3.4.5. *$\mathbb{Z}$ is a Jacobson ring. Most prime ideals are already maximal ideals so it's the intersection of itself. The only left is (0), which is the intersection of all prime ideals in $\mathbb{Z}$.*

Remark that if P is not maximal, this intersection has to be infinite because otherwise it violates prime decomposition thing.

Example 3.4.6. *Local rings are typically not Jacobson rings. If we take $\mathbb{Z}_{(2)}$, we only have 2 prime ideals (0) and (2), and (0) fails to be the intersection of maximal ideals.*

The idea is that local rings are sort of "too small" to be Jacobson rings.

Example 3.4.7. *Fields are jacobson rings. (0) is the only ideal.*

Theorem 3.4.8 (Nullstellensatz(general version))**.** *Suppose R is a Jacobson ring and S is a finitely-generated R-algebra. In other words there is a surjection from $R[x_1, \ldots, x_n]$ to S. Then*

1. *S is also a Jacobson ring*
2. *If η is any maximal ideal of S, then $m = R \cap \eta$ is a maximal ideal of R, and the map*
$$R/m \to S/\eta$$
is a finite field extension. In other words, S/η is a finite dimensional module over R/m.

Suppose R is an algebraically closed field ($\mathbb{C}$). Then R is a Jacobson ring. Note that $\mathbb{C}[x_1, \ldots, x_n]$ is a finitely generated algebra over $\mathbb{C}$.

Then Nullstellensatz tells us that

1. Every prime ideal $P \subseteq \mathbb{C}[x_1, \ldots, x_n]$ is an intersection of maximal ideals.
2. If $\eta \subseteq \mathbb{C}[x_1, \ldots, x_n]$ is maximal, then $\eta \cap \mathbb{C} = (0)$, and the map
$$\mathbb{C} \to \mathbb{C}[x_1, \ldots, x_n]/\eta$$
is a finite field extension. Then, $\mathbb{C}[x_1, \ldots, x_n]/\eta \cong \mathbb{C}$. There exists $(a_1, \ldots, a_n) \in \mathbb{C}^n$ such that $(x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n) \subseteq \eta$, which is already maximal. Thus this is not only a containment but an equality.

If J is any ideal, then

$$\sqrt{J} = \{x \in \mathbb{C}[x_1, \ldots, x_n] \mid x^n \in J \text{ some } n\} = \bigcap_{J \subseteq P} P.$$

If every prime is an intersection of maximal ideals, then

$$\bigcap_{J \subseteq P} P = \bigcap_{J \subseteq P} \bigcap_{P \subseteq m} m = \bigcap_{J \subseteq m} m,$$

where P prime and m maximal. We could rewrite the maximal ideals as

$$\begin{aligned} &= \bigcap_{J \subseteq (x_1 - a_1, \ldots, x_n - a_n)} \{f \in \mathbb{C}[x_1, \ldots, x_n] \mid f(a_1, \ldots, a_n) = 0\} \\ &= \{f \in \mathbb{C}[x_1, \ldots, x_n] \mid f(a_1, \ldots, a_n) = 0 \text{ for all } (a_1, \ldots, a_n) \in V(J)\} \end{aligned}$$

What do we know about $\mathbb{R}[x_1, \ldots, x_n]$? Take $\eta \in \mathbb{R}[x_1, \ldots, x_n]$. We have finite field extensions
$$\mathbb{R} \to \mathbb{R}[x_1, \ldots, x_n]/\eta \cong \mathbb{C} \text{ or } \mathbb{R}.$$

Then we could play the same argument which tells us that the maximal ideal looks like $(x_1 - a_1, \dots, x_n - a_n)$ where $a_i \in \mathbb{R}$.

Iso to $\mathbb{C}$ tells us that for some i, we have $x_i \mapsto \mathbb{C} - \mathbb{R}$, which gives us $x_i^2 - ax_i - b$. For any $j \neq i$, we have j goes to some complex number, which is equal to $r_j + s_j x_i$. Thus

$$\eta = (x_i^2 - ax_i - b, r_1 + s_1 x_i - x_1, r_2 + s_2 x_i - x_2, \dots, r_n + s_n x_n - x_n) = \mathbb{C}^n.$$

Every maximal ideal of $\mathbb{R}[x_1, \dots, x_n]$ is of one of the forms

1. $(x_1 - a_1, \dots, x_n - a_n)$ where $a_i \in \mathbb{C}$
2. or it corresponds to a pair of complex conjugate points

$$(a_1, \dots, a_n), (\overline{a_1}, \dots, \overline{a_n}) \in \mathbb{C}^n.$$

Then in 1 variable: $\mathbb{R}[x]$ have $(x - a)$ or $(x^2 + bx + c)$ where $b^2 - 4c < 0$ are the maximal ideals.

We'll prove that Theorem 3.4.8 implies the standard Nullstellensatz. Before that, we prove the following lemma.

Lemma 3.4.9. *Suppose $R \subseteq S$ are both domains, with fields of fractions K, L respectively. Suppose that S is a finitely generated R-algebra and L is obtained from S by inverting finitely many elements ($L = S[\frac{1}{b_1}, \dots, \frac{1}{b_k}]$).*

Then

1. *K is obtained from R by inverting finitely many elements*
2. *L is a finite extension of K. In other words, L is a finite-dimensional K-vector space, or equivalently, L is integral over K.*

Remark that inverting finitely many elements is equivalent to inverting one element because $\frac{1}{ab} = \frac{1}{a} \cdot \frac{1}{b}$.

Proof. It suffices to prove this when S is obtained from R by adding one generator.

