Comm & Hom

Yuxuan Sun

October 16, 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 $J \subset \mathbb{C}[x_1, \ldots, x_n]$ 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.

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

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. $$\mathrm{Hom}_R\left(\oplus_{i\in I} M_i, N\right) \cong \prod_{i\in I} \mathrm{Hom}_R(M_i, N).$$
   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.

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

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.
$$(\oplus M_i) \otimes_R N \cong \oplus (M_i \otimes_R N).$$

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
$$\frac{m}{u} \mapsto \frac{1}{u} \otimes m \quad \frac{rm}{u} \leftarrow\!\shortmid \frac{r}{u} \otimes m.$$
□

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 $a_0 + a_1x + a_2x^2 + \cdots + a_nx^n, a_n \neq 0, a_i \in R$, 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.

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

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*

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

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 $I \subseteq R$ 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 $r \in R$.*

local rings have unique maximal ideal.

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

Theorem 3.3.4. *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 3.3.5. An *idempotent* in R is an element $e \in R, e^2 = e$.

Proposition 3.3.6. *If $e \in R$ is idempotent, then $R \cong R/(e) \times R/(1-e)$.*

Proposition 3.3.7. *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 3.3.8 (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 3.3.9. 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 3.3.10 (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 3.3.11. 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 3.3.12. *$\overline{R}$ is a ring containing R.*

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

Definition 3.3.13. 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 3.3.14. *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 3.3.15. *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 3.3.16. *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 3.3.17. 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 3.3.18. *Consider $\mathbb{Z} \subseteq \mathbb{Q}$. lying over No, going up No, going down Yes.*

Example 3.3.19. *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 3.3.20. *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'. □

How do we usually solve these types of lying-over problems? Localizations.