MATH 771: Commutative Algebra

Reese Lance

Fall 2022

Abstract

Graduate course in Commutative Algebra taught by Prakash Belkale at UNC-CH. Notes are handwritten during lecture then typeset later. Any comments, concerns, questions, corrections, or communications of any type are encouraged to be directed to my email. These notes are primarily a documentation of my personal learning journey while following along with the class: There is material in this document that did not come from the lecture, and some of the lecture material may not have been included in these notes. Any errors found in the text are assumed to be introduced by me. Nevertheless this should provide some non-zero utility for any and all readers, primarily my future self.

Table of Contents

CHAPTER 1

I. Overview and Ring Theory

Lecture 1, Aug 15.

We will primarily be following 2 books, Aatiyah-Macdonald and Reed's Undergraduate Commutative Algebra. The exercises will be coming from these two books. For further, more advanced reading, consult Eisenbud.

Definition: A ring is a set A with two operations, $+, \cdot$ such that $(A, +)$ is an abelian group and $\cdot$ is associative and distributes over the sum.

If R has a 1, a multiplicative identity, we call it unital. If $\cdot$ is commutative and R has a 1, we call the ring R commutative.

Example: The set of $n \times n$ matrices is a non-commutative ring.

Example: The set $\{0\}$ is a commutative ring with $0 = 1$.

Example: The set of integers, $\mathbb{Z}$, and the Gaussian integers, $\mathbb{Z}[i]$, are commutative rings.

Example: Given a smooth manifold, we get a commutative ring, $C^\infty(M)$, the smooth functions on M. This is commutative because the ring structure is pointwise multiplication, and multiplication in the ground field $\mathbb{R}$ is commutative.

Example: An algebraic variety similarly gives rise to a commutative ring of algebraic/regular functions, but we will see more about this later. We associate the algebraic variety $\mathbb{C} \rightsquigarrow \mathbb{C}[x]$, polynomials with complex coefficients. We can also consider the affine variety $x^2 + y^2 = 1.$. The associated commutative ring is $\mathbb{C}[x, y]/(x^2 + y^2 - 1)$.

Example: If k is an arbitrary commutative field, then $k[x_1, \ldots, x_n]$ is commutative.

Example: The group ring of a group G is defined as set $\{\sum e_g \cdot g\}$, formal expressions with the condition that $g \cdot h = gh$, as defined by the group multiplication law and enforcing distribution rules. If the group G is non-abelian, the group ring need not be commutative[1].

Example: Lie algebras, that is vector spaces equipped with a Lie bracket, are not associative. The Jacobi identity measures the failure of the bracket to be associative.

I think from this point on we assume all rings to be commutative.

Definition: A map $f : A \to B$ is a ring homomorphism if $f(x+y) = f(x) + f(y)$, $f(1) = 1$, and $f(xy) = f(x)f(y)$ for all $x, y \in A$.

Example: Fix $a \in k$. Then $ev_a : k[x] \to k$ is a ring homomorphism, sending $p(x) \mapsto p(a) \in k$. Check ring hom axioms:

$$\begin{gathered} ev_a(p(x) + q(x)) = p(a) + q(a) = ev_a(p(x)) + ev_a(q(a)) \\ ev_a(1) = 1(a) = 1 \\ ev_a(p(x)q(x)) \equiv p(a)q(a) = ev_a(p(x))ev_a(q(x)) \end{gathered}$$

Definition: $S \subset A$ is called a subring if it is closed under $+, \cdot$ and contains 1.

Example: The inclusion $\mathbb{Z} \hookrightarrow \mathbb{C}$ is a ring homomorphism and identifies $\mathbb{Z}$ as a subring of $\mathbb{C}$.

Definition: $I \subset A$ is an ideal if it is closed under $+$ and absorbs under $\cdot$: for any $x \in I, y \in A, xy \in I$. The second condition can be written as $I \cdot A \subset I$.

