MATH 470-3 Commutative Algebra

Chi Li

Contents

If you see any typos, please email chili2025@u.northwestern.edu.

0 Syllabus

Topics

1. Commutative algebra, linear algebra, tensor algebra.
2. Rings, ideals, modules, localization, Zariski topology/spec, tesor products.
3. Further topics include: Noether's normalization, going up and going down, completions of rings, dimension theory, Zariski's main thoerem, Nullstellensatz.
4. Representation theory, noncommutative algebra.

References

1. Atiyah and Macdonald (lots of problems here but pretty terse)
2. Milne's notes on commutative algebra

Both are available for free online.

Grades

- Midterm: 20%
- Final: 20%
- Problemsets (fortnightly): 60%

Ask for hints on the problemsets only for the first 9 days. Office hours Saturday 1-2 on zoom. Further OH TBD.

1

Notation

All rings are commutative, usually denoted R, A, B and have multiplicative identity 1.
I, J, M, P denote ideals. M ideals are maximal and P ideals are prime.
Modules are denoted by M, N.

Definition 1.1 (Prime Ideal)

An ideal P is prime if

$$xy \in P \implies x \in P \text{ or } y \in P.$$

Definition 1.2 (Maximal Ideal)

An ideal M is maximal if $M \subset I \implies I = R$.

Proposition 1.3

Maximal ideals are prime

Proof. We can show something stronger. We have equivalent definitions that

- An ideal I is prime iff R/I is an integral domain.
- An ideal I is maximal iff R/I is a field.

A field is an integral domain so we are done. ✿

Definition 1.4 (Special elements of ring)

Let $x \in R$. Then x is

1. A unit, if there is $y \in R$ such that $xy = 1$.
2. A zero divisor, if there is $y \in R \backslash 0$ such that $xy = 0$.
3. Nilpotent, if there is some n such that $x^n = 0$.

Remark. *The set of units form a multiplcative set. The complement of units need not form an ideal, for instance $\mathbb{Z}/6$. Similarly, the set of zero divisors need not form an ideal.*

Proposition 1.5

The set of nilpotent elements form an ideal. We call this the nilradical of R and denote it $n(R)$.

Proof. 0 is nilpotent, $n(R)$ is nonempty. Let $x^n = 0, y^m = 0$. Then $(x+y)^{n+m} = 0 = (rx)^n$ for any $r \in R$. So the nilradical is closed under addition and multiplcation. ✿

Proposition 1.6

We have

$$n(R/n(R)) = \{0\}.$$

Proof. Let $[a]$ be nilpotent in $R/n(R)$. Then there exists k such that $a^k \in n(R)$. But then this means a is nilpotent in R too. So $[a] = 0$. ✿

Definition 1.7 (Reduced ring)

R is reduced if $n(R)$ is trivial.

Similarly we can define nilradicals based on other ideals.

Definition 1.8 (Nilradical)

Let $I \subseteq R$ be an ideal. Then the nilradical of I is

$$n(I) \overset{\text{def}}{=} \{r \in R : \exists n \text{ s.t. } r^n \in I\}.$$

Proposition 1.9

- $n(I)$ is an ideal.
- $n(R/n(I))$ is trivial.

Proof. The same as above.

2

Theorem 2.1

$$n(R) = \bigcap_{\text{prime ideals } P \subseteq R} P.$$

Proof. The inclusion $\subseteq$ is easy. Let $r \in R$ be nilpotentent and P be a prime ideal. Then $r^n = 0 \in P$. Backwards induction on n gives that $r \in P$.

We now prove the opposite inclusion. Let $r \in R$ be not nilpotent. Let S be the set of all ideals of R that do not contain any power of r. We give this a partial order by inclusion. This is non-empty as the trivial ideal satisfies this condition. Every ascending chain is bounded by the union of the ideals, and the union of the ideals in an ascending chain is an ideal that does not contain any power of r. So we apply Zorn's lemma to obtain a maximal element of the set P. We want to show that P is prime.

Suppose not, then there is $xy \in P$ but $x \notin P$ and $y \notin P$. But now we have ideals (P, x) and (P, y) that both contain some power of r, say r^n and r^m respectively. We have

$$r^n = p_1 + a_1 x, r^m = p_2 + a_2 y.$$

But now $r^{n+m} = (p_1 + a_1 x)(p_2 + a_2 y) \in P$ giving a contradiction.

Definition 2.2

$S \subseteq R$ is multiplcatively closed $s_1, s_2 \in S \implies s_1 s_2 \in S$.

Theorem 2.3

Let S be multiplcatively closed. Then there is a prime ideal that is disjoint from S.

Proof. Same as above. But now set the set of ideals to be those that are disjoint from S, and find the maximal element. The previous example for the nilradical proof is for the multiplcatively closed set $\{r, r^2, r^3 ...\}$. ✿

Remark. *This ideal need not be maximal. For instance, take the ring of integers and S be $\mathbb{Z} - \{0\}$. The only prime ideal disjoint from this is the zero ideal. Another example would be $\mathbb{C}[x, y]$. By Hilbert's Nullstellensatz the only maximal ideals are in the form $(x-a, y-b)$. The set of polynomials*

$$\{f \in \mathbb{C}[x, y] - \{0\} : f(x, y) = g_1(x)g_2(y), g_1, g_2 \in \mathbb{C}[t]\}$$

intersects every maximal ideal. A non trivial prime ideal that does not intersect S would be $(x - y^2)$ which does not split into products of x and y.

We now consider the intersection of all maximal ideals.

Definition 2.4 (Jacobson Radical)

The Jacobson radical of R is denoted $J(R)$ and is the intersection of all maximal ideals in R.

Theorem 2.5

$J(R)$ consists of exactly the elements $x \in R$ such that $1 - xy$ is a unit for all $y \in R$.

Proof. For the $\subseteq$ direction, let $1-xy$ be not a unit. Then there is a maximal ideal containing $1-xy$. This ideal cannot contain x, as this would be the ideal would also contain $(1 - xy) + x(y) = 1$. Therefore x is not in the Jacobson radical.

For the other direction, suppose that x is not contained in a maximal ideal m. Then we would have $(m, x) = R$, so that $m + xy = 1$ for some y, then $1 - xy = m$ is not a unit. ✿

Definition 2.6 (Local Ring)

R is called a local ring if it contains exactly one maximal ideal.

Example 2.7

- A field is a local ring.
- Let P be a prime ideal that does not contain 1. Take its complement S, which is a multiplcatively closed set. The localization $S^{-1}R$ is a local ring. This is because set of non-units in this ring are in the form $\frac{p}{s}$ for $p \in P, s \in S$, the others $\frac{s_1}{s_2}$ are invertible.

Lemma 2.8

R is a local ring iff there is an ideal M such that $R \backslash M$ is the set of all units in R.

Proof. The backwards direction is obvious. This M is maximal, and contains all other ideals except for R.

For the forwards direct, suppose not, then consider a maximal ideal. Take an element from its complement that is not a unit and consider a maximal ideal containing it. ✿

Lemma 2.9

Let $M \subset R$ be maximal. Then if $1 + m$ is a unit for every $m \in M$, R is local.

Proof. We have R/M is a field. Therefore, for every $r \in M^c$. We have y such that $ry = 1 + m$ for some $m \in M$. Since ry is a unit, r is a unit.

Example 2.10

The formal power series ring $\mathbb{C}[[x_1, ..., x_n]]$ is local. Take the ideal $(x_1, ..., x_n)$. Then for every power series f in $x_1, ..., x_n$ with 0 constant term, we show that $1 + f$ is a unit. This is apparent as we have the formal power series $(1 + f)^{-1} = (1 - f + f^2 - f^3 + ...)$.

3

Theorem 3.1

Let R be a ring. Let $P_1, ..., P_n \subseteq R$ be prime ideals. Let $I \subseteq \cup P_i$ be an ideal. Then I is contained in some P_i.

Remark. *There is a counterexample. In $\mathbb{F}_2[x, y]$ pick $I = (x, y)$. We can find three ideals in $\mathbb{F}_2[x, y]$ whose union contains (x, y) but none contains (x, y). (left as an "interesting" exercise) The same is not true for an infinite field.*

Proof. We induct on n. $n = 1$ is easy. We look at the case for $n = 2$ as an example. Let $n = 2$. We suppose that I is not contained in either P_1 or P_2. Suppose $a_1, a_2 \in I$ such that $a_1 \notin P_1$, $a_2 \notin P_2$ (so that $a_1 \in P_2$, $a_2 \in P_1$). Then $a_1 + a_2 \in I$ is not an element of P_1 or P_2. This gives a contradiction.

The idea is to pick element in $I \cap P_{k \neq i}$ for each i from $1 - n$.

Suppose the statement holds for $n - 1$, we want to show for n. Then by contradiction suppose I is not contained in either of the P_i's. Then by the induction hypothesis we can assume that there are no inclusion among the P_i's, since this will reduce to the case for $n - 1$. Choose elements $a_i \in I$ but $a_i \notin P_i$. Then for each other $P_{j \neq i}$ pick an element b_k distinct from P_i and multiply a_i by b_k. Then this product of b_k's and a_i is not in P_i, as P_i is prime. However, it is in the intersection of I and the $P_{k \neq i}$'s. The sum of all the products $b_{k \neq i} a_i$ is not in each of the ideals.

Definition 3.2 (Coprime ideals)

Let $I_1, I_2 \subseteq R$. Then they are coprime $I_1 + I_2 = R$.

Proposition 3.3

Let $I_1, I_2 \subseteq R$. Let

$$I_1 \cdot I_2 \overset{\text{def}}{=} (ab : a \in I_1, b \in I_2).$$

We have

$$I_1 \cdot I_2 \subseteq I_1 \cup I_2,$$

with equality when the ideals are coprime.

Remark. *The equality condition of coprime is not an if and only if in the first statement. For example the* 0 *ideal plus the* 0 *ideal does not have* 1*. The algebraic completion* $\bar{\mathbb{Z}} \subseteq \bar{\mathbb{Q}}$ *is a non-noetherian subring and contains* $p, p^{1/2}, p^{1/3} \ldots.$ *The ideal generated by* $I = p^{a/b} : a/b$ *is a positive real number satsifies* $I^2 = I = I \cap I$*.*

Proof. We prove the specific statement first. The first inclusion is obvious as $ab \in I_1 \cap I_2$. For the other inclusion, let I, J coprime ideals Pick $i \in I, j \in J$ such that $i + j = 1$. Then for every $a \in I \cap J$ we have

$$a = a \cdot 1 = ai + aj$$

is a sum of an element in I and an element in J. ✿

Theorem 3.4 (Chinese Remainder)

Let I, J be coprime ideals. Then

$$R/(I \cap J) \to R/I \oplus R/J$$

is an isomorphism.
In general, let $I_1, ..., I_n$ be ideals of R such that they are pairwise coprime. Then we have

$$R/\cap_i I_i \to \oplus R/I_i$$

is an isomorphism.

Proof. We prove the case for two ideals. The case for multiple ideals is an exercise. We have a natural ring morphism from $R \to R/I \oplus R/J$. So we want to show that this is surjective with kernel $I \cap J$.

The kernel is $I \cap J$ by definition as $x = 0 \mod I$ and $x = 0 \mod J$ iff $x \in I$ and $x \in J$.

For surjection, pick $i \in I$, $j \in J$ such that $i + j = 1$. Then $i = 1 \mod J$ and $j = 1 \mod I$ Then for every $([a], [b]) \in R/I \oplus R/J$, $aj + bi$ maps to this element by linearity. ✿

Theorem 3.5 (Nakayama's Lemma)

Let $J \subseteq J(R)$ be an ideal. Let M be a finitely generated R module such that $JM = M$. Then $M = 0$.

Proof. Let $(e_1, ..., e_n)$ be a minimal set of generators for M. Then we have

$$m_1 = j_1 m_1 + j_2 m_2 + ... + j_n m_n.$$

Such that $j_i \in J \subseteq J(R)$. But then

$$(1 - j_1) m_1 = j_2 m_2 + ... + j_n m_n.$$

Because $1 - j_1$ is a unit by the characterization of Jacobson radical, we are done. ✿

Remark. *The thing fails if* M *is not finitely generated. Let* R *be the set of fractions* $\{a/b :$ p *does not divide* $b\}$*. Then* (p) *is the unique maximal ideal. If we take* $M = \mathbb{Q}$*, we have* $(p)M = M$*.*

4

Let R be a local ring with maximal ideal m, M a finitely generated $R-$module.

Corollary 4.1: If the $m_1, ..., m_n \in M$ generate M/m as a R/m vector space, then $m_1, ..., m_n$ generate M as an R module.

Proof. This is an application of Nakayama's Lemma.

Let N be the module generated by the m_i's. We have

$$M = N \oplus mM.$$

Now we can mod everything by N to get

$$M/N = 0 \oplus mM/N.$$

Thus by Nakayama's lemma, $N = M$.

Theorem 4.2

Let M be a non-zero Noetherian R module. Then $\exists$ a filtration by submodules $\{0\} = M_0 \subset M_1 \subset ... \subset M_n = M$ such that $M_{i+1}/M_i = R/p_i$ for some for some prime ideal p_i.

Definition 4.3 (Annihilator)

Let M be an R module. For $m \in M$ we define the annihilator of m

$$\mathrm{Ann(m)} \overset{\text{def}}{=} \{\mathrm{r \in R : rm = 0}\}.$$

This is an ideal.

Proof. Look at all Ann(m) for each $0 \neq m \in M$. There is a maximal element in this set by Zorn's lemma. (Exercise) The maximal element is a prime ideal.

Let $M_1 = Rm_1$, where m_1 is picked such that annihilator is maximal. This is isomorphic to $R/\mathrm{Ann(m_1)}$. Now we can repeat the process on M/M_1 to pick the second prime ideal. This process terminates by Noetherian condition of module.