This is because the fact that S is a finitely generated R-algebra by definition will give us

$$R \subseteq R[s_1] \subseteq R[s_1, s_2] \subseteq \cdots \subseteq R[s_1, \dots, s_n] = S.$$

If we can prove for adding one generator, then inductively we get result for R.

Suppose S is obtained from R by adding a single generator t. This means that there's a surjective homomorphism

$$R[x] \to S \quad \text{where} \quad x \mapsto t.$$

This means $S \cong R[x]/J$ for some ideal J. Then $K[t] \cong K[x]/P$ for some ideal P, but in a field we just have $P = (f(x))$ where $f(x)$ is monic or 0.

Since we can get L by inverting finitely many elements of S, we can also get L by inverting finitely many elements of $K[t] \cong K[x]/(f(x))$. If $f(x) = 0$, then $K[t] \cong K[x]$. We cannot get a field from $K[x]$ by inverting finitely many polynomials. Why? Adding $g(x)^{-1}$ only inverts prime factors of $g(x)$.

$K[x]$ has infinitely many primes. If we had finitely many primes p_i, we take $\prod p_i + 1$ and it has to be divisible by some new prime but it's not indivisible by any $p_i(x)$.

Thus $K[t] \ncong K[x]$ and we must have $K[t] \cong K[x]/(f(x))$ where $f(x)$ is monic such that $f(t) = 0$.

$$0 = t^n + \frac{a_1}{b_1} t^{n-1} + \cdots + \frac{a_n}{b_n} \quad a_i, b_i \in R.$$

Then we multiply by $\prod b_i$ to get

$$0 = c_0 t^n + c_1 t^{n-1} \cdots + c_n \quad c_i \in R, c_0 \neq 0.$$

This identity holds in $K[t] \subseteq L$ so it also holds in the ring S.

If we invert $c_n \in R$, then $R[c_0^{-1}]$ has element t satisfies a polynomial

$$0 = t^n + \frac{c_1}{c_0} t^{n-1} + \cdots + \frac{c_n}{c_0}.$$

So $R[t, c_0^{-1}]$ is integral over $R[c_0^{-1}]$. If L is formed by inverting finitely many elements of S, then $L = S[g^{-1}]$ with $g \in S \subseteq R[c_0^{-1}, t]$. Thus g satisfies a monic polynomial with coefficients in $R[c_0^{-1}]$:

$$g^m + d_1 g^{m-1} + \cdots + d_m = 0.$$

WLOG we assume $d_m \neq 0$. If we invert d_m, then g becomes a unit, so $R[c_0^{-1}, d_m^{-1}][t] = L$.

Thus L is integral over $R[c_0^{-1}, d_m^{-1}]$, since L is a field, $R[c_0^{-1}, d_m^{-1}]$ is a field and L is finite over $R[c_0^{-1}, d_m^{-1}]$. □

Proposition 3.4.10. *A ring R is a Jacobson ring iff one of the following criteria is satisfied.*

1. *Every prime P is an intersection of maximal ideals.*
2. *For any prime P and any $f \in S$, if $P[f^{-1}]$ is maximal in $R[f^{-1}]$ then P was maximal in R.*
3. *If $P \subseteq R$ is prime and $(R/P)[f^{-1}]$ is a field, then R/P is a field.*

Proof. First notice that $P[f^{-1}]$ is maximal iff $R[f^{-1}]/P[f^{-1}]$ is a field, which iff $(R/P)[f^{-1}]$ is a field, with condition from (3) we'll get R/P is a field.

We proceed with the equivalence of (1) and (2).

Suppose P is not an intersection of maximal ideals. This is true iff there exists f s.t. $f \notin P$ but $f \in m$ for any $m \supseteq P$. Iff there exists f such that in the ring $R[f^{-1}]$, $P[f^{-1}]$ is prime and all the maximal ideals containing P become $R[f^{-1}]$. Choose a maximal ideal of $R[f^{-1}]$ containing $P[f^{-1}]$. This ideal is

$Q[f^{-1}]$ for some prime $Q \supseteq P$. Then Q would be a prime ideal with $f \notin Q$, and $Q[f^{-1}]$ would be maximal even though Q was not, because all maximal ideals containing P also contain f. □

Nullstellenstaz proof. Let R be a Jacobson ring and S a finitely generated R-algebra. Suppose $Q \subseteq S$ is prime such that $(S/Q)[f^{-1}]$ is a field. We want to show S/Q is a field. Then $P = R \cap Q$ is prime and get an injective map

$$R/Q \to S/Q.$$

between domains. Thus S/Q is finitely generated over R/P. By assumption, $(S/Q)[f^{-1}]$ is a field, the lemma implies that there exists $g \in R/P$ such that $(R/P)[g^{-1}]$ is a field. and $(S/Q)[f^{-1}]$ is finite over $(R/P)[g^{-1}]$.

Since R is a Jacobson ring, $(R/P)[g^{-1}]$ is a field implies that R/P is a field. And $(S/Q)[f^{-1}]$ is finite implies S/Q is finite, which shows S/Q is a field.

If Q was maximal, then $P = R \cap Q$ is also maximal because R/P is a field. □

3.5 Graded Rings

Definition 3.5.1. A *graded ring* R is a ring with a collection of subgroups $R_n \subseteq R$ such that

1. if $f \in R_n, g \in R_m$, then $fg \in R_{n+m}$.
2. the ring R is the direct sum of the R_n: for any $f \in R$, there exists q unique $f_n \in R_n$ such that $f_n = 0$ all but finitely many n, and $\sum f_n = f$.

Example 3.5.2. *Take* $\mathbb{C}[x_0, \dots, x_n] = R$. *We could take*

$$R_n = \operatorname{span}\langle x_0^{m_0} \cdots x_n^{m_n} \mid \sum m_i = 0\rangle.$$

We say $f \in R$ is *homogeneous* of degree n iff $f \in R_n$, otherwise *inhomogenous*.