Proposition: *If $f : A \to B$ is a ring homomorphism, $\ker f$ is an ideal of A.*

Proof: First we claim $0 \cdot a = 0$ for any $a \in A$. Note this was not one of our ring axioms, it is a consequence of the distributive law:

$$0 \cdot a = (0+0) \cdot a = 0 \cdot a + 0 \cdot a \Rightarrow 0 \cdot a = 0$$

Then for any $a \in kerf$ and $b \in A$,

$$f(ab) = f(a)f(b) = 0 \cdot f(b) = 0$$

For any $a, b \in kerf$,

$$f(a+b) = f(a) + f(b) = 0 + 0 = 0$$

□

Example: $\{0\}, A \subset A$ are ideals.

[1] I'd like to explore what statements you can make. Is it that the group ring is commutative iff the group is abelian? Perhaps modulo some pathological counterexamples. Come back to this when I have time.

Definition: If x_α is a collection of elements in A, where α is indexed by some set I, then the ideal generated by x_α, denoted by (x_α), is the ideal

$$\left\{ \sum^{finite} c_\alpha x_\alpha \mid c_\alpha \in A \right\}$$

Note the indexing set I could be infinite, but we still require all sums to be finite, since there are no notions of convergence here.

Example: There is an ideal $(x) \subset k[x]$ for any field k. This is equal to $ker\ ev_0$. Similarly, $(x-a) = ker\ ev_a$.

Definition: If $I \subset A$ is an ideal, then A/I is an abelian group, where the quotient is taken wrt $+$. The quotient ring A/I is formed with the group law of the abelian group A/I and equipped with multiplication law $\bar{a}\bar{b} = \overline{ab}$, where $\bar{a}$ denotes the image of a through the quotient map.
To see this is well defined, take any other representative: $\overline{(a+i)}\bar{b} \equiv \overline{(a+i)b} = \overline{ab+ib} = \overline{ab} + \overline{ib} = \overline{ab}$, and similarly for b.

Example: $k[x]/(x^2)$. This quotient kills all the powers of x greater than or equal to 2. So the resulting ring is

$$k[x]/(x^2) \cong \{\overline{a+bx}\ a, b \in k\}$$

In general, A/I is a ring and $A \to A/I$ is a surjective ring homomorphism with kernel equal to I.

Recall if $H \leq G$ is a subgroup there is a correspondence

$$\{\text{subgroups of G/H}\} \leftrightarrow \{\text{subgroups of } G \text{ containing } H\}$$

Induced by the quotient map $G \to G/H$. Similarly for rings, we have

$$\{\text{ideals of } A/I\} \leftrightarrow \{\text{ideals of } A \text{ containing } I\}$$

CHAPTER 2

II. Ring Theory II

Lecture 2, Aug 17.

Definition: $a \in A$ is a 0-divisor if $a \mid 0$.

Example: In $\mathbb{Z}/7\mathbb{Z}$, 0 is the only 0 divisor. But in $\mathbb{Z}/6\mathbb{Z}$, 2 and 3 are 0 divisors.

Definition: A ring with no 0 divisors is called an integral domain.

Example: In $k[x,y]/(x^2 - y^2)$, $(x+y)$ and $(x-y)$ are 0 divisors, so it is not an integral domain.

Definition: $a \in A$ is nilpotent if $\exists n \in \mathbb{N}$ such that $a^n = 0$.

Example: $6 \in \mathbb{Z}/12\mathbb{Z}$ is nilpotent.

Proposition: *$a \in \mathbb{Z}/m\mathbb{Z}$ is nilpotent iff $m \mid a^n$ for some n.*

Note in general, $m \mid a^n \not\Rightarrow m \mid a$. For example, you can always choose m to be a^n. For this to hold, you need m to be “square-free”.

Definition: $a \in A$ is a unit if $\exists b \in A$ s.t. $ab = 1$.

Definition: $a \in A$ is irreducible if $a = bc \Rightarrow b$ or c is a unit.

Definition: A principal ideal domain (PID) is an integral domain such that all ideals are principal, i.e. generated by one element.

Proposition: *$\mathbb{Z}$ is a PID.*

Proof: Let I be an ideal, and n the smallest positive integer in I. Then claim $I = (n)$. Suppose not. Then by the division algorithm, $\exists a \in I$ s.t.

$$a = bn + r \qquad 0 < r < n$$

$$a - bn = r$$

But $a \in I$ and $bn \in I$, so $r \in I$. But $r < n$ is a contradiction. So $I = (a)$.