Theorem 4.4 (Krull's Intersection)

Let R be a noetherian ring. $I \subset R$ an ideal. Then

$$I \cap_{n \geq 1} I^n = \cap_{n \geq 1} I^n.$$

Remark. *This is not in Atiyah Macdonald, but is in Milne.*

It is tempting to move the I into the intersection, but it is not the same. Counterexample: exercise (smile)

Proof. Let $I = (a_1, ..., a_r)$. Then $I^2 = (a_i a_j)$, and so on $I^n = (n-$ products of the $a_i)$. The trick now is to notice that this is related to the symmetric polynomials

$$I^n = \{g(a_1, ..., a_r) : g \text{ is a } R\text{-homogenious polynomial of degree } n.\}$$

Let $S_m \overset{\text{def}}{=} \{g(x_1, ..., x_r) \in R[x_1, ..., x_r] : g(a_1, ..., a_r) \in \cap_{a \geq 1} I^n\}$. Then

$$(\bigcup_{m \geq 1} S_m) \subseteq R[x_1, ..., x_r]$$

is a finitely generated (generated by (f_i)) ideal by Hilbert Basis theorem.

Let d be such that $f_i \in S_{m_i}$ satisfies $d \geq m_i$.

Let $b \in \cap I^n$. Then $b \in I^{d+1}$, and we write

$$b = f(a_1, ..., a_r),$$

$f \in S_{d+1}$, so can be written as

$$f = \sum_i g_i f_i.$$

We can pick g_i such that these are homogeneous with degree $\mathrm{deg\ f} - \mathrm{deg\ f_i} > 0$. If not, the different degrees have to cancel each other. So the g_i have no constant terms. Evaluate these at the a_i's. Since g has no constant term, $g(a_i) \in I$ and we have expressed f in the left hand side. ❀

Localization

Definition 4.5 (Multiplicatively Closed Set)

$S \subseteq R \backslash \{0\}$ is multiplicatively closed if it contains 1 and $s, t \in S \implies st \in S$.
We define localization

$$S^{-1}R \overset{\text{def}}{=} \{\left[\frac{r}{s}\right] : r \in R, s \in S\} / \sim,$$

were the equivalence relation is

$$\frac{r_1}{s_1} \sim \frac{r_2}{s_2} \text{ if } (r_1 s_2 - r_2 s_1) \cdot s = 0$$

for some $s \in S$.

Proposition 4.6

$S^{-1}R$ is a ring by the standard definitions plus and minuses.

$$\frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{r_1 s_2 + r_2 s_1}{s_1 s_2}$$
$$\frac{r_1}{s_1} \cdot \frac{r_2}{s_2} = \frac{r_1 r_2}{s_1 s_2}.$$

It has additive and multiplicative identity $\frac{0}{1}, \frac{1}{1}$ respectively.

Proposition 4.7

There is a canonical ring homomorphism $R \to S^{-1}R$. This sends $r \to \frac{r}{1}$.

Theorem 4.8 (Universal property of localization)

Let $S \subset R$ be multiplcatively closed. Let $g : R \to R'$ be a ring homomorphism such that $g(s)$ is a unit for every $s \in S$. Then there is a unique map $g_s S^{-1}R \to R'$ such that the composite $R \to S^{-1}R \to R'$ is equal to g.
In other words, $S^{-1}R$ is the smallest ring such that every element in S is a unit.

5

We now prove the Universal property of localization.

Proof. We need to define $S^{-1}f(a/s)$. Notice we must have $S^{-1}f(a/s)S^{-1}f(s) = S^{-1}f(a)$. So we must have

$$S^{-1}f(a/s) = f(a)f(s)^{-1}.$$

This is the uniqueness. We now need this to be well defined.

Suppose $\frac{a}{s} = \frac{a'}{s'}$. Then there is $\tilde{s} \in S$ such that $(as' - sa')\tilde{s} = 0$. Then we have

$$(f(a)f(s') - f(s)f(a'))f(\tilde{s}) = 0$$

$f(\tilde{s})$ is a unit, so we have

$$f(a)f(s') - f(s)f(a') = 0 \implies f(a)f(s)^{-1} = f(a')f(s')^{-1}.$$

Now we can confirm that this indeed satisfy ring homomorphism properties (this is just tedious).

Proposition 5.1

It is useful to think of quotients A/I as surjective maps $A \to B$ with kernel I.
In the same way, it is useful to think of localization $S^{-1}R$ as

$$f : A \to B,$$

such that

- $f(s)$ is a unit for $s \in S$
- Every element in B is in the form $f(a)/f(s)$.
- $f(a) = 0 \implies \exists s \in S$ such that $as = 0$

Proof. By the universal property of quotients and the first property, we have $S^{-1}A \to B$. The second property guarantes this map is surjective. We now need this map to be injective.

$$S^{-1}f(\frac{a}{s}) = 0 \implies f(a)f(s)^{-1} = 0 \implies f(a) = 0$$

By the third property, we have $s' \in S$ such that $as' = 0$. But this would mean $\frac{a}{s} = \frac{as'}{ss'} = 0$ to begin with.

Let M be an A-module. We define $S^{-1}M$

$$S^{-1}M \overset{\text{def}}{=} \{\frac{m}{s} : m \in M, s \in S\}/\sim,$$

with the equivalence

$$\frac{m}{s} \sim \frac{m'}{s'}$$

if $\exists \tilde{s} \in Ss.t.\tilde{s}(s'm - sm') = 0$.

Notation. *If $S = A/p$ for some prime ideal p, we write $A_p \overset{\text{def}}{=} S^{-1}A, M_p \overset{\text{def}}{=} S^{-1}M$. If $S = \{1, f, f^2 ...\}$, we denote A_f, M_f respectively.*

Proposition 5.2

S^{-1} is an exact functor in $\mathrm{Mod}_{\mathrm{R}}$.

Proof. Let $M' \xrightarrow{f} M \xrightarrow{g} M''$ exact. Consider exactness at $S^{-1}M$.

Let $m \in M, s \in S$ such that $g(m/s) = 0$. Then $g(m)/s = 0$. Then $\exists s' \in S$ such that $s'g(m) = 0$. So that $g(s'm) = 0$. Then we have $s'm \in f(M')$. So take this and divide by $s's$ to get m/s.

Definition 5.3

Let $\phi : A \to B$. Then we can consider B an A-module by

$$a \cdot b = \phi(a)b.$$

Let $A \to B$. If M is an A-module, we can look at

$$B \otimes_A M,$$

viewed as the tensor product of A modules. This is also a B-module. This is because we can define

$$b \cdot (\sum_i b_i \otimes m_i) = \sum_i bb_i \otimes m_i.$$

Therefore, we can build another $S^{-1}A$ module by

$$S^{-1}A \otimes_A M.$$

Proposition 5.4

There is an isomorphism

$$S^{-1}A \otimes_A M \to S^{-1}M.$$

Proof. Consider the map $S^{-1}A \times M \to S^{-1}M$ by

$$(\frac{a}{s}, m) \mapsto \frac{am}{s}.$$

This induces a map

$$S^{-1}A \times M \to S^{-1}A \otimes_A M \to S^{-1}M$$

where we have

$$f(\sum_i a_i/s_i \otimes m_i) = \sum_i \frac{a_i m_i}{s_i},$$

which is obviously surjective. For injectivity, we would expect that every element in $S^{-1}A \otimes_A M$ to be a pure tensor element.

Now we have (let $s = s_1 ... s_n$)

$$\sum_i \frac{a_i}{s_i} \otimes m_i = \sum_i \frac{1}{s_i} \otimes a_i m_i = \sum_i \frac{1}{s} \otimes a_i (s/s_i) m_i$$

is a pure tensor. So every element in $S^{-1}A \otimes_A M$ can be written as a primitive tensor. This makes life easier. Let $r = \frac{1}{s} \otimes m$ such that $f(r) = 0$. Then we have $m/s = 0$. So there is $s' \in S$ such that $s'm = 0$. Then

$$r = \frac{s'}{ss'} \otimes m = 0.$$

✿

Definition 5.5 (Local properties)

Let P be a property of some an A-module. We say that P is a **Local property** if

$$M \text{ has } P \iff M_p \text{ has } P$$

for all prime ideals $p \subset A$.

Proposition 5.6

The following are equivalent:

1. $M = 0$
2. $M_p = 0 \forall p \subset A$ prime
3. $M_m = 0 \forall m \subset A$ maximal.

Proof. Trivially, 1 implies 2 implies 3. We now show 3 $\implies$ 1. Suppose $M \neq 0$. Then let $x \in M \backslash 0$. Consider the annihilator of x. Consider a maximal ideal m containing $\text{Ann}(x)$. Then $s \cdot x \neq 0$ for all $s \notin m$. But then $\frac{x}{1}$ is not 0 in M_m. ✿

Proposition 5.7

Let $\phi : M \to N$. TFAE:

1. ϕ injective
2. $\phi_p : M_p \to N_p$ injective for all $p \subset A$
3. $\phi_m : M_m \to N_m$ injective for all $m \subset A$

Proof. Similar as above. ✿

Definition 5.8 (Flatness)

Let M be an A-module. Then M is flat if $\otimes M$ is an exact functor.

Theorem 5.9

TFAE

1. M is flat.
2. M_p is a flat A_p module for all p prime.

3. M_m is a flat A_m module for all m maximal.

Proof. (3 $\implies$ 1) Tensor products are right exact, so we need left exactness. Suppose M is not flat. Then there is $N \to N''$ injective but $M \otimes N \to M \otimes N''$ not injective.

Then by the previous proposition we have a maximal ideal such that

$$M_m \otimes N_m \to M_m \times N''_m$$

is not injective.

Remark. *We have* $(S^{-1}A \otimes_A M) \otimes_{S^{-1}A} (S^{-1}A \otimes_A N) \simeq S^{-1}A \otimes (M \otimes_A N)$.

6 Spec

Definition 6.1 (Spec)

Let R be a ring. The Spec of R is the set of all prime ideals in R, denoted as Spec (R).

Notation. *Write* $x \in$ *Spec* (R). *This corresponds to prime ideal* $p_x \subseteq R$.

Definition 6.2

Let $E \subset R$. Define

$$V(E) \overset{\text{def}}{=} \{x \in \text{Spec }(R) : E \subseteq p_x\}.$$

Proposition 6.3

Let a be the ideal generated by E.

$$V(E) = V(a) = V(r(a)).$$

Proof. The inclusions $\supseteq$ are tautological.

Now we need if $p \supseteq E$ then $p \supseteq r(a)$. Trivially $p \supseteq a$. Now if $r \in r(a)$, then for some n, $r^n \in a \subseteq p$. Since p is prime we must have $r \in p$.

Definition 6.4 (Topology on Spec)

We define the topology on Spec, such that the closed sets are exactly all the sets $V(a)$. This is known as the Zariski Topology.

Proposition 6.5

This is a well defined topology.

We will complete the proof later.

Proposition 6.6

$$\bigcap_{i\in I} V(E_i) = V(\bigcup_{i\in I} E_i).$$

Proof. If $x \in \bigcap_{i\in I} V(E_i)$, then $p_x \supseteq E_i$ for all $i \in I$. Then $p \supseteq \cup_i E_i$. On the other hand, if $p_x \supseteq \cup E_i$ then $p_x \supseteq E_i$, so $x \in V(E_i)$ for all i. ✿

Proposition 6.7

$$V(ab) = V(a) \cup V(b).$$

Proof. $(\subseteq)$ Supposed $p \supseteq ab$. We want $p \supseteq a$ or $p \supseteq b$.

Suppose not, then pick $r_1 \in a - p, r_2 \in b - p$, but then $ab \ni r_1 r_2 \notin p$.

$(\supseteq)$ On the other inclusion, if $x \in V(a)$ then $p_x \supseteq ab$. ✿

Proof of 6.5. We need

1. Empty set and Spec to be closed. This is easy as Spec $R = V(\{0\})$, $\{\} = V(R)$.
2. Arbitrary intersections as closed.
3. Finite unions are closed.

The other two statements are from proposition 6.7 and 6.6. ✿

Proposition 6.8

$$V(ab) = V(a \cap b).$$

Proof. This is because $r(a \cap b) = r(ab)$. The inclusion $\supseteq$ is trivial. For the other inclusion, if $x^n \in a \cup b$, then $x^{2n} \in ab$. ✿

Remark. *This proof breaks down when we have infinite intersections. Therefore we cannot use it.*

Example 6.9

- Spec $(K) = \{(0)\}$ for any field K.
- Spec $(\mathbb{Z}) = (0), (2), (3), (5)....$ Since each ideal generated by a prime number is prime, we have $V((p)) = (p)$.

Proposition 6.10

$x \in$ Spec R is closed iff $p_x \subseteq R$ is maximal.

Proof. $\Longrightarrow:$ Suppose not maximal, then there is a maximal ideal m containing it. Then for any $p_x \in V(a)$, we would have $m \in V(a)$.

$\Longleftarrow:$ Consider $V(p_x) = \{x\}$. ✿

Remark. *We have if $p_y \supseteq p_x$, then $x \in V(a) \implies y \in V(a)$.*

Corollary 6.11: Let $x \in \text{Spec } R$. Then the closure $\bar{x} = \{y : p_y \supseteq p_x\}$.

Proposition 6.12

The only closed subsets of Spec $\mathbb{Z}$ are $V((l))$, some positive integer l.

Proof. Since $\mathbb{Z}$ is a pid, every closed set is of the form $V((l))$. If $l = 0, 1$ then we are done. Else consider the prime factorization of l. This means we have the $V((l)) = \cup(p_i)$. This is also finite unions of closed points in Spec .

Example 6.13

Let $R = \mathbb{C}[x, y]$. Assume that a maximal chain of prime ideals in R has the form

$$(0) \subset (f) \subset m \subset \mathbb{C}[x, y],$$

where f is irreducible. We can reason through this by the nullstellensatz, i.e. all $m = ((x - \alpha), (y - \beta))$.
I.e. we can think of every closed point in Spec R corresponds to a point in the 2D plane. Now every f, we have $f \in m \iff f(\alpha, \beta) = 0$, so we can think of f as the curve $f = 0$ in the 2D plane (with a fuzzy point corresponding to the curve itself).