Remark 3.5.3. Usually, $n \in \mathbb{Z}$. But sometimes we have $n \in \mathbb{N}$, $n \in \mathbb{Z}/2$, or $n \in \mathbb{Z}^k, \mathbb{N}^k$. Generally, we just need to graded on some commutative monoid.

We could also take a different perspective on graded rings.

Definition 3.5.4. A *graded ring* is a collection of abelian groups (R_n) with multiplication maps

$$\cdot : R_p \times R_q \to R_{p+q},$$

and $1 \in R_0$, satisfying associativity, commutativity, unitality and distributivity.

3.6 Graded Modules

Definition 3.6.1. A *graded R-module* is an abelian gropu with subgroups (M_n) making M into a graded, and an R-module structure on M such that for $f \in R_p, m \in M_q$, we have $fm \in M_{p+q}$.

Example 3.6.2. *Say* $R = \mathbb{C}[t]$, *deg*$(t) = |t| = 1$, $M = \mathbb{C}[t]$, *and* $M_k = \langle t^{k+d}\rangle$ *for fixed* d.

More generally, if R is a graded ring and M is a graded R-module, d a number, we could define $M(d)$ to be a new graded R-module with

$$M(d)_n = M_{n+d}.$$

Definition 3.6.3. A *homogeneous ideal* in a graded ring R is

1. an ideal $I \subseteq R$ such that I is also graded where $I_p = I \cap R_p$ then $I = \oplus I_p$.
2. an ideal $I \subseteq R$ such that for any $f \in I$, if we break it into homogeneous components $f = \sum_n f_n$ then $f_n \in I$.
3. an ideal $I \subseteq R$ such that I is generated by homogeneous elements. There exists homogeneous elements $f_i \in I$ such that any element is of the form $\sum a_i f_i, a_i \in R$.
4. a graded R-submodule of the graded R-module R.

Example 3.6.4. *Some homogeneous ideals:* $(x^2, x^3 + y^3) \subseteq \mathbb{C}[x, y]$*;* $(x^2, x^2 + y^3) \subseteq \mathbb{C}[x, y]$

Example 3.6.5. *Non-homogeneous ideal:* $(x + y^2) \subseteq \mathbb{C}[x, y]$ *because* $(x + y^2)$ *in ideal but* $x \notin$ *the ideal.*

Example 3.6.6. *In* $\mathbb{C}[x_0, \ldots, x_d]$ *where* $|x_i| = 1$*. We have the "*irrelevant ideal*": the one spanned by* $(x_0 \cdots x_d)$*. In fact, every non-trivial homogeneous ideal is contained in the irrelevant ideal.*

If I have a non-trivial homogeneous ideal $f(x_0, \ldots, x_d) \in I$, then the degree-zero part of f is in I. Either all the elements in the ideal have no constant coefficient or I contains a nonzero element $a \in \mathbb{C}$, then $\frac{1}{a}a = 1 \in I$ which implies I is everything.

For the next bit, restrict to

$$R = \mathbb{C}[x_0 \cdots x_d] \quad |x_i| = 1.$$

If we have a graded R-module, M, where $(M_m)_n \in \mathbb{Z}$. Then each M_m is a $\mathbb{C}$-vector space. So it has a dimension.

If M_n is finite-dimensional for all n, we get two things:

1. Hilbert function

   $$H_M : \mathbb{Z} \to \mathbb{N} \quad H_M(s) = \dim(M_s).$$

   With shifting, we have

   $$H_{M(k)}(s) = H_M(s + k).$$

2. Poincare series.

   $$\sum H_M(s) t^s.$$

3.7 Oct 30

Prove that if M is a finitely-generated graded module over $\mathbb{C}[x_0, \dots, x_d]$, then

$$P_M(t) = \frac{f(t)}{(1-t)^{d+1}}.$$

then $f(t)$ some *Laurent polynomial*:

$$f(t) = a_k t^k + a_{k+1} t^{k+1} + \cdots + a_l t^l.$$

where $a_i \in \mathbb{Z}$, and $k \le l$ are integers.

[Proof omitted]

Consequence of the Hilbert function

The poincare series is

$$P_M(t) = \sum_n H_M(n) \cdot t^n.$$

Note that now we have

$$\begin{aligned}
P_M(t) &= \sum_{j=k}^{l} a_j t^j \frac{1}{(1-t)^{d+1}} & a_j \in \mathbb{Z} \\
&= \sum_{j=k}^{l} a_j t^j \left(\sum_{n=0}^{\infty} \binom{-d-1}{n} (-1)^n t^n \right) \\
\binom{-d-1}{n} &= \binom{d+n}{d} \\
P_M(t) &= \sum_{j=k}^{l} a_j t^j \left(\sum_{n=0}^{\infty} \binom{d+n}{d} t^n \right) \\
&= \sum_m t^m \left(\sum_{j=k}^{l} a_j \binom{d+m-j}{d} \right)
\end{aligned}$$

Notice that for large m, $\sum a_j \binom{d+m-j}{d}$ is a polynomial in m of degree d with coefficients in $\mathbb{Q}$.

Therefore $H_M(m)$ is a polynomial in M for sufficiently large m. (when $m \ge l$).

3.8 filtration

What is nice about power series rings?

Suppose M is a module over a ring R. A *decreasing filtration* on M is a sequence of submodules

$$M = M^0 \supseteq M^1 \supseteq M^2 \supseteq \cdots.$$

Example 3.8.1. *The trivial filtration is $M^n = M/$*

Example 3.8.2. *Say $J \subseteq R$ is an ideal. Then*

$$R \supseteq J \supseteq J^2 \supseteq J^3 \supseteq \cdots .$$

This is the J-adic filtration of R.

