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, Zarski topology/spec, tesor products.
3. Further topics include: Noether's normalization, going up and going down, completions of rings, dimension theory, Zarski'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

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

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

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

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* $p, p^{1/2}, p^{1/3}....$ *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

$$m_1 = j_1m_1 + j_2m_2 + ... + j_nm_n.$$

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

$$(1 - j_1)m_1 = j_2m_2 + ... + j_nm_n.$$

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 $\{a/b : p \text{ does not divide } b\}$. 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

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

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

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

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 guarantees 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 $S^{-1}M$

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

with the equivalence

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

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

Notation. *If $S = A/p$ for some prime ideal p, we write $A_p \stackrel{\text{def}}{=} S^{-1}A, M_p \stackrel{\text{def}}{=} S^{-1}M$. 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 $\mathrm{Ann}(x)$. 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* $(S^{-1}A \otimes_A M) \otimes_{S^{-1}A} (S^{-1}A \otimes_A N) \simeq S^{-1}A \otimes (M \otimes_A N)$.