Definition 6.14 (Open sets of Zariski topology)

Define $D(f) \overset{\text{def}}{=} \{p : f \notin p\} = \text{Spec } R \backslash V(f)$.

Proposition 6.15

- $D(f_i)$ forms a basis for the topology.
- $D(f) \cap D(g) = D(fg)$
- $D(f) = \{\} \iff f$ if nilpotent
- $D(f) = \text{Spec } R \iff f$ is a unit.
- $D(f) = D(g) \iff r(f^n) = r(g^n)$.

Proposition 6.16

$$D(f) \simeq \text{Spec } R_f,$$

and Spec R is a quasi-compact topological space. I.e. every open cover has a finite subcover

Proof. Exercise.

7

Remark. *Atiyah Macdonald is so terse...*

We continue the discussion of Open sets of Zariski topology.

Proposition 7.1

Let Spec $R = \cup_{i \in I} X_i$, where each X_i open. Then there is a finite cover

$$\text{Spec } R = X_1 \cup ... \cup X_n.$$

Proof. We assume that $X_i = D(f_i)$ since D forms a basis. We claim that $(f_i)_{i \in I} = R$. Suppose not, then there is some prime (maximal) ideal p containing every f_i. But this is absurd because then we would not have a covering. Write $1 = \sum_i a_i f_i$. Then We would have a finite covering. ✿

Definition 7.2

Let $\phi : A \to B$ be a ring homomorphism. Since each prime ideal's preimage is prime, we can define a map induced by ϕ

$$\phi^* : \text{Spec } B \to \text{Spec } A.$$

Proposition 7.3

ϕ^* is continuous.

Proof. Let $V(I)$ be closed in Spec A. We want $\phi^{*-1}(V(I))$ be closed. We just check that $\phi^{*-1}(V(I)) = V(\phi(I))$ ✿

Example 7.4

Let $f \in R$. We have a ring homomorphism $\phi_f : R \to R_f$. Show that the map

$$\phi_f^* : \text{Spec } R_f \to \text{Spec } R$$

is a homeomorphism onto D_f.

Proof. In exercise 2. ✿

Let $x \in \text{Spec } R$. Consider the $R_x \overset{\text{def}}{=} \text{Frac(R/p}_\text{x})$, the field of fractions of the integral domain. Given $f \in R$ we can define a map that sends

$$x \mapsto f \mod p_x.$$

Example 7.5

In $\mathbb{C}[x, y]$, take a maximal ideal $(x - a, y - b)$. Take f a polynomial, then the map

$$(x - a, y - b) \mapsto f(a, b)$$

is the evaluation map.
Now take $I \subseteq \mathbb{C}[x, y]$ a radical ideal i.e. if $a^k \in I$ then $a \in I$. We now evaluate this on

$V(I)$. a function f induces the identically zero map if and only if it is nilpotent. Similarly, the function f is identically zero on $V(I)$ if and only if $f \in r(I) = I$. So $f \in I$. So if two functions are in the same coset $\mathbb{C}[x,y]/I$, they induce the same function on $V(I)$. So we can view functions on $V(I)$ as functions onto R/I.

Example 7.6

Let $I = r(I)$. Let $\phi : R \to R/I$. Show that $\phi^* : \text{Spec }(R/I) \to \text{Spec } R$ is a homeomorphism onto $V(I)$.

Definition 7.7 (Integral)

Let B be an A-algebra. We say that $\alpha \in B$ is **integral** over A if α satisfies

$$\alpha^n + a_{n-1}\alpha^{n-1} + ... + a_1\alpha + a_0 = 0.$$

for some $a_i \in A$.

Example 7.8

$1/2 \in \mathbb{Q}$ is not integral in $\mathbb{Z}$. This is because the polynomial has to be a monic.
$i \in \mathbb{C}$ is integral over $\mathbb{Z}$.

We want to prove the following result:

Theorem 7.9

If two elements are integral then their sum and products are integral.

Proposition 7.10

The following are equivalent.

1. $\alpha \in B$ is integral over A.
2. There is a faithful $A[\alpha] \subseteq B$ submodule that is finitely generated as an A module.

Remark. *An R-module M is faithful if $r_1 m = r_2 m$ for all $m \in M \implies r_1 = r_2$.*

Proof. $1 \implies 2:$ Let $\alpha \in B$ be integral. Such that $\alpha^n + a_{n-1}\alpha^{n-1}... + a_0$. Consider the submodule $M = A[\alpha]$. It contains 1_M and we have $r \in A[\alpha]$ satisfies $r \cdot 1 = r_m$. So this module is faithful.

Now notice that $A[\alpha]$ is generated by $\{1, \alpha, ..., \alpha^{n-1}\}$ by the monic polynomial relation.

$2 \implies 1$. Let $e_1, ..., e_n$ be a generating set (over A). Then

$$\alpha e_i \in \mathrm{Span_A\{e_i\}}.$$

Then there is some matrix transformation

$$(M - \alpha I_n) \begin{bmatrix} e_1 \\ e_2 \\ \vdots \\ e_n \end{bmatrix} = \vec{0}.$$

Multiply by the adjucate of $(M - \alpha I_n)$ gives

$$\det(M - \alpha I_n) I_n \begin{bmatrix} e_1 \\ e_2 \\ \vdots \\ e_n \end{bmatrix} = \vec{0}$$

kills every element in By faithfulness this has to be the zero transformation, so that

$$\det(M - \alpha I_n) = 0 \in A[\alpha].$$

The characteristic polynomial is a monic (up to factor of -1) polynomial in α, so we are done.

8

Definition 8.1 (Integral module)

We say B/A is **integral** if every element in B is integral over A.

Definition 8.2 (Finite algerbra)

B is a finite A-algebra if B is finitely generated as an A-module.

Remark. *This is stronger than finitely generated algebra. For instance, take $\mathbb{Q}[i]$ over $\mathbb{Q}$. This is finitely generated by $(1, i)$ as a module. But $\mathbb{Q}[x]$ is not finitely generated as a $\mathbb{Q}$ module, but finitely generated as an algebra by $(1, x)$.*

Proposition 8.3

B is a finite A-algebra iff B is a finitely generated A-algebra and generated by integral elements.

Proof. ($\implies$). This follows from the previous proposition. B is finitely generated as an A-algebra by the same elements. Moreover, each generating element is integral as B is a $A[\alpha]$-module that is finitely generated as A-module. This is faithful because $1 \in B$ is not killed by $A[\alpha]$ except for 0.

($\impliedby$). Let $B = A[\alpha_1, ..., \alpha_n]$ such that each α_i is integral. Then $(\alpha_1, \alpha_1^2, ..., \alpha_2, \alpha_2^2, ..., \alpha_n, ..., \alpha_1\alpha_2, ...)$ is finitely generated by finite powers of α_I, since each α_i satisfies a monic polynomial, we can pick multi-index I such that it is of degree $\sum$ order of monic polynomial. So B is finitely generated as an A-module by $(\alpha_1, ..., \alpha_1^{k_1}, ..., \alpha_n, ..., \alpha_n^{k_n}, \alpha_1\alpha_2, ...)$.

Proposition 8.4

B is a finite A-algebra iff B is a finitely generated A-algebra and generated by integral elements **and every element in B is integral over A.**

Proof. Backward direction is the same. For the forward direction, we apply for $b \in B$ the $A[b]$-module B which is finitely generated as an A-module and is faithful.

Proposition 8.5

Let B be an A-algebra, and C be a B-algebra. Then if C integral over B and B integral over A, then C is integral over A.

Proof. Let $c \in C$. Then we have for some n and $b_i \in B$,

$$c^n + b_{n-1}c^{n-1} + ... + b_0 = 0.$$

So c is integral over $B' = A[b_0, ..., b_{n-1}]$. Consider the algebra generated by $C' = A[b_0, ..., b_{n-1}, c]$. This is a finite B' algebra by integral element $c, c^2, ..., c^{n-1}$. But B' is also a finite A-algebra by previous proposition. So then C' is finite. By the previous proposition, every element in C' is integral over A, in particular, c is integral over A.

Lemma 8.6

If C finite over B and B finite over A as algebras, then C is finite over A.

Proof. Let $\{b_i\}$ generate B as A module and $\{c_j\}$ generate C as B module. Then $\{b_i c_j\}$ generate C as A module. As every $c \in C$ is some

$$\sum_j r_j c_j = \sum_{i,j} a_{i,j} b_i c_j.$$

Theorem 8.7

Let B be an A-algebra. Then the set of elements of B that are integral over A is a subalgebra of B.
That is, sum, difference, products of integral elements are integral.

Proof. Let $\alpha, \beta \in B$ integral over A. Consider $A \subseteq A[\alpha, \beta]$. $A[\alpha, \beta]$ is a finite A algebra as it is finitely generated by integral elements. Therefore, we have the stronger statement that every element in $A[\alpha, \beta]$ is integral over A.

Corollary 8.8: The set of elements in $\bar{\mathbb{Q}}$ that satisfy monic polynomials in $\mathbb{Z}[x]$ is a subring.

Now let A be in integral domain, and F be its field of fractions.

Definition 8.9 (Integrally closed/Normal)

We say that A is integrally closed/normal if the only elements of F that are integral over A already lie in A.

Remark. *For instance, $\mathbb{Z}$ is integrally closed.*

Theorem 8.10

Let A be a unique factorization domain. Then A is integrally closed. In particular, all PID's are integrally closed.

Proof. Let $\frac{a}{b} \in F$. Let p a prime element such that $p|b$ (so that it does not divide a or else there will be cancellation). Suppose that $\frac{a}{b}$ is integral. Then clearing out denominators gives

$$a^n = b \cdot (\tilde{a})$$

for some $\tilde{a} \in A$. Because A is a UFD, this is a contradiction as the LHS is not divisible by p but the right is.

Remark. *$\mathbb{Z}[2i]$ is not integrally closed. The field of fractions is $\mathbb{Q}[i]$, and $i^2 + 1 = 0$ gives an integral element $i \in \mathbb{Q}[i]$ not in $\mathbb{Z}[2i]$.*

Another non example: $\mathbb{C}[t^2, t^3]$. The fraction field is the fraction field of $\mathbb{C}[t]$, for which t is integral as it satisfies $x^2 - t^2 = 0$.

Proposition 8.11

Let A be normal integral domain, and F be its field of fractions. Let K/F be a finite extension. Then $\alpha \in K$ is integral over A iff the minimal polynomial of α is in $A[x]$.

Remark. *The minimal polynomial is the unique monic polynomial.*

Proof. The backwards direction is obvious. For the forward direction, suppose that $\alpha \in K$ integral over A. Let $f \in A[x]$ kill α. Let $g \in F[x]$ be the minimal polynomial. We have $g|f$. Let K' be an extension of F for which g splits. Then set $\alpha_1, ..., \alpha_n \in K'$ are the roots. So each $f(\alpha_i) = 0$. So each α_i is integral over A. So by Vieta's formulae, we have each coefficient in g is a sum of products in the α_i. So the coefficients are integral over A. Since A is integral, we have $g \in A[x]$.

9 Integral Closure

For the following statements, let B be an integral algebra over A.

Proposition 9.1

If A and B are integral domains then A is a field iff B is a field.

Proof. $\implies$: Let A be a field. Let $0 \neq b \in B$. Then consider the monic polynomial

$$b^n + ... + a_0 = 0.$$

WLOG we can assume a_0 is non zero, as integral domain. Then subtract a_0 on each side and divide by $-a_0$. We can factor b out to find an inverse.

$\Longleftarrow$: **We first prove it assuming that A is integrally closed.** Let B be a field. Then FracA $\subseteq$ B. So the field of fractions is integral over A. But A is integrally closed, i.e. the field of fractions of A lies in A.

Now we drop the integrally closed condition. Let $a \in A$. Consider $a^{-1} \in B$. There is a monic polynomial

$$a^{-n} + ... + a_0 = 0.$$

Multiplying both sides by a^{n-1} gives

$$a_0 a^{n-1} + ... + a^{-1} = 0.$$

Now we have expressed a^{-1} in A. ❀

Proposition 9.2

Let $S \subset A$ be a multiplicatively closed set. Then $S^{-1}B$ is integral over $S^{-1}A$.

Proof. Let $\frac{b}{s} \in S^{-1}B$. Then we have

$$b^n + ... + a_0 = 0.$$

Dividing both sides by s^n will produce a polynomial with coefficients in $S^{-1}A$. ❀

Proposition 9.3

Let $q \subset B$ a prime ideal. Then q is maximal iff $p \overset{\text{def}}{=} q \cap A$ is maximal.

Proof. Consider B/q is integral over A/p (because quotients). Since q is prime, these two are both integral domains. By the previous proposition, one is a field if and only if the other is field. Translating back to ideals, one is maximal if and only if the other is maximal. ❀

Proposition 9.4

Let $q_1 \subseteq q_2 \subset B$ both prime ideals, and

$$q_1 \cap A = p = q_2 \cap A.$$

Then $q_1 = q_2$.

Proof. If p is maximal then the statement follows directly from the previous proposition. Else consider the multiplcatively closed set $S = A \backslash p$. Then $S^{-1}B$ integral over $S^{-1}A$. Now $S^{-1}p$ is maximal. So $S^{-1}q_1 = S^{-1}q_2$. Since we have bijection between prime ideals that avoid S and prime ideals in $S^{-1}B$, they have to be the same before localization. ❀

Example 9.5

Let $\mathbb{K}/\mathbb{Q}$ be a finite extension of fields.
$\mathbb{Z} \subset \mathbb{Q}$. We would like to find something in $\mathbb{K}$ that looks like an extension of $\mathbb{Z}$.

Definition 9.6 (Integral closure)

The closure $\mathcal{O}_K \subseteq K$ is the ring of elements in K that satisfies a monic $\mathbb{Z}$-polynomial.

Remark. *This is a ring because the sum and products of integral elements are integral.*

Proposition 9.7

Every non-zero prime ideal in $\mathcal{O}_K$ is maximal.