Example 3.8.3. *Look at $\mathbb{C}[x]$, and let $J = (x)$, we could have*

$$\mathbb{C}[x] \supseteq (x) \supseteq (x^2) \supseteq (x^3) \supseteq \cdots .$$

Example 3.8.4. *Look at $\mathbb{Z}$, and let $J = (p)$ where p prime. Then*

$$\mathbb{Z} \supseteq (p) \supseteq (p^2) \supseteq \cdots .$$

This is p-adic filtration of $\mathbb{Z}$.

Associated to a filtration

$$M^0 \supseteq M^1 \supseteq \cdots .$$

we have

1. associated graded $gr(M)$ where

$$gr^k(M) = M^k/M^{k+1}.$$

2. To any element $m \in M$, we could take n to be the supremum of k such that $m \in M^k$. Then the *initial form* of m:

$$[m] \in gr^n(M).$$

since $m \in M^n$ and $m \notin M^{n+1}$, the initial form $[m]$ is not zero. Therefore the initial form and initial degree are well-defined for all $m \notin M^0 \cap M^1 \cap \cdots$.

3. We say this filtration on M is *separated* if

$$\cap_{k=0}^{\infty} M^k = (0).$$

4. Associated to M we also get a sequence of quotients

$$0 = M/M^0 \twoheadleftarrow M/M^1 \twoheadleftarrow M/M^2 \twoheadleftarrow \cdots .$$

Definition 3.8.5. Suppose we have a tower

$$\to \cdots \to S_2 \to S_1 \to S_0.$$

of sets and functions. The *limit*

$$\lim_k S_k$$

is the set

$$\{(a_0, a_1, a_2, \ldots) \in S_0 \times S_1 \times S_2 \times \cdots \mid \forall n \geq 0, f_n(a_{n+1}) = a_n\}.$$

Example 3.8.6. *If*
$$\cdots \subseteq S_2 \subseteq S_1 \subseteq S_0,$$
then
$$\lim_k S_k \cong \bigcap_{k=0}^{\infty} S_k.$$

Proposition 3.8.7. *If S_k are groups and F_n are group homomorphisms, then $\lim_k S_k$ is also a group.*

Proof. Standard algebra proof. At the end we have
$$\lim_k S_k \subseteq \prod S_k$$
is a subgroup. □

Example 3.8.8. *For any ring R and ideal $J \subseteq R$, we get a tower*
$$\to \cdots \to R/J^2 \to R/J^1 \to R/J^0$$
of rings and ring homomorphisms. So we get a limit:
$$\lim_k R/J^k = R_J^\wedge.$$

Remark 3.8.9. If we take a "subsequence" of S_k then the limit is the same.

Example 3.8.10. *Consider $\mathbb{C}[x]/(x^n)$. Then*
$$\mathbb{C}[x]_{(x)}^\wedge \cong \lim_k \mathbb{C}[x]/(x^k) \cong \mathbb{C}[[x]],$$
the power series ring.

WHat's the point of power series?

Give solutions to equations that didn't have them before. For example, if we have $y^2 = 1 + x$ and solve for y, this has no solutions in $\mathbb{C}[x]$. But it has approximate solutions. For example, $y = 1 + \frac{x}{2}$ will give $1 + x + \frac{x^2}{4}$ which is pretty close to $1 + x$.

We could do the induction to add terms to y to get a pretty close solution. This technique relies on a notion of things being "close" to each other. In $\mathbb{C}[[x]]$ and $\mathbb{C}[x]$, we say $1 + x + \frac{x^2}{4}$ is close to $1 + x$ because $\frac{x^2}{4}$ is small.

Consider
$$R \supseteq J \supseteq J^2 \supseteq J^3 \cdots.$$

Definition 3.8.11. Suppose R is a ring $J \subseteq R$ an ideal, M an R-module with a filtration
$$M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots.$$
We say this filtration is *compatible* with J if
$$J \cdot M_m \subseteq M_{n+1}.$$

Example 3.8.12. *If M any module,*

$$M \supseteq JM \supseteq J^2M \supseteq \cdots$$

is the J-adic filtration on M and it's compatible with J.

Example 3.8.13. *If $I \supseteq J$ then the I-adic filtration on M is compatible with the J adic one.*

Proof. We have

$$M \supseteq IM \supseteq I^2M \supseteq \cdots .$$

Then

$$J(I^kM) \subseteq I(I^kM) = I^{k+1}M.$$

$\square$

Proposition 3.8.14. *If M has a filtration compatible with J, then $gr(M)$ (graded abelian group) is a module over $gr_J(R) \oplus J^n/J^{n+1}$.*

The problem is that:

Mostly for an R-module, M, we are interested in the J-adic filtration

$$M \supseteq JM \supseteq J^2M \supseteq \cdots .$$

and the associated J-adic completion is defined as

$$\lim_k (M/J^kM) = M_J^\wedge.$$

If $N \subseteq M$ is a submodule, then I have a J-adic filtration on N.

Whenever $N \subseteq M$ is a submodule, and M has a filtration, then N gets a natural filtration:

$$M = M_0 \supseteq M_1 \supseteq \cdots \quad N_k := M_k \cap N.$$

This filtration has the property that

$$gr(N) \subseteq gr(M).$$

However, for J-adic ones, we have two choices:

$$\{J^kN\} \qquad \{N \cap J^kM\}.$$

Definition 3.8.15. A filtration on M that is compatible with J is called *stable* if for all $n \geq N$, $JM_n = M_{n+1}$.