Proof. Let p be prime. If $p \cap \mathbb{Z} = (0) = (0) \cap \mathbb{Z}$, then we have $p = (0)$. Else consider the maximal ideal $p \cap [Z] = (p_0)$. Take a maximal ideal q containing p, then $q \cap \mathbb{Z} = p \cap \mathbb{Z}$. So $p = q$ is maximal.

Proposition 9.8

The field of fractions of $\mathcal{O}_K$ is K.

Proof. We will show that $\alpha \in K$ there exists $0 \neq n \in \mathbb{Z}$ such that $n\alpha \in O_k$. Since $K/\mathbb{Q}$ finite, write

$$\alpha^n + \ldots + k_0 = 0.$$

Each $k_i = a_i/b_i$. So multiply each side by $b = \prod_i b_i^n$. Then $b\alpha$ satisfies a monic polynomial with coefficients in $\mathbb{Z}$.

Proposition 9.9

$\mathcal{O}_K$ is integrally closed.

Proof. Let $\alpha \in K$ integral over $\mathcal{O}_K$. Then $\mathcal{O}_K(\alpha)$ integral over $\mathcal{O}_K$ integral over $\mathbb{Z}$, so that α integral over $\mathbb{Z}$.

Calculation of integral closures

Example 9.10

We find the integral closure of $\mathbb{Q}[\sqrt{2}]$. We know these are the set of elements that satisfy minimal polynomials in $\mathbb{Z}[x]$. Since this is a field of degree 2, we just compute

$$x^2 - (a + b\sqrt{2} + a - b\sqrt{2})x + (a + b\sqrt{2})(a - b\sqrt{2}) = 0$$

such that these coefficients are in $\mathbb{Z}$. This turns out to be $a, b \in \mathbb{Z}$, so the integral closure is just $\mathbb{Z}[\sqrt{2}]$. This is not the case with $\mathbb{Q}[\sqrt{5}]$, as we have $a = 1/2, b = 1/2$. The integral closure of $\mathbb{Q}[\sqrt{5}]$ is $\mathbb{Z}[(1 + \sqrt{5})/2]$.

10

Theorem 10.1

$\mathcal{O}_K$ is Noetherian.

Proof. We will show that **every ideal of $\mathcal{O}_k$ is finitely generated over** $\mathbb{Z}$, thus finitely generated over $\mathcal{O}_k$.

Suppose $K/\mathbb{Q}$ is an extension of degree n. Let $\beta_1, \beta_n \in \mathcal{O}_K$ that forms a $\mathbb{Q}$-basis for K. This is possible because $\mathbb{Z}^{+\ -1}\mathcal{O}_K = K$.Then $\exists \beta_1^*, ..., \beta_n^* \in K$ such that $\mathrm{Tr(\beta_i\beta_j^*) = \delta_{ij}}$.

We want to show

$$\oplus_i \mathbb{Z}B_i \subseteq \mathcal{O}_K \subseteq \oplus_i \mathbb{Z}B_i^*.$$

First notice (exercise)

$$\oplus_i \mathbb{Z}\beta_i^* = \{\beta \in K : B(\beta, \beta_i)\imath\mathbb{Z}\forall i\}.$$

So we want to show that

$$\mathrm{Tr(\alpha\beta_i) \in \mathbb{Z}\forall\alpha \in \mathcal{O}_K}.$$

This is true because trace is in the fixed field $\mathbb{Q}$ and the trace is integral if $\alpha \in \mathcal{O}_K$. So that the trace is an integer.

Definition 10.2 (Trace)

Let $\alpha \in K$, then the trace

$$\mathrm{Tr_{K/\mathbb{Q}}(\alpha) = \alpha_1 + ... + \alpha_n},$$

the sume of all conjugates of α. I.e. take the galois extension of $\mathbb{Q}$ containing K. Let $\sigma_i : K \to N$ where σ_1 is inclusion. Then the trace is the sum of $\sigma_i(\alpha)$.

Proposition 10.3

1. $\mathrm{Tr}(\alpha + \beta) = \mathrm{Tr}\alpha + \mathrm{Tr}\beta$
2. $\mathrm{Tr(a\alpha/b) = a/bTr\alpha}$

Let $B_{K/\mathbb{Q}} : K \times K \to \mathbb{Q}$ that sends $(\alpha, \beta) \mapsto \mathrm{Tr}(\alpha\beta)$. This is bilinear and nondegenerate.

Remark. *In general,* $\mathrm{Tr_{L/F}}$ *not* $\equiv 0 \iff L/F$ *is separable.*

Definition 10.4 (Dedekind domain)

An integral domain R is a **Dedekind domain** if

1. R is Noetherian
2. All non-zero prime ideals are maximal
3. R is normal (integrally closed).

Corollary 10.5: $\mathcal{O}_K$ is a Dedekind domain.

Corollary 10.6: A Dedekind domain, F field of fractions, and K/F separable extension, then the integral closure of A in K is a Dedekind domain.

Theorem 10.7

Let B/A integral. Let $p \subseteq A$ prime ideal. Then there is a prime ideal in B that contracts to p in A. i.e.

$$q \cap A = p.$$

Proof. Localize p. $A \to A_p$. Then pA_p is (uniquely) maximal. Moreover, since A_p is not a field, B_p is not a field and has a nonzero maximal ideal m. Then $m \cap A_p$ is maximal so it is pA_p. Now we have $m \cap A = p$. Then $m \cap B$ contracts to p. ✿

Theorem 10.8 (Going Up)

Let B/A integral. Let $q \subseteq B$ prime, $p \subseteq p' \subseteq A$ prime. Also suppose that $q \cap A = p$. Then there exists $q \subseteq q' \subseteq B$ prime such that it contracts to p'.

Proof. Consider A/p and B/q. By the previous theorem, we have a prime ideal of $\bar{q}' \subseteq B/q$ that contracts to $p'/p \subseteq A/p$. Now take the preimage of $\bar{q}'$ in B. We can check that it contracts to p'. (exercise) ✿

Corollary 10.9 (Going Up): Let B/A integral. Let $p_1 \subseteq p_2 \subseteq ... \subseteq p_n \subseteq A$ be a chain of prime ideals, and $q_1 \subseteq B$ prime that contracts to p_1. Then we can extending the chain in q to the full length n i.e. $q_1 \subseteq q_2 \subseteq ... \subseteq q_n$, such that each q_i contracts to p_i.

We would like to work towards going down theorem. To extend the chain the other way, we need a few more statements and some additional assumptions.

Definition 10.10

Let $a \subseteq A$, B/A integral. Then $b \in B$ integral over a if B satisfies a monic polynomial with coefficients (except the first monic one...) lying in the ideal a.
The set of elements that are integral over a is called the integral closure of a in B.

Proposition 10.11

Consider B/A. Then $b \in B$ is integral over $a \subseteq A$ iff there is a faithful $A[b]$ section (module) $M \subseteq B$ that is finitely generated as an A module and $bM \subseteq aM$.

Proof. Exercise. ✿

Theorem 10.12

The integral closure of a in B is $r(aB)$.

Proof. $\supseteq$: Let $b \in r(aB)$. Then write

$$b^n = \sum_i^m a_i x_i$$

for some $x_i \in B$, $a_i \in a$. Then let $M = A[x_i]$. We thus have $b^N M \subseteq aM$. So that b^N integral over a. So b integral over a.

$\subseteq$: For the other way, let b be integral over a. Write

$$b^n = \sum_{i<n} a_i b^i \in aB$$

so $b \in r(aB)$.

11

Proposition 11.1

Let $I \subseteq A$ ideal, $F = \text{Frac(A)}$. Then if $\alpha \in K/F$ is integral over I the minimal polynomial of α has non-leading coefficients in $r(I)$.

Proposition 11.2

Let B integral over A. Then $\alpha \in B$ is integral over $I \subseteq A$ iff $\alpha \in r(aB)$.

We want to prove the going down theorem.

Theorem 11.3 (Going down)

Let B/A integral. Further assume that A is an integral domain and is integrally closed. Let $q \subseteq B$ prime, $p' \subseteq p \subseteq A$ prime. Also suppose that $q \cap A = p$. Then there exists $q' \subseteq q \subseteq B$ prime such that it contracts to p'.

Lemma 11.4

Let $\phi : R_1 \to R_2$ ring homomorphism. Let $p_1 \subset R_1$ prime. Then there is prime $p_2 \subset R_2$ with $\phi^{-1}(p_2) = p_1$ iff $\phi^{-1}(\phi(p_1)R_2)$.

Proof. We localize at q. We want to show $p'B_q \cap A = p'$. Then there is some prime ideal $\tilde{q} \subseteq B_q$ such that $\tilde{q} \cap A = p'$ (by the reverse direction of the previous lemma). B_q is local, so qB_q contains $\tilde{q}$. Take $q' = \tilde{q} \cap B$.

One inclusion is simple, so we show the $\subseteq$ direction. Let $b \in p'B_q$. Then

$$b = \frac{y}{s}, y \in p'B, s \in B - q.$$

So $y \in r(p'B)$. So by proposition b is integral over $p' \subset A$. Then the minimal polynomial of y has non leading coefs in $r(p') = p'$. Now let we have $b \in A \cap p'B_q$. Then we must have $b = y/s \implies s = y/b$, as evaluated in $b^{-1} \in \text{FracA}$.

So if y satisfies

$$y^n + ... + a_1 y + a_0$$

then

$$s^n + a_{n-1}/bs^{n-1} + ... + a_0/b^n = 0.$$

Now this is a minimal polynomial of s over FracA, as the degree of extension of y and s have to be the same over the fraction field (they are the same extension). Therefore, we can now apply the fact that $s \in B$ is integral over A to get each a_{n-i}/b^i is in A. But now we have

$$\frac{a_{n-i}}{b^i} \cdot b^i = a_{n-i} \in p'.$$

If $b^i \in p'$ we are done as p' is prime. Else,

$$s^n = \sum_{i>0} -\frac{a_{n-i}}{b^i} s^{n-i} \in p'B \subseteq q,$$

this contradicts our assumption of $b = \frac{y}{s} \in B_q$.

Theorem 11.5 (Noetherian Normalization)

Let K be a field, R a finitely generated K-algebra. Then R is finite over a polynomial algebra.

Proof. We induct on the number of generators on R.

Let m be the minimal number of generators needed to generate R. If $m = 1$ we are done as $R = K[\alpha]$. If α is transendental, this is a polynomial ring and we are good. If α is integral, then R is finite over K.

Now we show for m-element generated algebras assuming the statement holds for $m-1$ generators.

Let $R = K[\alpha_1, ..., \alpha_m]$. If all of them are algebraically independent, then R is a polynomial ring generated by α_I for each multiindex I.

WLOG assume that α_m satisfies a polynomial in coefficients $R_m \overset{\text{def}}{=} K[\alpha_1, ..., \alpha_{m-1}]$. If the polynomial is monic $T^d + c_{d-1}T^{d-1} + ... + c_1T + c_0$ and each $c_i \in K[\alpha_1, ..., \alpha_{m-1}]$, then α_m is integral over this ring. So this R is finite over R_{m-1}. Since $Rm - 1$ finite, a finite extension is also finite.

If the polynomial is not monic, write

$$f(\alpha_1, ..., \alpha_{m-1}, T) = \sum_{I,j} c_I \alpha_I T^j, c_I \in K$$

Now we make the change of variables $\alpha_i' = \alpha_i - T^{N^i}$ for big $N > 4 * (m + \text{degf})$. Then the power of T is uniquely determined by exactly one multiindex (i.e. there are no cancellations). Then the leading coefficient of

$$f(\alpha_i' - T^{N^i}, ..., T)$$

is some $c_I \in K$, so is essentially a monic polynomial. Now α_m is integral over $K[...\alpha_i - \alpha_m^{N^i}, ...]$. This is a ring in $m - 1$ elements so is finite. The extension is finite so we are done.

12 Nullstellensatz

Theorem 12.1 (Zariski's Lemma)

Let K be a field. Let L/K a field which is a finitely generated K-algebra. Then L is a finite extension of K.

will fix this proof later. We induct on the number of generators of L.

Let $L = K[\alpha]$. If α is algebraic, we are done. Else α is transendental and $L \simeq K[x]$ which is not a field.

Suppose we have the statement for m generated L. We want to show for

$$L = K[\alpha_0, \alpha_1, ..., \alpha_m].$$

Let $K_0 = K(\alpha_0)$, $R_0 = K[\alpha_0]$. $L = K_0[\alpha_1, ..., \alpha_m]$, where each is algebraic over K_0 (induction).

Set $g_i(\alpha_i) = 0, g_i \in K_0[t]$.

Let $s \in R_0 \backslash \{0\}$, such that $s \cdot g_i \in R_0[t] \forall i$.

So g_i's are monic with coefficients $R_0[1/s]$. $L = R_0[1/s][\alpha_1, ..., \alpha_m]$.

So L is finitely generated R_0-algebra. Each generator is integral over $R_0[1/s]$. So L is integral over $R_0[1/s]$. In particular, K_0 is integral over $R_0[1/s]$. If α_0 algebraic over K, we are done. Else, suppose that α_0 is transendental over K. Then $R_0 \simeq K[x]$.

Then we have $R_0[1/s] \simeq K[x][1/f(s)]$. R_0 is integrally closed (because it is PID so UFD), so that the integral closure of $R_0[1/s] = K_0[1/s] = R_0[1/s]$. Therefore $R_0[1/s] = K_0$.

This is not possible because $K[t][1/f(t)]$ is never a field. Just find a prime ideal that avoids $f(t)$ i.e. an irreducible polynomial that is not $f(t)$. As a concrete example, take maximal ideal containing $f(t) + 1$.

Corollary 12.2: Let K be a field. Let R a finitely generated K algebra. Then for any maximal ideal $m \subseteq R$, R/m is a finite extension of K.

Proof. Any quotient of R is finitely generated as a K-algebra. Apply Zariski's lemma.

Corollary 12.3: Let K be algebraically closed, $m \subset K[x_1, ..., x_n]$. Then $m = (x_1 - a_1, x_2 - a_2, ..., x_n - a_n)$ for some $a_i \in K$.

Proof. Mod $K[x_1, ..., x_n]$ by m. This is a finite extension of K which is K because it is algebraically closed.

Now the map $K[x_1, .., x_n] \to K$ is determined uniquely by where x_i goes, so we have

$$(x_1 - f(x_1), ..., x_n - f(x_n)) \subseteq \mathrm{ker(f) = m}.$$

But the left hand side is maximal, so we are done.

Remark. *If you relax the condition for algebraically closed, we map*

$$K[x_1, ..., x_n] \to \bar{K}.$$

Each x_1 maps to the algebraic closure of K. Let g_i be the minimal polynomial of $f(x_i)$, then $(g_i) \subseteq m$. The left hand side is maximal because

$$K[x_1, ..., x_n]/(f_1(x_1)) = K[\alpha_1, x_2, ..., x_n]$$

repeat this to get $K[x_1, ..., x_n]/(f_i(x_i)) = K[\alpha_1, ..., \alpha_n]$. This only works if the polynomials are disjoint.

Non-example: $\mathbb{Q}[x, y] \to \mathbb{C}$, where both $x, y \mapsto i$. Then we have kernel $(x^2 + 1, x - y) \supset (x^2 + 1, y^2 + 1)$.

Corollary 12.4: Let $I \subset K[x_1, ..., x_n]$. Then there is some point in $\bar{K}$ such that there is some $a_1, ..., a_n \in K^{a.c}$ such that $f(a_i) = 0$ for all $f \in I$.

Proof. Take maximal ideal containing I. Mod by this ideal and embed the quotient into the algebraic closure of $K^{a.c.}$. Then the image of each x_i is the a_i's.

Lemma 12.5

Let R, S be finitely generated K algebras. Let $f : R \to S$. Then for maximal $m \subset S$ we have $f^{-1}(m)$ is maximal.

Proof. Let m maximal. Then consider

$$R \xrightarrow{\text{f}} S \xrightarrow{\text{e}} S/m.$$

Then $R/f^{-1}(m) \simeq e \circ f(R)$. By Zariski's lemma, S/m is a finite extension of K. But now the image of R is a subring of L containing K(*), so the image is a field. Therefore the pullback is maximal.

(*) each element is algebraic, so adjoining each element also adjoins the inverse.

13

Prelim syllabus is almost done. Midterm after covering more spec stuff.

Midterm on Monday May 12.

Definition 13.1 (Jacobson ring)

A ring R is **Jacobson** if

$$\bigcap_{m \supseteq I} m = r(I)$$

for all ideals $I \subsetneq R$.

Proposition 13.2

A ring is Jacobson if and only if $\cap_{m \supseteq p} m = p$ for all prime ideals p.

Theorem 13.3

Every finitely generated K-algebra R is Jacobson.

Proof. It is enough to show that

$$\bigcap_{m \subset R} m = 0$$

for every integral domain finitely generated K algebra R. If this holds, let R_0 be a finitely generated K algebra. Let $p_0 \subset R_0$. Consider $R = R_0/p_0$. This is a finitely generated integral domain, so (0) is prime. The intersection of all maximal ideals in R is $\{0\}$, so the intersection of all maximal ideals in R_0 containing p_0 is p_0.

Now we show that statement. Consider the special case where R is a polynomial ring $= K[x_1, ..., x_n]$. We want to show that for any $f \neq 0$, there is some point in the algebraic closure such that evaluated at that point f is non zero. Suppose this work is true, then the maximal ideal corresponding to that point does not contain f.

This is true for $n = 1$. For $n = 2$, if there is a point $y_0 \in K^{ac}$such that $f(x, y_0) \neq 0$ we are done. Else we have $f(x, y_0) = 0$ for all $y_0 \in K^{ac}$. Consider f as in $K(x)[y]$.

Now we solve for a general R. By Noetherian normalization, R is finite over some K-algebra $K[x_1, ..., x_n]$. Let $0 \neq f \in m$ for every $m \in R$. Consider the minimal polynomial

$$f^k + a_{k-1}f^{k-1} + ... + a_1 f + a_0 = 0,$$

for $a_i \in K[x_1, ..., x_n]$. So that

$$a_0 = -f^k - ... - a_1 f \in m.$$

But now $a_0 \in \cap_{m \subset K[x_1,...,x_n]} m = 0$ so $a_0 = 0$. This gives a contradiction.

MSpec vs Spec

MaxSpec is the set of all closed points in Spec.

If R is Jacobson, for $\eta \in$ Spec , we have $\bar{\eta} = \overline{\{y : y \in \max \text{Spec }, y \in \bar{\eta}\}}$.

Equivalently, Let $Z \subset \text{Spec } R$ be a closed subset. Then $Z \cap \max \text{Spec } R$ is dense in Z.

Corollary 13.4: For R finitely generated K algebra, closed subsets of Spec R are in bijection with closed subsets of $\max \text{Spec } R$.

Proof. Take intersection and closure for the directions respectively.

Example 13.5

Exercise: show that these two maps are inverses of each other.

Corollary 13.6: Every closed subset of $\max \text{Spec } R$ has the form $Z(a) = \{m \subseteq R, m \supseteq a\}$.

Theorem 13.7 (Strong Nullstellensatz)

Let $a \subset K[x_1, ..., x_n]$ be an ideal. If f satisfies $f(P) = 0$ for all $P \in (K^{ac})^n$, with $m_p \supset a$. Then $f \in r(a)$.
m_p is the maximal ideal corresponding to the point.
If K is algebraically closed, $Z(a) = \{P \in K : f(P) = 0 \forall f \in a\}$.

Proof. Let $a = (g_1, ..., g_m)$. Then consider the ideal

$$I = (g_1, ..., g_m, 1 - fy) \in K[x_1, ..., x_n, y]$$

We claim that there is no point $(a_1, ..., a_n, b) \in (K^{ac})^{n+1}$ that I vainishes. Suppose there is. Then $g_i(a_1, ..., b) = 0$ for all i. So then $f(a_1, ..., a_n) = 0$ But then $1 - fb$ is non zero.

By the nullstellensatz, $I = (1)$. Then we set $1 = h_1 g_1 + ... + h_m g_m + h(1 - fy)$. Quotient this by $y = 1/f$. Then $1 = h'_1 g_1 + ... + h'_m g_m$ for some $h'_i \in K[x_1, ..., x_m][1/f]$. Clear denominators and we get $f^N = h''_1 g_1 + ... + h''_m g_m \in a$.

14

Fulton algebraic curves chapter 1.

Remark. *I am just a child please be nice to me on the midterm.*

Notation. *Let K be an algebraically closed field for this lecture.*

Definition 14.1 (Subvariety)

$Z \subseteq K^n$ is a **closed subvariety** if

$$Z = Z(a) \overset{\text{def}}{=} \{P \in K^n : g(P) = 0 \forall g \in a\}$$

for some ideal $a \subseteq K[x_1, ..., x_n]$

Remark. *By the Strong Nullstellensatz, for any $f \in K[x_1, ..., x_n]$ and a ideal such that $f|_{Z(a)} = 0$ then there is some n such that $f^n \in a$. So we have bijection between radical ideals in $K[x_1, ..., x_n]$ and closed subvarireties of K^n.*

K^n is $\max \operatorname{Spec} K[x_1, ..., x_n]$ which is a subspace of Spec . So the Zariski toplogy induces topology on K^n. We can think of this as evaluating function f at P, or taking $f \mod m$ (which is the same as evaluation).

We also have functions on $Z(a)$ are $K[x_1, ..., x_n]/a$. Conversely, we can recover $Z(a)$ from $K[x_1, ..., x_n]/a$ by looking at the MSpec.

Definition 14.2 (Affine variety)

An **affine variety** is an object of the form

$$\max \operatorname{Spec} R$$

such that R is a finitely generated K-algebra.

Remark. *Picking a "presentation" of R i.e. $R = K[x_1, ..., x_n]/I$. We get a map from $\max \operatorname{Spec} R \to K^n$ with closed image and is a homeomorphism onto its image.*

Given an affine variety, an open subvariety is an open subset (in the Zariski topology).

Example 14.3

For $K = \max \operatorname{Spec} K[x]$ we have $K^\times$ is open. We can think of it as the set of points where $x(p) \neq 0$.
Nevertheless, this is an affine variety, as this is $K[x, x^{-1}]$ which has maximal ideals in bijection with maximal ideals in $K[x]$ that avoid (x). The only maximal ideal that does not avoid (x) is itself. Therefore the MSpec of this localization is an affine variety.
We view this $K[x, x^{-1}]$ as $K[x, y]/(xy - 1)$. In K^2 the image of $K^\times \to K^2$ is equation $xy = 1$ which is now closed.
The map going from $K^\times \to K^2$ is the projection.

Proposition 14.4

Let V be an affine variety, R finitely generated. Then for $f \in R$, $D(f) \subseteq V$ is an affine variety.

Proof. $D(f) = \max\operatorname{Spec} R[1/f]$. Give an extra variable y and quotient further with $fy - 1$ gives an embedding from $D(f) \to K^{n+1}$

Proposition 14.5

Let R be a finite K-algebra. Then R has finitely many maximal ideals. (keyword: Artinian rings).

Proof. R is Artinian. We can first treat R as a finite dimensional vector space. Any descending chain of ideals must be strictly decreasing in dimension.

Now let S be the set of products of finitely many maximal ideals i.e. every element can be written as $m_1 ... m_n$ for m_i maximal in R. By Artinian property this contains a minimal element $m' = m_1 ... m_k$.

Now for every other maximal $m \subseteq R$ we have

$$mm' \subseteq m' \overset{\text{minimality}}{\subseteq} mm'.$$

So $m \supseteq mm' = m'$. But because m is prime, then m must contain at least one of the m_i's. (else the product will lie outside of m). By maximality $m = m_i$ for some i.

Theorem 14.6 (Going donw for finitely generated K algebras)

Let R_1 be an integral domain, R_2 integral over R_1.
Let $\max\operatorname{Spec} R_2 \xrightarrow{\phi} \max\operatorname{Spec} R_1$. This is well defined because integral preserves maximal ideals.

1. ϕ is surjective.
2. The fibers of ϕ are finite.

Proof. For the first claim, we can always construct things in R_2 that contract to $m \subset R_1$.

For the second claim, let $m \subset R_1$ and m' be the ideal generated by m in R_2. Then R_2/m' is integral over R_1/m which is a field. R_2/m' is a finite K-algebra, so has finitely many maximal ideals contracting to 0 in R_1/m thus has finite fibers.

Now let A be a finitely generated K algebra and an integral domain. Noetherian normalization gives that it is a finite extension of $K[x_1, ..., x_n]$. The map between max specs is surjective and has finite fibres.

Example 14.7

Consider $K[x, y] \to K[x, z]$ by sending $x \mapsto x$ and $y \mapsto xz$. $K[x, z]$ is not finitely generated as a module as z^k are not integral.
But if you can invert x, then it is finite. Inverting x is equivalent to throwing out the y axis in K^2 $(x = 0)$.

The map between MSpec sends $(x, z) \mapsto (x, xz)$, so we get $(a, b/a) \mapsto (a, b)$. But if $x = 0$, then $(x = 0, y = c)$ intersects $K[x, y]$ at $x = 0, y = 0$, so the whole y axis collapses to the origin.

15

Example 15.1

Look at $\mathbb{C}$ with the Zariski topology. I.e. look at MSpec $\mathbb{C}[x]$. We cannot write this as a union of two closed strict subsets of $\mathbb{C}$. This is because by PID, closed sets are represented as $V(f)$, and contains finite set of points (or is the whole space).

Definition 15.2 (Irreducible Topological Space)

A topological space X is **irreducible** if it cannot be written as $X = A \cup B$, where both A and B are closed strict subspaces of X.

Proposition 15.3

$A^n \overset{\text{def}}{=} K^n$ with the Zariski topology is irreducible.

Proof. Suppose we can. Write $A^n = X \cup Y$, where $X = Z(I)$, $Y = Z(J)$. But then $X \cup Y = Z(IJ)$ gives f vanishes everywhere on A^n for all $f \in IJ$. So $IJ = 0$. Because $K[x_1, ..., x_n]$ is an integral domain, $I = 0$ or $J = 0$.

Proposition 15.4

Let y be an affine variety i.e. $y = \max \operatorname{Spec} R$, then if f vanishes everywhere then f is nilpotent.

Proof. Write $k[x_1, ..., x_n] \to R$ with kernel I. Then we can identify $\max \operatorname{Spec} R$ with $Z(I)$. But if f vanishes on $Z(I)$ then $f \in r(I)$. So f is nilpotent in R.

Theorem 15.5

Suppose the radical of R is 0. $V = \max \operatorname{Spec} R$ is irreducible is irreducible if and only if R is an integral domain. Equivalently, if $V = Z(I) \subseteq A^n$ we would have $I = r(I)$, which means I is prime.

Proof. We prove the backward direction first. Let $V = X \cup Y$ both closed, $X = Z(I), Y = Z(J)$. Then $V = Z(IJ) \implies IJ = (0)$. Since the ring is integral, we get I or J is 0.

For the other direction, if R is not an integral domain, then we have $x, y \neq 0$, but $xy = 0$. Then $Z((x)) \cup Z((y)) = V$.

Definition 15.6 (Noetherian space)

A topological space X is **Noetherian** if every sequence of closed subsets $X_1 \supset X_2 \supset X_3..$ stabilizes.

Remark. *This is Noetherianess of a ring, but the inclusion is reversed.*

Proposition 15.7

Let R be Noetherian. Then $\max \operatorname{Spec} R$ and $\operatorname{Spec} R$ are noetherian.

Remark. *The reverse implication is not necessarily true. This is because the Zariski topology only looks at the radical ideals. For example take $\cup_n \mathbb{C}[[t^{1/2^n}]]$. It has a unique maximal ideal (constant term $= 0$).*

Theorem 15.8

Let V be an affine variety. Then $V = X_1 \cup ... \cup X_n$, where each X_i is an irreducible closed subset of V.