Proposition 3.8.16 (The Artin-Rees Lemma)**.** *If R is Noetherian, $J \subseteq R$ an ideal, M is a finitely-generated module with a J stable filtration, and $M' \subseteq M$ a submodule. Then the filtration*

$$(M' \cap M_k)$$

is also a stable filtration of M'.

Proposition 3.8.17. *If we have a J-stable filtration on M then*

$$\lim_k M/M_k \cong M_J^\wedge := \lim_k (M/J^k M).$$

Example 3.8.18. *If M is a finitely generated module and $M' \subseteq M$ a submodule, then*

$$\lim_k (M'/J^k M \cap M') \cong (M')_J^\wedge.$$

Example 3.8.19. *Say $R = \mathbb{Z}, J = (2).M = \mathbb{Z}^2$. Then this has 2-adic filtration*

$$M_k = \{(2^k a, 2^k b) \mid a, b \in \mathbb{Z}\}.$$

Let

$$M' = \{(a, b) \mid a \text{ is even}\} = \{(2c, d) \mid c, d \in \mathbb{Z}\}.$$

There are 2 filtrations on M:

1. *standard 2-adic filtration*

$$(M')_k = \{(2^{k+1} c, 2^k d) \mid c, d \in \mathbb{Z}\}.$$

2. *filtration inherited from M.*

$$M' \cap M_k = \{(2^k a, 2^k b) \mid a, b \in \mathbb{Z}\} \text{ for } k \geq 1 = M_k.$$

More generally

If we have a J-stable filtration on a module N, then

$$N_k \supseteq J^k N_0.$$

and J-stability says that for some N,

$$JN_n = N_{n+1} \text{ for } n \geq N,$$

which tells us

$$J^k N_n = N_{n+k}.$$

Proposition 3.8.20. *If M is a finitely generated module over a Noetherian ring and $N \subseteq M$ is a submodule, then $N_J^\wedge$ is isomorphic to a submodule of $M_J^\wedge$.*

Proposition 3.8.21. *If the filtration on M is compatible with J (meaning: $JM_k \subseteq M_{k+1}$), the $gr(M)$ is a graded module over $gr(R)$.*

Proof. We want to know the multiplication

$$(r_0, r_1, r_2, \ldots) \cdot (m_0, m_1, m_2, \ldots) \quad r_k \in J^k/J^{k+1}, m_k \in M_k/M_{k+1}.$$

Suppose $[r] \in J^k/J^{k+1}$ and $[m] \in M_j/M_{j+1}$, we want to define

$$[r] \cdot [m] = [rm] \in M_{j+k}/M_{j+k+1}.$$

Then we need to ask ourselves that

1. Is $rm \in M_{j+k}$?
2. Well-defined?

$\square$

Definition 3.8.22. Suppose R is a ring, and $J \subseteq R$ an ideal, the *Rees algebra* or *Blow up algebra* is a graded ring $B_J R$ with

$$(B_J R)_k = J^k.$$

It is a subring of $R[t]$ if we think like

$$R \oplus Jt \oplus J^2t^2 \oplus \cdots$$

which is contained in

$$R \oplus Rt \oplus Rt^2 \oplus \cdots.$$

Proposition 3.8.23. *If J is a finitely generated ideal, then $B_J R$ is a finitely generated R-algebra.*

Proof. If $J = \langle x_1, \ldots, x_n rangle$. Then we get elements $y_k = x_k t$ which are in $Jt \subseteq B_J R$. Any element in $B_J R$ is of the form

$$(r_0, r_1, r_2, \ldots) \quad \text{where} \quad r_k \in J^n.$$

Then $r_k \in J^k$ implies that

$$r_k = \sum a_{m_1 \cdots m_n} x_1^{m_1} \cdots x_n^{m_n}, \sum m_i = k.$$

Thus we could multiply r_k by t^k and get

$$r_k t^k = \sum a_{m_1 \cdots m_n} y_1^{m_1} \cdots y_n^{m_n}.$$

So $r_k t^k$ is in $R[y_1 \cdots y_n]$ and thus $\sum r_k t^k$ is in $R[y_1 \cdots y_n]$. $\square$

We like blowup algebra because it has two homomorphism, one to R by setting $t = 0$, the other goes to $gr(R) = R/J \oplus J/J^2 \oplus + \cdots$.

Suppose M is an R-module with a filtration $\mathfrak{J}$

$$M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots.$$

compatible with $J : JM_n \subseteq M_{n+1}$.

We define

$$B_{\mathfrak{J}} M = M_0 \oplus M_1 \oplus M_2 \oplus \cdots \subseteq M[t].$$

where

$$B_{\mathfrak{J}} M = \left\{ \sum a_i t^i \mid a_i \in M_i \right\}.$$

Proposition 3.8.24. *$B_{\mathfrak{J}} M$ is a module over $B_J R$.*

Proof. Writing things down using definition kind of proof. $\square$

Proposition 3.8.25. *Suppose that M is a finitely generated R-module with a compatible filtration $\mathfrak{J}$, compatible with J, R is Noetherian. Then this filtration is J-stable iff $B_{\mathfrak{J}}M$ is a finitely generated module over $B_J M$.*

Before we prove that, we observe that if we assume the proposition to be true we get the Artin-Rees Lemma.

Corrallary 3.8.26 (Artin-Rees Lemma)**.**

Proof. Suppose M is a finitely-generated R-module, $J \subseteq R$ an ideal, R is Noetherian and M has a J-stable filtration.

$$M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots .$$

N is a submodule of M. We want to show $N_k = N \cap M_k$ is a J-stable. Since R is Noetherian,

- N is also finitely-generated as an R-module.
- Proposition we are assuming: we are assuming that $B_{\mathfrak{J}}M$ is a finitely generated $B_J R$-module, and we want to show $B_{\mathfrak{J}}N$ is a finitely-generated $B_J R$-module.