Proof. Suppose V is irreducible. Then we are done.

Else write $V = X_1 \cup X_2$, each closed. Repeat the decomposition on X_1 and X_2. This must stabilize because $R = K[x_1, .., x_n]/I$ is Noetherian.

Corollary 15.9: $V = V(I)$, $X_i = V(p_i)$ gives $\cup X_i = V(\prod p_i)$. So the radical of I is radical of product of finitley many prime ideals.

Theorem 15.10

If $0 \neq p \subset K[x, y]$ is not maximal, then p is principal and any $p' \supset p$ is maximal.

Proof. Let $f \in p$, by unique factorization we write $f = \prod f_i^{n_i}$, each prime (irreducible). WLOG suppose that $f_1 \in p$. So let f be a prime element in p. We claim $p = (f)$. Suppose not, then there is another prime element g (by unique factorization) in p. We claim that there are only finitely many points where both f and g vanish. If so, p only vanishes on finitely many points. Because $V(p)$ is irreducible, there $Z(p)$ can only have one point and thus p is maximal.

To prove the claim, let $R = K[x, y]/(f)$. g maps to something non zero in R. We want to show that there are only finitely many maximal ideals containing g in R.

R has transendence dimension 1 over K. (in other words, R is an algebraic extension of $K[x]$). Noetherian normalization gives R is a finite extension of $K[t]$. Write g as a root of

$$g^n + ... + b_1 g + b_0 = 0, b_i \in K[t].$$

Then all maximal ideals containing g must contain b_0. But there are only finitely many maximal ideals in $K[t]$ that contain b_0. Moreover for each maximal ideal $n \subseteq K[t]$ we have finitely many ideals in R contracting to n (this is by the fact that R is a finite $K[t]/n$) algebra.

16 Recap before midterm

> "if you need to miss class because of an exam feel free to tell me so I can do non-essential stuff" – GOAT

Recaps

Definition 16.1 (Integral)

Let $A \subseteq B$. We say $\alpha \in B$ is **integral** over A if α satisfies a **monic** polynomial in $A[x]$.

Proposition 16.2

$\alpha \in B$ is integral over A if and only if there is a faithful $A[x]$-submodule of B which is finitely generated as an A module.

From this proposition we deduce:

Theorem 16.3

The set of $\alpha \in B$ integral over A is an A-subalgebra.

Definition 16.4 (Finiteness)

B is a **finite** A-algebra if B is finitely generated as an A-module.

Proposition 16.5

B is a finite A-algebra if and only if it is finitely generated as an A algebra and every $\alpha \in B$ is integral.

Corollary 16.6: If B/A integral and C/B integral then C/A integral.

Corollary 16.7: Let $S \subset A$ multiplcatively closed. Then if B/A integral then $S^{-1}B$ is integral over $S^{-1}A$.

Definition 16.8 (Integrally closed)

Let A be an integral domain. Then A is **integrally closed/normal** if all integral elements in FracA are in A.

Example 16.9

UFDs $(\mathbb{Z}[i], \mathbb{Z}[x], \mathbb{C}[x_1, ..., x_n])$ are integrally closed.
$\mathbb{Z}[\sqrt{5}]$ is not integrally closed. The fraction field contains $(1+\sqrt{5})/2$ which satisfies $x^2 - x - 1$.
$\mathbb{C}[x, y]/(y^2 - x^3)$ is not normal. Can confirm that this ring is $\mathbb{C}[t^2, t^3]$ (send $x \mapsto t^2, y \mapsto t^3$ and check kernel). But the fraction field contains t and satisfies monic polynomial. In general

$\mathbb{C}[x,y]/(y^2 - f(x))$ is integrally closed if and only if f is square-free.

Proposition 16.10

Let A and B domains, and that B/A integral, then A is a field if and only if B is a field.

Remark. *Non example:* $\mathbb{C}[x]/(x^2+1)$ *is integral over* $\mathbb{C}$ *but has zero divisors.*

Corollary 16.11: Let $A \subseteq B$ domains and B/A integral. Then every element in Frac(B) is of the form b/a for $b \in B$ and $a \in A$.

Proof. Localize with $(A - \{0\})^{-1}$. Then $A^{-1}B$ is integral over the field of fractions, so is a field and is thus the field of fractions. ✿

Proposition 16.12

Let $A \subseteq B$ integral extension. Let $q \subset B$ prime and $p = q \cap A$. Then p is maximal if and only if q is maximal.

Proof. B/q is integral over A/p. Both are domains. Now apply the previous proposition. ✿

Proposition 16.13

Let B/A integral. Let prime $p \subset A$. There is prime $q \subset B$ that pullsback to p.

Proposition 16.14

Let B/A integral. Let primes $q \subseteq q' \subset B$. Then if they pullback to the same ideal in A they are the same ideal.

Example 16.15

You can have multiple ideals pulling back to the same ideal without inclusion. Take $A = \mathbb{Z}$, $B = \mathbb{Z}[i]$. Then the ideals $(1+2i), (1-2i)$ are both prime and pullback to (5).

Proposition 16.16

Let B be a finite A algebra, then the fibers of spec is finite.

Proof. HW. ✿

Theorem 16.17 (Going Up)

Let B/A integral. Let $q \subseteq B$ prime, $p \subseteq p' \subseteq A$ prime. Also suppose that $q \cap A = p$. Then there exists $q \subseteq q' \subseteq B$ prime such that it contracts to p'.

Proof. Consider A/p and B/q. We have a prime ideal of $\bar{q}' \subseteq B/q$ that contracts to $p'/p \subseteq A/p$. Now take the preimage of $\bar{q}'$ in B. We can check that it contracts to p'. ✿

Theorem 16.18 (Going down)

Let B/A integral. Further assume that A is an integral domain and is integrally closed. Let $q \subseteq B$ prime, $p' \subseteq p \subseteq A$ prime. Also suppose that $q \cap A = p$. Then there exists $q' \subseteq q \subseteq B$ prime such that it contracts to p'.

Corollary 16.19: Going up and down also holds for extending chains by induction.

Theorem 16.20 (Noetherian Normaliztion)

Let K be a field, R a finitely generated K algebra. Then R is finite over a polynomial algebra.

Remark. *This theorem is powerful for when R is a domain. $K[x_1, ..., x_n]$ is integrally closed (UFD). Therefore you can apply going up and going down to extend chains of prime ideals in $K[x_1, ..., x_n]$.*

In the chain of prime ideals, the inclusion in R is strict if and only if the inclusion in $K[x_1, ..., x_n]$ is strict.

Theorem 16.21

Let B/A integral. Then TFAE:

1. Any maximal chain of prime ideals in A consists of $n + 1$ prime ideals.
2. Any maximal chain of prime ideals in B consists of $n + 1$ prime ideals.

Remark. *this is not true :)*

Theorem 16.22

Let R be an integral domain which is finitely generated as a K algebra. Then any maximal chain of prime ideals in R has $1 + d$ elements where d is the transendence degree of Frac(R).

Definition 16.23 (Krull Dimension)

Let R be a ring. The **Krull dimension** of R is the length of the maximal chain of prime ideals minus 1.

17 Dimension

Goal of today: Recall the definition of Krull Dimension.

Definition 17.1 (Krull Dimension)

Let R be a ring. The **Krull dimension** of R is the length of the maximal chain of prime ideals minus 1.

Remark. *Krull dimension of a field is* 0. *The Krull dimension of a PID is* 1.

We want to prove the following result.

Theorem 17.2

Let R be an integral domain which is finitely generated as a K algebra. Then

1. Any two maximal chains of prime ideals have the same length.
2. The Krull dimension of R is the transendence degree of Frac(R).

Lemma 17.3

Let p be a minimal non-zero prime ideal of $K[x_1, ..., x_n]$. Then p is principal.

Proof. Let $\alpha \in p$. By UFD property we can write $\alpha = f_1 ... f_n$, where each f_i is prime. WLOG by primality of p we set $f_1 \in p$. So p contains a prime element f. Then $p \supset (f)$. By minimality $(f) = p$. ❀

Corollary 17.4: Let R be a unique factorization domain. Then every minimal prime ideal is principal.

Lemma 17.5

Let $(p) \subset K[x_1, ..., x_n]$ be a principal prime ideal. The transendence degree of Frac $K[x_1, ..., x_n]/(p)$ is $n-1$.

Proof. Exercise. Suppose p contains every variable x_i. Then every element (p) contains every variable x_i. So that $[x_1], ..., [x_n]$ are algebraically independent in $K[x_1, ..., x_n]/(p)$. So the transendence degree is at least $n-1$.

But since we have x_n dependent with the remaining $[x_i]$'s and they generate $K[x_1, ...x_n]/(p)$, the transendence degree is less than n.

If p does not contain every variable, then consider p in $K[x_1, ..., x_m]$ and set

$$\frac{K[x_1, ..., x_m]}{(p)}[x_{m+1}, ..., x_n] \simeq \frac{K[x_1, ..., x_n]}{(p)}.$$

❀

Lemma 17.6

Let $p \subset R$ be a minimal prime ideal. The transendence degree of Frac R/p is $n-1$.

Proof. $p \cap K[x_1, ..., x_n]$ is minimal. If not, apply going down. Then R/p is integral over $R/(p \cap K[x_1, ..., x_n])$ which has transendence degree $n-1$. ❀

Proof of theorem 17.2. By Noetherian normalization, R is finte over some $K[x_1, ..., x_n]$. Thus by 16.21 it suffices to show that any maximal chain of prime ideals in R has $n+1$ ideals.

We induct on the transendence degree of Frac $R = n$. It is obviously true for $n = 0$, as fields have chains of length 1.

Now if it works for $n-1$, we obtain a minimal prime ideal p which is principal.

Now the remaining chain of prime ideals corresponds to a maximal chain of prime ideals in $K[x_1, ..., x_n]/(p)$ which has transendence degree $n-1$. So the maximal chain has $n+1$ ideals. ❀

18 Exam review

Example 18.1 (Computing Krull Dimension)

The Krull dimension of $K[x_1,...,x_n]$ is n. This is because we have a maximal chain

$$(0) \subset (x_1) \subset (x_1,x_2) \subset ... \subset (x_1,...,x_n) \subset K[x_1,...,x_n].$$

This is because (x_1) is principal, and if there is a minimal prime ideal within this, then x_1 would be a multiple of the generator.
Now we mod everything by (x_1), in $K[x_1,...,x_n]/(x_1) \simeq K[x_2,...,x_n]$ we get the ideals

$$(0) \subset (x_2) \subset (x_2,x_3)...$$

inductively x_2 is minimal prime ideal.
Another algebra: $K[x_1,...,x_n]/(x_1^2+...+x_n^2)$ for $n \geq 3$. The images of $x_1,...,x_{n-1}$ are algebraically independent. However, $x_1,...,x_n$ is not algebraically independent.
If you mod out by more quotients, we would expect with high probability that each polynomial reduces the transendence degree by 1.

Remark. *The next homework should not include exam material, probably.*

Remark. *You should be need to prove the intersection of theorems of the prelim syllabus and the theorems we have seen in class.*

Example 18.2

Look at $\max\operatorname{Spec} K[x_1,...,x_n] \simeq K^n$. Now if R integral over $K[x_1,..,x_n]$ we have a surjection into K^n with finite fibers. So $\max\operatorname{Spec} R$ is somewhat n-dimensional.

Example 18.3

Homeomorphism between spec is not enough to show homeomorphism between rings. Take two fields F_1, F_2 of the same cardinality (but not characteristics). The spec $F_1[x]$ is $p_1 + F_1$, resp. $p_2 + F_2$. The open sets are generated by $p +$ finitely many points . Now take any bijection between F_1 and F_2.

19 Limits

One of the hardest questions on the exam was the second question:

Example 19.1 (Midterm question 2)

Show that Spec R is disconnected if and only if there is a non-trivial idempotent element.

Proof. For the backward direction, let e be non trivial and idempotent. Then take $V(1-e)$ and $V(e)$ disjoint closed sets covering spec.

For the forward direction, let Spec $R = V(I) + V(J)$. Then $I + J = R$ and $IJ \subseteq n(R)$. Let $a \in I, b \in J$ such that $a + b = 1$, and $(ab)^k = 0$.

Then consider $1 = (a+b)^k = a^k + b^k + ab(\text{something})$. Therefore $a^k + b^k$ is 1 plus a nilpotent element which means it is a unit. Set s to be the inverse, then we have

$$sa^k = sa^k s(a^k + b^k) = s^2 a^{2k}.$$

a is not zero or unit, so we are done.

Remark. *Moral of the story: if you have nilpotent elements, usually raise it to that power or a multiple of the power.*

Check Aluffi on limits and stuff.

> The cool people call direct limits "colimits" and inverse limits "limits". I have no idea why. - Ananth Shankar, 2025

Definition 19.2 (Limits and colimits)

A limit is a terminal/final object in a slice category. A colimit is a final object in a slice category.

Definition 19.3 (Directed system)

A directed system gives maps for $i \leq j$, $\psi_{i,j} : R_i \to R_j$ that satisfy $\psi_{j,k}\psi_{i,j} = \psi_{i,k}$, and $\psi_{i,i}$ is the identity.

Definition 19.4 (Direct Limit)

The direct limit is given by

$$\varinjlim_i R_i = \cup R_i / \sim,$$

where the equivalence relation is $a_i \in R_i \sim a_j \in R_j$ if $\exists k$ s.t. $i \leq k, j \leq k$ and $\psi_{i,k}(a_i) = \psi_{j,k}(a_j)$.
This is equipped with injections

$$\iota_i : R_i \to \varinjlim_i R_i$$

by the natural embedding.