Since $B_J R$ is a finitely-generated algebra of R.(R Noetherian implies J is fin-gen implies $B_J R = R[y_1 \cdots y_n]$ implies $B_J R$ is Noetherian). Thus $B_{\mathfrak{J}}N$ is also finitely generated. ☐

Proof of proposition. First $\implies$.

Note that $B_{\mathfrak{J}}M$ is finitely generated over $B_J R$ iff there exists finitely many elements in $M_0, M_1, M_2 \cdots$ such that $B_{\mathfrak{J}}M$ is generated by these. This is true iff there exists n_0 such that $B_{\mathfrak{J}}M$ is generated over $B_J R$ by $M_0 \oplus M_1 \oplus \cdots \oplus M_{n_0}$. This is the same as

$$B_{\mathfrak{J}}M = \left(R \oplus J \oplus J^2 \oplus \cdots\right) \cdot (M_0 \oplus \cdots \oplus M_{n_0}) .$$

An arbitrary element inside looks like

$$\sum_n \left(\sum_{p+q=n} r_k a_p\right) t^n \quad r_k \in J^k, a_p \in M_0 \cdots M_{n_0}.$$

Since it's stable, we know

$$\left(\sum_{p+q=n} r_k a_p\right) \in J^{n-p} M_p.$$

This iff for all $n \geq n_0$, any element in M_n is $b_n t^n = \sum r_k a_j$, which shows $M_n = J^{n-n_0} M_{n_0}$. ☐

Remark 3.8.27. If $N \subseteq M$ is a submodule, M finitely generated, and R is Noetherian, $N_J^\wedge \to M_J^\wedge$ is injective, so "$N_J^\wedge \subseteq M_J^\wedge$".

Theorem 3.8.28 (Krull intersection theorem)**.** *Suppose R is Noetherian and either*

- *R is a domain, or*
- *R is local*

If $J \subseteq R$ is any ideal, then

$$\bigcap_{k=0}^{\infty} J^k = 0.$$

None-Example 3.8.29. *Let $R = \mathbb{Z} \times \mathbb{Z}$. Then the ideal $J = ((0,1)) = 0 \times \mathbb{Z}$ satisfies $J^2 = J$ since $(0,1)$ is idempotent.*

None-Example 3.8.30. *Let R be the ring of continuous functions $\mathbb{R} \to \mathbb{R}$. Let J be the ideal containing functions $f(0) = 0$. Then $J^2 = J$.*

4 Flat Families

free R-module.

4.1 Tor

4.2 Homological algebra

Definition 4.2.1. Suppose M is a module over R. A *differential* on M is a map $d : M \to M$ satisfying $d^2 = 0$. In this case, there are submodules $M \supseteq ker(d) \supseteq Im(d)$. The associated *homology* $\mathcal{H}(M)$ is $ker(d)/Im(d)$.

Definition 4.2.2. A *chain complex* is a graded R-module such that d decreases grading by 1. Specifically

$$M = \oplus M_n \qquad d(M_n) \subseteq M_{n-1}.$$

or

$$\to \cdots \to M_2 \to M_1 \to M_0.$$

by d.

Note that $\mathcal{H}(M) = 0$ iff $ker(d) = Im(d)$. In the graded case, it's equivalent to say that it's an exact sequence.

Definition 4.2.3. A *cochain complex* is a graded R-module such that d increases grading by 1. In this case we write

$$M^0 \to M^1 \to M^2 \to .$$

Remark 4.2.4. Chain complex is equivalent data to cochain complex by taking $M_n \leftrightarrow M^{-n}$.

Often when we say chain complex or cochain complex we implicitly are assuming a "boundary" (where the chain complex stops).

Remark 4.2.5. We can have a graded module over a graded ring with d.

Suppose we have two R-modules with differentials. A *map of differential modules* is a map of R-modules $f : M \to N$ satisfying $f(dx) = d(fx)$. *Isomorphism* is a map which is invertible. A *map* of (co)chain complexes is a map of graded modules that is also a map of differential modules.

Proposition 4.2.6. *A map $f : M \to N$ of differential modules induces a map $\mathcal{H}(M) \to \mathcal{H}(N)$.*

Proof. Take $[x] \in \mathcal{H}(M)ker(d)/Im(d)$ where $d_M(x) = 0$. Then

1. $d_N(fx) = f(d_M x) = f(0) = 0$, so $[fx] \in \mathcal{H}(N)$.
2. well-defined: If $[x_1] = [x_2]$, then $x_1 - x_2 = d_M y$, then $f(x_1 - x_2) = f(d_M y) = d_N(fy)$ which implies $[fx_1] = [fx_2]$.
3. check preserves addition and multiplication by scalars.

□

Proposition 4.2.7. *If M is a chain complex then $\mathcal{H}(M)$ is also a graded module. If $f : M \to N$ is a map of chain complexes, then $\mathcal{H}(M) \to \mathcal{H}(N)$ is also a map of graded modules.*

Sketch of proof.

$$\begin{aligned} M &= \left\{ \sum m_k \mid m_k \in M_k \right\} \\ ker(d) &= \left\{ \sum m_k \mid d\left(\sum m_k\right) = \sum d\left(m_k\right) = 0 \right\} \\ &= \left\{ (m_k) \mid d(m_k) = 0 \forall k \right\}. \end{aligned}$$

□

Definition 4.2.8. For an R-module M, a *free resolution* is an exact sequence

$$\cdots F_2 \to F_1 \to F_0 \to M \to 0,$$

such that each F_k is a free R-module.