Proposition 19.5 (Universal property of direct limits)

Let I be a directed set and $R_i : i \in I$ be a direct system of Rings. The direct limit satisfies the following universal property:

> Let A be a ring and maps $f_i : R_i \to A$. Then there exists $f : \varinjlim_i R_i \to A$ such that the following diagram commutes.

$$\begin{tikzcd}
R_i \arrow[d, "\iota_i"] \arrow[dr, "f_i"] & \\
\varinjlim_i R_i \arrow[r, dashed, "f"'] & A
\end{tikzcd}$$

Remark. *We can use a different formulation here. We define the direct limit to be the initial object of the slice category defined by the commutative diagram*

$$\begin{tikzcd}
\dots \arrow[r] \arrow[drr] & R_3 \arrow[r] \arrow[dr] & R_2 \arrow[r] \arrow[d] & R_1 \arrow[dl] \\
 & & X &
\end{tikzcd}$$

(used 1,2,3 indices for simplicity) Then colimit satisfies the universal property of direct limits. By uniqueness this will be the direct limit up to isomorphism. Then we can verify that the definition of the direct limit indeed satisfies this universal property of being an initial object, thus direct limit exists.

Similarly, the inverse limit is the final object of the slice category of

$$\begin{tikzcd}
\dots & R_3 \arrow[l] & R_2 \arrow[l] & R_1 \arrow[l] \\
 & & X \arrow[ull] \arrow[ul] \arrow[u] \arrow[ur] &
\end{tikzcd}$$

Example 19.6

Let A be a ring, and $S \subset A - \{0\}$ multiplicatively closed and contains 1.
Express $S^{-1}A$ as a direct limit of rings. I.e. $A_f, f \in S$.
where $r_1 \leq r_2$ if $r_2 = r_1 a$. Should have maps $A_{r_1} \to A_{r_2}$.

Proof. exercise.

Example 19.7

Let $S = \{K \subseteq \mathbb{C} st [K : \mathbb{Q}] \text{finite}\}$. With partial order on inclusion.
Then $\overline{\mathbb{Q}}$ is the direct limit of this system.

Definition 19.8 (Inverse Limit)

For a directed system with morphisms $\psi_{i,j} R_i \to R_j$ for $i \geq j$, the inverse limit is given by the subset

$$\varprojlim_i R_i \overset{\text{def}}{=} \{r \in \prod_{i \in I} R_i : r = (r_i)_{i \in I}, \psi_{i,j}(r_i) = r_j\}.$$

This is equippend with the projection maps

$$\pi_i : \varprojlim_i R_i \to R_i.$$

Example 19.9

Consider the chain of maps

$$R/(p)^n \to R/(p)^{n-1}.$$

The inverse limit

$$\varprojlim_n \mathbb{Z}/p^n\mathbb{Z} \overset{\text{def}}{=} \mathbb{Z}_p \subseteq \prod_n \mathbb{Z}/p^n\mathbb{Z}$$

with for each element $a = (..., a_3, a_2, a_1)$ we have $a_n \mapsto a_{n-1}$.
This is a ring with addition, multiplication ptwise, zero element all zeros, 1 element all 1s.

Proposition 19.10 (Universal Property of Inverse Limit)

The inverse limit is a limit in the slice category. I.e. it satisfies the universal property of being a terminal object.

Proposition 19.11

There is an injection for $\mathbb{Z} \to \mathbb{Z}_p$.

Proof. Let $n \in \mathbb{Z}$ map to 0 in $\mathbb{Z}_p$. Then n divides every power of p. By unique factorization, n is zero. ✿

Proposition 19.12

$\mathbb{Z}_p$ is in integral domain.

Proof. Let $a, b \neq 0$ in $\mathbb{Z}_p$. Then for some entry a_i and b_i onwards these enties are not zero. Consider $a_{2i}b_{2i}$. p^i does not divide a_{2_i} so p^{2i} does not divide $a_{2i}b_{2i}$ by unique factorization. ✿

20

Example 20.1

Let $I \subseteq R$ ideal. For every $n \in \mathbb{N}$ let $R_n \overset{\text{def}}{=} R/I^n$.
We have a directed set indexed by $\mathbb{N}$ and (natural) projections

$$R/I^m \overset{\pi_{m,n}}{\to} R/I^n$$

for $m \geq n$.
Then the inverse limit is

$$\varprojlim_n R_n \overset{\text{def}}{=} \hat{R}^{/I} \subseteq \prod_n R_n$$

such that each element $(..., x_2, x_1, x_0)$ satisfies $\pi_{m,n}(x_m) = x_n$ for $m \geq n$.

We restate the universal property of the inverse limit (Proposition 19.10).

Proposition (Universal property of Inverse Limit)

The inverse limit is a limit in the slice category. I.e. it satisfies the universal property of being a terminal object.
Concretely, let A be any ring with homomorphisms $f_n : A \to R_n$ commuting with $\pi_{m,n}$. Then there is a unique map of $f : A \to \hat{R}^{/I}$ such that $f_n = \pi_n \circ f$.

Proof. The inverse limit is evidently a ring with addition and multiplication entry-wise.
The universial property is left as exercise... TODO.

Corollary 20.2: There is a canonical map from $R \to \hat{R}^{/I}$.
This map is given by

$$r \mapsto (..., r \mod I^n, ...)$$

and has kernel

$$\bigcap_n I^n.$$

Remark. *The map is not necessarily surjective.*
Consider $\mathbb{Z} \subset \mathbb{Z}_{(p)}$. Then we have the diagram

$$\begin{tikzcd}
\mathbb{Z} \arrow[r] \arrow[d, hook] & \mathbb{Z}/p^n \arrow[d, "\simeq"] \\
\mathbb{Z}_{(p)} \arrow[r] & \mathbb{Z}_{(p)}/p^n
\end{tikzcd}$$

So the natural inclusion into the localization is a morphism in the slice category. Thus we have

$$\begin{tikzcd}
\mathbb{Z} \arrow[r] \arrow[d] & \mathbb{Z}_p \arrow[r, phantom, "="] & \varprojlim_n \mathbb{Z}/p^n \\
\mathbb{Z}_{(p)} \arrow[ur] & &
\end{tikzcd}$$

In general, this is even bigger than the localization of $\mathbb{Z}$. Hensel's lemma gives a compatible sequence of numbers $b_n \in \mathbb{Z}/19^n\mathbb{Z}$ with $b_n^2 \equiv 6 \mod 19^n$. Thus $\mathbb{Z}_p$ has irrational numbers.

Definition 20.3 (I-adic topology)

Fix $I \subseteq R$ ideal. We give $\hat{R}^{/I}$ a topological ring structure. We give a basis of neighborhoods around 0, then the translation $+r$ gives a basis of neighborhoods around r for each r. The union of all these generates a topology known as the ***I*-adic topology**.
Concretely, the basis around 0 is

$$\{\{\ker \hat{R}^{/I} \to R/I^n\}\}.$$

Proposition 20.4

$\hat{R}^{/I}$ is complete with respect to this topology.

Example 20.5

As an example of ‘completeness’, consider $R = \mathbb{Z}, I = (p)$. The topology on $\mathbb{Z}_p$ is induced by a metric (two numbers are close if their difference is a multiple of a big power of p). Each Cauchy sequence may not converge in $\mathbb{Z}$ but will converge in $\mathbb{Z}$.

TODO: spec of $\mathbb{Z}_p$.

21 Adjointness

Notation. *Let R be a ring. We work in R-mods.*

Proposition 21.1

Let $A \xrightarrow{f} B \xrightarrow{g} C$. Then if $\mathrm{Hom(C,M)} \xrightarrow{(-)\circ g} \mathrm{Hom(B,M)} \xrightarrow{(-)\circ f} \mathrm{Hom(A,M)}$ is exact, the original sequence is exact too.

Proof. Let $a \in A$. Then pick $M = B/f(a) = B'$, and consider the quotient map $(B \xrightarrow{\pi} B') \in \mathrm{Hom(B,B')}$. Then $\pi \circ f \equiv 0$. So we have a lift $\pi' : C \to B'$.

$$\begin{tikzcd}
 & C \arrow[d, dashed, "\pi'"] & & \\
B \arrow[ur, "g"] \arrow[r, "\pi"'] & B' & = & B/f(A)
\end{tikzcd}$$

But then this means π factors through $\mathrm{ker(g)}$. So that $\mathrm{Im(f)} \supseteq \mathrm{ker(g)}$.

For the other inclusion, take $M = C$. The identity from $C \to C$ maps to $g \circ f$ becomes zero by exactness.

Proposition 21.2 (assigned as exericse)

The contravariant functor $\mathrm{Hom(-,N)}$ sends right exact sequences to left exact sequences.

Proof. Let $A \xrightarrow{f} B \xrightarrow{g} C \to 0$. We want

$$0 \to \mathrm{Hom(C,N)} \to \mathrm{Hom(B,N)} \to \mathrm{Hom(A,N)}$$

exact. Let $\alpha : C \to N$. Because g is an epimorphism (surjective) we have for $\alpha \circ g = 0 = 0 \circ g \implies \alpha = 0$. So we have exactness at $\mathrm{Hom(C,G(M))}$.

For the exactness at B, the composite is zero from $g \circ f = 0$. This gives one inclusion. Now let $\alpha : B \to N$ such that $\alpha \circ f = 0$. Then $\mathrm{ker(g)} = \mathrm{Im(f)} \subseteq \mathrm{ker}(\alpha)$. By the mapping property of quotients we have a lift

$$\begin{tikzcd}
B \arrow[r, "g"] \arrow[dr, "\alpha"'] & B/\mathrm{ker(g)} \arrow[d, dashed] & = & C \\
 & M & &
\end{tikzcd}$$

Similarly we have the same statement for the covariant functor

Proposition 21.3 (assigned as exericse)

In R-mod, $A \xrightarrow{f} B \xrightarrow{g} C$ is exact if $\mathrm{Hom(N, A)} \to \mathrm{Hom(N, B)} \to \mathrm{Hom(N, C)}$ is exact for all N.

Proof. For the first inclusion, take $N = A$, so then we have $g \circ f = 0$ by considering the identity from $A \to A$. Now we want $\mathrm{ker\ g} \subseteq \mathrm{im\ f}$. Pick $N = \mathrm{ker\ g}$. Then the composite $N \to B \to C$ is zero, so has a lift $N \to A \to B \to C$.

$$\begin{tikzcd}
& \mathrm{ker\ g} \arrow[dl, dashed] \arrow[d, hook] & \\
A \arrow[r] & B \arrow[r] & C
\end{tikzcd}$$

But this is a lift of the embedding of ker g into B, so the kernel of g is a subset of the image of f. 🌸

Proposition 21.4 (assigned as exercise)

The covariant functor $\mathrm{Hom(N, -)}$ sends left exact sequences to left exact sequences.

Proof. Let $0 \to A \xrightarrow{f} B \xrightarrow{g} C$. We want

$$0 \to \mathrm{Hom(N, A)} \to \mathrm{Hom(N, B)} \to \mathrm{Hom(N, C)}$$

exact. Because f is injective, this is an monomorphism so we have $\mathrm{Hom(N, A)} \to \mathrm{Hom(N, B)}$ injective. This gives exactness at $\mathrm{Hom(N, A)}$.

For exactness at B, we have that the composition $g \circ f = 0$, so that gives one inclusion. For the other inclusion, let $N \xrightarrow{h} C$ such that $g \circ h = 0$. Then $\mathrm{Im\ h} \subseteq \mathrm{ker\ g} = \mathrm{Im\ f}$. f is injective, so we can identify Im f with its preimage in A. This gives us a factoring of h through Im f in A. 🌸

Definition 21.5 (Adjoint)

Let $\mathcal{C}, \mathcal{D}$ categories. Let $F : \mathcal{C} \to \mathcal{D}$ and $G : \mathcal{D} \to \mathcal{C}$ functors. We say F is a left adjoint of G and G is a right adjoint of F if

$$\mathrm{Hom(F(x), y)} \overset{\text{natural isom}}{\simeq} \mathrm{Hom(x, g(y))}$$

Remark. *As a recall natural isomorphism means that for every pair* $(x, y) \in \mathcal{C} \times \mathcal{D}$ *there is an isomorphism* $\eta_{x,y} \in \mathrm{Hom_{Set}Hom(F(x), y), Hom(x, G(y))}$ *such that the following square commutes for every pair of morphisms* $(f, g) \in \mathrm{Hom}_{\mathcal{C}}(\mathrm{x_1, x_2}) \times \mathrm{Hom}_{\mathcal{D}}(\mathrm{y_1, y_2})$

$$\begin{tikzcd}
\mathrm{Hom}_{\mathcal{D}}(\mathrm{F(x_1), y_1}) \arrow[r, "\mathrm{Hom}_{\mathcal{D}}(\mathrm{F(f), g})"] \arrow[d, "\eta_{x_1,y_1}"'] & \mathrm{Hom}_{\mathcal{D}}(\mathrm{F(x_2), y_2}) \arrow[d, "\eta_{x_2,y_2}"] \\
\mathrm{Hom}_{\mathcal{C}}(\mathrm{F(x_1), y_1}) \arrow[r, "\mathrm{Hom}_{\mathcal{C}}(\mathrm{f, G(g)})"'] & \mathrm{Hom}_{\mathcal{C}}(\mathrm{F(x_2), y_2})
\end{tikzcd}$$

Theorem 21.6

In the setting of R-Mods, S-Mods, let F, G adjoints. Then G is left exact and F is right exact.

Proof. F is right exact: Let $A \xrightarrow{f} B \xrightarrow{g} C \to 0$. We want $F(A) \to F(B) \to F(C) \to 0$ exact, so want to show that

$$0 \to \mathrm{Hom(F(C), M)} \to \mathrm{Hom(F(B), M)} \to \mathrm{Hom(F(A), M)}$$

exact for every $M \in \mathcal{D}$.

By adjointness, this is equivalent to saying that

$$0 \to \mathrm{Hom(C, G(M))} \to \mathrm{Hom(B, G(M))} \to \mathrm{Hom(A, G(M))}$$

is exact for every M. But this is a direct result of (let $N = G(M)$) the (left) exactness of the functor $\mathrm{Hom(-, N)}$.

For the left exactness of G, we want

$$0 \to G(A) \to G(B) \to G(C)$$

exact, so we want to show exactness of

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Hom(N, G(A))} \arrow[r] \arrow[d, "\simeq"] & \mathrm{Hom(N, G(B))} \arrow[r] \arrow[d, "\simeq"] & \mathrm{Hom(N, G(C))} \arrow[d, "\simeq"] \\
0 \arrow[r] & \mathrm{Hom(F(N), A)} \arrow[r] & \mathrm{Hom(F(N), B)} \arrow[r] & \mathrm{Hom(F(N), C)}
\end{tikzcd}$$

Which is true by the left exactness of the covariant functor. 🌸

22

Proposition 22.1

$\otimes N$ and $\mathrm{Hom(N, -)}$ are adjoints.

Proof. Consider this pair of morphisms. We can check that they are inverses of each other and are well defined, and are natural.

$$\begin{tikzcd}
\mathrm{Hom(A \otimes N, B)} \arrow[r, "\simeq"'] & \mathrm{Hom(A, Hom(N, B))} \\
f \arrow[r, mapsto] & {[a \mapsto (n \mapsto f(a \otimes n))]} \\
a \otimes n \mapsto g(a)(n) & g \arrow[l, mapsto]
\end{tikzcd}$$

🌸

Corollary 22.2: $\otimes M$ is right exact. $\mathrm{Hom(M,-)}$ is left exact.

Example 22.3

Tensoring is not left exact.

$$0 \to \mathbb{Z} \overset{\times 2}{\to} \mathbb{Z}$$

tensored with $\mathbb{Z}/2$ gives

$$0 \to \mathbb{Z}/2 \overset{\times 0}{\to} \mathbb{Z}$$

is not exact.

Definition 22.4 (Free resolution)

Let M be an R module. A **free resolution** is an exact sequence

$$... \to F_2 \to F_1 \to M \to 0$$

such that each F_i is free.

Remark. *In fact we only need F_i's to be projective.*

Definition 22.5 (Derived Functor (Tor))

Let M, N be R-modules. Take a free resolution of M and tensor with N.

$$\begin{tikzcd}
... \arrow[r] & F_2 \arrow[r] \arrow[d, Rightarrow, "\otimes N"] & F_1 \arrow[r] & M \arrow[r] & 0 \\
... \arrow[r] & F_2 \otimes N \arrow[r] & F_1 \otimes N \arrow[r] & M \otimes N \arrow[r] & 0
\end{tikzcd}$$

The i-th homology of this complex is the $\mathrm{Tor^i}$, with the exception that Tor^0 is the homology at $F_2 \otimes N \to F_1 \otimes N \to 0$ which is $M \otimes N$ by the right exactness of tensoring.

Remark. *Tor is symmetric and distributes over direct sums. This is because the original functor ($\otimes N$) also has these properties.*

Example 22.6 (Tor for PIDs)

Let R be a PID. M a finitely generated R-module. Then write

$$M = M^{\text{free}} \oplus M^{\text{torsion}}$$

where

$$M^{\text{torsion}} \simeq \oplus R/(p_i^{a_i}).$$

We have $\mathrm{Tor^i(M^{free}, N)} = 0$ for $i \geq 1$. This is because it is already a free resolution.
On the torsion part, we work with each $R/(p^a)$ piece separately.
We get the free resolution

$$... \to 0 \to R \overset{\times p^a}{\to} R \to R/a \to 0$$

We tensor this with N. $\mathrm{Tor^2(R/(p^a),N)}$ and above vanish. The special case is Tor^1 which is the kernal of $R \otimes N \overset{\times p^a}{\to} R \otimes N$.
But as N is already an R module, we have isomorphisms

$$\begin{tikzcd}
r \otimes n \arrow[d, mapsto] & R \otimes N \arrow[r, "p^a"] \arrow[d, "\simeq"'] & R \otimes N \arrow[d, "\simeq"] \\
r \cdot n & N \arrow[r, "p^a"'] & N
\end{tikzcd}$$

So that $\mathrm{Tor^1(R/(p^a),N) = \{n \in N : p^a n = 0\}}$.
The same argument goes through for $\mathrm{Tor(R/(a),N)}$ for any principal ideal a.

Proposition 22.7

Let R be an integral domain, $a \in R$. Then as R-modules

$$\mathrm{Tor^1(R/(a),N) = \{n \in N : an = 0\}},$$

and 0 for degrees 2 and above.

Example 22.8

Over $\mathbb{Z}/8$ modules, a free resolution of $\mathbb{Z}/2$ is

$$\ldots \overset{\times 2}{\to} \mathbb{Z}/8 \overset{\times 4}{\to} \mathbb{Z}/8 \overset{\times 2}{\to} \mathbb{Z}/8 \to \mathbb{Z}/2 \to 0$$

Tensoring with N would be multiplication by 2 and 4 (alternating).

23

Example 23.1 (Calculating Tor)

Let $R = K[x,y]$. We want to find $\mathrm{Tor}(\mathrm{K},\mathrm{K})$.
We have a free resolution

$$\begin{tikzcd}
 & 1 \arrow[r, mapsto] & (y,-x) \arrow[r, mapsto] & 0 & & & \\
...0 \arrow[r] & R \arrow[r] & R^2 \arrow[r] & R \arrow[r] & R \arrow[r, two heads] & K \arrow[r] & 0 \\
 & & (a,b) \arrow[r, mapsto] & (ax+by) & & &
\end{tikzcd}$$

Tensor with K and we get

$$\begin{tikzcd}
0 \arrow[r] & K \arrow[r, "0"] & K^2 \arrow[r, "0"] & K \arrow[r] & 0
\end{tikzcd}$$

The boundary maps $\times x, \times y$ all become the zero maps. So we have the homology is exactly the module in the respective degree.

Example 23.2

As an exercise, calculate Tor of (m, K) and (K, m), for $m = (x,y)$. (this will be on final w.h.p) Verify that they are the same.

Tor and long exact sequences

Theorem 23.3 (Long Exact Sequence of Tor)

Let $0 \to M' \to M \to M'' \to 0$ exact. We have a long exact sequence

$$\begin{tikzcd}
 & & \cdots \arrow[dll] & \\
\mathrm{Tor}^2(\mathrm{M}',\mathrm{N}) \arrow[r] & \mathrm{Tor}^2(\mathrm{M},\mathrm{N}) \arrow[r] & \mathrm{Tor}^2(\mathrm{M}'',\mathrm{N}) \arrow[dll] & \\
\mathrm{Tor}^1(\mathrm{M}',\mathrm{N}) \arrow[r] & \mathrm{Tor}^1(\mathrm{M},\mathrm{N}) \arrow[r] & \mathrm{Tor}^1(\mathrm{M}'',\mathrm{N}) \arrow[dll] & \\
M' \otimes N \arrow[r] & M \otimes N \arrow[r] & M'' \otimes N \arrow[r] & 0
\end{tikzcd}$$

Proof. Take a free resolution of N

$$F_3 \to F_2 \to F_1 \to N \to 0$$

We tensor this with the exact seqeunce

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

and get the exact sequence of complexes

$$\begin{tikzcd}
 & \cdots \arrow[d] & \cdots \arrow[d] & \cdots \arrow[d] & \\
0 \arrow[r] & F_3 \otimes M' \arrow[r] \arrow[d] & F_3 \otimes M \arrow[r] \arrow[d] & F_3 \otimes M'' \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & F_2 \otimes M' \arrow[r] \arrow[d] & F_2 \otimes M \arrow[r] \arrow[d] \arrow[d, dotted, shift left=2] & F_2 \otimes M'' \arrow[r] \arrow[d] \arrow[l, dotted, shift left=2, "lift"] & 0 \\
0 \arrow[r] & F_1 \otimes M' \arrow[r] \arrow[d] & F_1 \otimes M \arrow[r] \arrow[d] \arrow[l, dotted, shift left=2] & F_1 \otimes M'' \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

Where the homology of each complex is exactly the derived Tor functors. We take the long exact sequence of this short exact sequence and we are done.

The boundary map from $\mathrm{Tor^{i+1}(M'', N)} \to \mathrm{Tor^{i}(M', N)}$ is defined through the pink arrows. 🌸

Remark. *I dont want to diagram chase. Just take homology functor for granted.*

Let me know if you really want the proof in the notes and I'll write it up. There is a possibility it'll be in the hw anyway.

Remark. *The only part in the proof that requires special properties of tensoring is that the exactness at each level is kept (free modules are flat).*

> Go to a quiet place. Put some music on, and go through the entire proof yourself. - Ananth Shankar, 2025

Corollary 23.4: Fix M. If $\mathrm{Tor^1(M, N)} = 0$ for all N, then M is flat.

Proof. Take any short exact sequence

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

the long exact sequence here preserves

$$0 \to M \otimes N' \to M \otimes N \to M \otimes N'' \to 0$$

🌸

24 Hom and Ext

Let M be an R-module. The functor $\mathrm{Hom(M, -)}$ is covariant and the functor $\mathrm{Hom(-, M)}$ is contravariant.

Both are left exact (see Propositions 21.2 and 21.4).

Definition 24.1 (Injective modules)

I is injective if there exists a dotted arrow for every solid diagram of the following.

$$\begin{tikzcd}
& I & \\
0 \arrow[r] & A \arrow[u] \arrow[r, hook] & B \arrow[ul, dashed]
\end{tikzcd}$$

Remark. *Free modules need not be injective. There is an embedding of $\mathbb{Z}$ into $\mathbb{Q}$ but the identity map $\mathbb{Z} \to \mathbb{Z}$ does not lift to $\mathbb{Q} \to \mathbb{Z}$.*

In general for an integral domain R,

$$\begin{tikzcd}
& I & \\
0 \arrow[r] & R \arrow[u, "1\mapsto n"] \arrow[r, "1\mapsto r"'] & \text{Frac(R)} \arrow[ul, dashed, "1\mapsto n'"']
\end{tikzcd}$$

means that we need $n' \in I$ such that $rn' = n$.

Definition 24.2 (Divisible)

Let R be an integral domain. I is divisible if for every $n \in I$, $r \in R \backslash \{0\}$, there is $n' \in I$ s.t. $rn' = n$.

Proposition 24.3

Let R be integral domain. Then injective modules are divisible.

Example 24.4

As $\mathbb{Z}$ modules, $\mathbb{Z}^k, \mathbb{Z}/n$ modules are not divisble.
$\mathbb{Q}^k, \mathbb{Q}/\mathbb{Z}$ are divisible.

An injective resolution of $\mathbb{Z}/n$ is

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{Z}/n \arrow[r] \arrow[d, phantom, "\simeq"] & \mathbb{Q}/\mathbb{Z} \arrow[r, "n"'] & \mathbb{Q}/\mathbb{Z} \arrow[r] & 0 \\
& \frac{1}{n}\mathbb{Z}/\mathbb{Z} & & &
\end{tikzcd}$$

Definition 24.5 (Projective Module)

P is projective if there is a dotted arrow for every solid diagram

$$\begin{tikzcd}
& P \arrow[d] \arrow[dr, dashed] & \\
0 & A \arrow[l] & B \arrow[l, two heads]
\end{tikzcd}$$

Proposition 24.6

I is projective $\iff$ Hom $(I,-)$ is exact.
Similarly P is injective $\iff$ $\mathrm{Hom}(-,P)$ is exact

Proof. Both functors fail to be exact at the right side. But the last map of Hom's being surjective is equivalent to saying that the module is projective/injective.

Ext measures the failure of $\mathrm{Hom}(M,-)$ and $\mathrm{Hom}(-,N)$ to be exact.

Definition 24.7 (Ext functor)

Let M,N modules, use a free resolution of M and apply with $\mathrm{Hom}(-,N)$ functor.

$$\begin{tikzcd}
\dots \arrow[r] & P_2 \arrow[r] & P_1 \arrow[rr] & \arrow[d, Rightarrow, "\mathrm{Hom(-,N)}"] & P_0 \arrow[r] & M \arrow[r] & 0 \\
\dots & \mathrm{Hom(P_2,N)} \arrow[l] & \mathrm{Hom(P_1,N)} \arrow[l] & {} & \mathrm{Hom(P_0,N)} \arrow[ll] & \mathrm{Hom(M,N)} \arrow[l] & 0 \arrow[l]
\end{tikzcd}$$

We define

$$\mathrm{Ext^i(M,N)} \overset{\mathrm{def}}{=} \mathrm{H_i}$$

the i-th degree (co)homology of this complex.

Remark. $\mathrm{Ext^0(M,N) = Hom(M,N)}$ *by exactness of the functor.*
The result is also the same by taking an injective resolution of N

$$0 \to N \to I_0 \to I_1 \to \dots$$

and applying $\mathrm{Hom(M,-)}$.

Theorem 24.8 (Baer's Criterion)

Let I be an R-module. The following are equivalent

1. I is an injective module.
2. For any ideal $a \subseteq R$, we have a lift

$$\begin{tikzcd}
 & I & \\
0 \arrow[r] & a \arrow[u] \arrow[r, phantom, "\subseteq"] & R \arrow[ul, dashed]
\end{tikzcd}$$

Proof. 1 $\implies$ 2.

We now show 2 $\implies$ 1. Suppose I satisfies 2. Let $A \xrightarrow{f} I$, and A injects into B. Let $S = \{A', f' : A \subseteq A' \subseteq B, f' : A' \to I \text{ extends } f\}$, with partial order by inclusion. Every chain has an upper bound so we can apply zorn's lemma to find a maximal $A' \subseteq B$, $f' : A' \to I$ that extends A. We want to show $A' = B$. Suppose not, then let $b \in B$ that is not in A'.

Let $a = \{r \in R : rb \in A'\}$.

We have a map $a \xrightarrow{g'} I$ that sends $r \mapsto f'(rb)$. This is well defined because $rb \in A'$ and can be lifted (by hypothesis) to $R \to I$.

Define

$$h : A' + Rb \to I$$

by $h(a_0 + rb) = f'(a_0) + g'(r)$.

We can check that this is well defined and extends f', which is a contradiction. 🌸

Corollary 24.9: Let R be a principal ideal domain and I be divisible. Then I is injective.

Proof. All ideals are of the form (r). This lifts by divisibility. Now apply Baer's Criterion. 🌸