From a free resolution, we get a chain complex

$$\cdots F_2 \to F_1 \to F_0 \to 0.$$

Then

$$\mathcal{H}_k(F) = \begin{cases} 0, & k > 0 \\ M, & k = 0 \end{cases}.$$

And $\mathcal{H}_k(F) \to \mathcal{H}_k(M)$ is an isomorphism.

Remark 4.2.9. A free resolution effectively replaces the chain complex

$$\cdots 0 \to 0 \to M \to 0$$

of “bad” modules with a chain complex

$$\cdots \to F_2 \to F_1 \to F_0 \to 0$$

of “good” modules with the same homology.

Definition 4.2.10. A *chain homotopy* consists of the following. Suppose we have differential modules M, N and two maps $f, g : M \to N$ of differential modules. A chain homotopy between them is a map of R-modules $h : M \to N$ satisfying

$$d_N h(x) + h d_M x = gx - fx \quad \text{for all } x \in M.$$

If M, N are graded (chain complexes), we take $h(M_n) \subseteq N_{n+1}$.

Proposition 4.2.11. *If there exists a chain homotopy from f to g then the two homology maps $\mathcal{H}M \to \mathcal{H}N$ are equal.*

Proof. Say $[x] \in \mathcal{H}(M) = ker(d_M)/Im(d_M)$, then

$$d_N h(x) = g(x) - f(x).$$

Thus $[g(x)] = [f(x)] \in ker(d_N)/Im(d_N) = \mathcal{H}(N)$. □

4.3 Fundamental Lemma of Homological Algebra

Suppose $f : M \to N$ is a map of R-module and

$$\cdots \to F_1 \to F_0 \to M \to 0$$

is a free resolution of M where F_i are free sequences exact. F_i are modules of syzygys. And

$$\cdots \to G_1 \to G_0 \to N \to 0$$

is a free resolution of N. Then

1. there exists a map of chain complexes. There exists $g_i : F_i \to G_i$ maps of R-modules satisfying $d \circ g_{i+1} = g_i \circ d$ and $d \circ g_0 = f \circ d$.
2. If we have two such extensions of f to maps of chain complexes, denoted by g, g'. Then g and g' are homotopic. There exists maps $h_i : F_i \to G_{i+1}$ satisfying $h_{i-1} \circ d + d \circ h_i = g - g'$.

4.4 Property of Free Modules

Suppose F is a free R-module and $p : N \to P$ is a surjective map of R-modules. Then for any $g : F \to P$ there exists a map $\tilde{g} : F \to N$ such that $p \circ \tilde{g} = g$.

A *projective* R-module F satisfies: suppose $p : N \to P$ is a surjective map of R-modules. Then for any $g : F \to P$ there exists a map $\tilde{g} : F \to N$ such that $p \circ \tilde{g} = g$.

Therefore we've shown free modules are projective, the other way around is not true.

Example 4.4.1. *In $\mathbb{Z}[\sqrt{5}]$, the module $(2, 1 + \sqrt{5})$ is projective but not free.*

Remark 4.4.2. What have we define? TFAE

- F is projective
- iff whenever $p : N \to P$ is onto every function $F \to P$ lifts to a function $F \to N$

- iff whenever $N \to P$ is onto,

$$\mathrm{Hom}_R(F, N) \to \mathrm{Hom}_R(F, P)$$

  is onto.

- whenever $N \to P \to 0$ is exact,

$$\mathrm{Hom}_R(F, N) \to \mathrm{Hom}_R(F, P) \to 0$$

  is exact.

Proposition 4.4.3. *A module F is projective iff for any short exact sequence*

$$0 \to N' \to N \to N'' \to 0,$$

the sequence

$$0 \to \mathrm{Hom}_R(F, N') \to \mathrm{Hom}_R(F, N) \to \mathrm{Hom}_R(F, N'') \to 0$$

is exact.

Start proving the fundamental lemma of homological algebra.

Proof. For point 1. We inductively define maps $g_i : F_i \to G_i$. The existence of g_0 is true by projectivity of F_0. For g_1, recall that d lands in $ker(d)$ since $d^2 = 0$. Thus we have $d : G_1 \to ker(d)$ is onto, and by projectivity we have g_1. Notice that for this part we only used F_i are free and $sequence G_1 \to G_0 \to \cdots$ is exact.

For point 2. Suppose we have two chain maps $g_i, g_i' : F_i \to G_i$, and we want to prove these are chain homotopic, i.e. we want to find h_i. We do so by first have k_0 from $g_0 - g_0'$, and then have a map $G_1 \to ker(d)$ be onto, then by surjectivity. □

4.5 derived functor

Say we have the category Mod_R of modules over R and R-linear maps. We have various functors that take in Rmodules and produce new ones. For example

$$M \mapsto M \otimes_R N, \quad M \mapsto \mathrm{Hom}_R(N, M), \quad M \mapsto \mathrm{Hom}_R(M, N).$$

THe first two are covariant and and the last is contervariant.

Problems with exactness: none of these generally preserve exact sequences. There are special cases where exactness is preserved.

Say we have $F : Mod_R \to Mod_R$ and

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

an exact sequence. Apply F. We have

$$F(0) \to F(M') \to F(M) \to F(M'') \to F(0)$$

where $F(i) : F(M') \to F(M)$ and $F(j) : F(M) \to F(M'')$. This could fail to be a short exact sequence in several situations:

1. $F(0) \neq 0$, where 0 the R-module.
2. $F(j) \circ F(i) = F(j \circ i) = F(0) \neq 0$, where 0 the map of R-module.

Definition 4.5.1. A functor $F : Mod_R \to Mod_R$ is *additive* if for any $f, g : M \to N$ we have $F(f) + F(g) = F(f + g)$. F is*R-linear* if $F(rf) = rF(f)$.

Proposition 4.5.2. *If F is additive, then $F(0) \cong 0$ and $F(0) = 0$, where the first 0 is the R-module and the second the function.*

Proof. Consider the zero map

$$0 : M \to N,$$

satisfying $0 + 0 = 0$ as functions. Apply F. We have $F(0+0) = F(0) + F(0) = F(0)$ and thus $F(0) = 0$. Then consider the zero module 0. Then $F(0) = F(id_0)$, since $0 = F(0)$ and $F(id_0) = id_{F(0)}$, and thus $F(0) = \{0\}$. □

Definition 4.5.3. A short exact sequence

$$0 \to M' \to M \to M'' \to 0 \text{ where } i : M' \to M, J : M \to M''$$

is *split* if any of the following equivalent statements hold.

1. There exists a map of R-module $s : M'' \to M$ such that

$$j \circ s = id_{M''}.$$

2. There exists a map $r : M \to M'$ such that

$$r \circ i = id_{M'}.$$

3. There exists an isomorphism $\phi : M \to M' \oplus M''$ such that

$$\phi(i(x)) = (x, 0) \text{ for } x \in M',$$

and

$$j(\phi^{-1}(x, y)) = y \text{ for } y \in M''.$$

Proposition 4.5.4. *If F is an additive functor then F automatically preserves split exact sequences.*

Definition 4.5.5. *Derived functors* take a functor F with bad exactness properties and replace it with a sequence of functors with good exactness properties.

Definition 4.5.6. Suppose F is some additive functor Mod_R. We define the *left-derived functor* of F in the following way. Given a left R-module M, we define $(L_k F)M$ as follows :

1. choose a free resolution

$$\cdots \to P_2 \to P_1 \to P_0 \to M \to 0.$$

2. throw away M to have a chain complex

$$\cdots \to P_2 \to P_1 \to P_0 \to 0.$$

3. Apply F level by level

$$\cdots \to F(P_2) \to F(P_1) \to F(P_0) \to 0,$$

which is still a chain complex.

4. Take homology.

$$\cdots \mathcal{H}_3 \quad \mathcal{H}_2 \quad \mathcal{H}_1 \quad \mathcal{H}_0.$$

We call $\mathcal{H}_i$ a $(L_iF)(M)$.

Proposition 4.5.7. *1. If F was right-exact, then $L_0F \cong F$.*

2. We can make the L_kF well-defined and functorial.

3. If we have a short exact sequence

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

Then we get a long exact sequence

$$\cdots \to (L_1F)(M') \to (L_1F)(M) \to (L_1F)(M'') \to (L_0F)(M') \to (L_0F)(M) \to (L_0F)(M'') \to 0.$$

4. The L_kF are additive. If F was R-linear then L_kF are R-linear.

5. $(L_kF)(M) = 0$ if M is free $k > 0$.

Example 4.5.8. *If $F(M) = M \otimes_R N$, then $(L_kF)(M) = Tor_k^R(M,N)$.*

Why do we get this and how does it work?

If we choose two free resolutions, why do we get the same answer?

Proposition 4.5.9. *For any $f : M \to N$ and resolutions $P_. \to M$ and $Q_. \to N$, there is a well-defined map*

$$f_* : (L_kF)(M, P.) \to (L_kF)(W, Q_.).$$

Proposition 4.5.10. *1. Given $\mathrm{id} : M \to M$, then*

$$id_* : (L_kF)(M, P) \to (L_kF)(M, P)$$

is the identity map.

2.

$$(g \circ f)_* = g_* \circ f_*.$$

3.

$$(f + g)_* = (f)_* + (g)_*.$$

4.

$$r(f_*) = (rf)_* \quad r \in R.$$

Proposition 4.5.11. *Derived functors are independent of the resolution chosen. In other words*

$$(L_kF)(M,P) \cong (L_kF)(M,Q).$$

Proposition 4.5.12. *L_kF is a functor.*

Properties of the derived functor of F:

1. If M is a free module, then

$$(L_0F)(M) \cong F(M) \qquad (L_kF)(M) \cong 0 \quad k > 0.$$

2. If

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

   is an exact sequence then there exits a long exact sequence

$$\cdots \to L_1F(M') \to L_1F(M) \to L_1F(M'') \to L_0F(M') \to L_0F(M) \to L_0F(M'') \to 0.$$

Lemma 4.5.13 (Horseshoe Lemma)**.** *Given*

$$\begin{tikzcd}
 & & & 0 \arrow[d] & \\
\cdots \arrow[r] & P_1' \arrow[r] & P_0' \arrow[r] & A' \arrow[r] \arrow[d] & 0 \\
 & & & A \arrow[d] & \\
\cdots \arrow[r] & P_1'' \arrow[r] & P_0'' \arrow[r] & A'' \arrow[r] \arrow[d] & 0 \\
 & & & 0 &
\end{tikzcd}$$

where the column is exact and the rows are resolutions, then it could be completed into a commutative diagram

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
\cdots \arrow[r] & P_1' \arrow[r] \arrow[d] & P_0' \arrow[r] \arrow[d] & A' \arrow[r] \arrow[d] & 0 \\
\cdots \arrow[r] & P_1 \arrow[r] \arrow[d] & P_0 \arrow[r] \arrow[d] & A \arrow[r] \arrow[d] & 0 \\
\cdots \arrow[r] & P_1'' \arrow[r] \arrow[d] & P_0'' \arrow[r] \arrow[d] & A'' \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

Once we have the Horseshoe lemma, we could apply F on the diagram.