□

Definition: A unique factorization domain (UFD) is a ring such that every $a \in A$ factors as a product of irreducibles elements of A, unique up to multiplication by units and permutation.

Proposition: *All PIDs are UFDs.*

Example: $k[x]$ is a Euclidean domain (long division).

In general,

$$\text{Euclidean Domain} \subset \text{PID} \subset \text{UFD}$$

Example: $k[x, y]$ is a UFD but not a PID, because of (x, y). So the second containment is not strict. The first is also not strict, but is a little more involved to show.

Theorem: *A UFD* $\Rightarrow A[x]$ *is a UFD*

Remark: The same is not true when you replace UFD with PID.

Definition: An ideal $P \subset A$ is prime if $ab \in P \Rightarrow a \in P$ or $b \in P$.

Proposition: *P is prime iff A/P is an integral domain.*

Definition: An ideal M is maximal if $M \subsetneq P \subset A \Rightarrow P = A$.

Proposition: *M is maximal iff A/M is a field.*

Proof: $\Rightarrow$:If M is maximal, then for any $[x] \neq 0 \in A/M$, consider $x \in A$. We know $x \notin M$ since $[x] \neq 0$. Then consider the ideal $M + (x)$. This is strictly larger than M, and so must be equal to $A \Rightarrow 1 \in M + (x) \Rightarrow \exists m \in M, a \in A$ such that

$$m + ax = 1 \Rightarrow [m + ax] = [1] \Rightarrow [ax] = [a][x] = 1$$

So $[x]$ is a unit in A/M. $[x]$ is arbitrary so every element in A/M is invertible, so A/M is a field.
$\Leftarrow$: If A/M is a field, and we want to show M is maximal, then consider any $M \subsetneq I \subset A$. Then $I + M$ is an ideal of A/M by the correspondence. But A/M is a field and so there are only two ideals, 0 and A/M, corresponding to $I = M$ and $I = A$, respectively.

□

Corollary: *A maximal ideal is also prime.*

Proof: A field is always an integral domain.

Remark: The opposite implication does not hold, for example $k[x,y]/(y) \cong k[x]$, by the map $f(x,y) \mapsto f(x,0)$. $k[x]$ is an integral domain but not a field, so (y) is a prime but not maximal ideal.

Remark: A is an integral domain iff $(0) \subset A$ is prime.

So if A is an integral domain but not a field, then (0) is prime but not maximal. This occurs, for example, in $\mathbb{Z}$.

Proposition: *If A is a UFD, then (a) is prime iff a is irreducible.*

Proposition: *In an integral domain, (a) prime implies a irreducible.*

Proof: Let $a = bc$. Then $bc \in (a) \Rightarrow b \in (a)$ or $c \in (a)$. WLOG assume $b \in (a)$. Then $b = \ell a$ for some $\ell \in A$. Then

$$a = bc = \ell ac \Rightarrow \ell c = 1$$

noting that we can cancel because we assumed A is an integral domain. This shows c is a unit.

□

Example: $(x^2 - y^2)$ is prime in $k[x,y]$.

Example: Ker $ev_{(a,b,c)} : \mathbb{C}[x,y,z] \to \mathbb{C}$ is a maximal ideal, since the quotient is isomorphic to $\mathbb{C}$. In fact, Ker $ev_{(a,b,c)} = (x-a, y-b, z-c)$. Also in fact, these are all the maximal ideals, and we will see that later.

CHAPTER 3

III. Maximal and Prime Ideals

Lecture 3, Aug 19.

Example: $(0) \subset \mathbb{Z}$ is a prime but not maximal ideal.

Example: Ker ev_p is a maximal ideal.

Proposition: *$\varphi : A \to B$ a ring homomorphism. Then $\varphi^{-1}J$ is an ideal of A if J is an ideal of B.*

Remark: The image of an ideal is not an ideal. Take for example $\mathbb{Z} \hookrightarrow \mathbb{C}$.

Proposition: *With the same setup as above, if P is a prime ideal of B, $\varphi^{-1}P$ is a prime ideal of A.*

Proof: Examine the homomorphism

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[rr, bend right, "g"'] & B \arrow[r, two heads] & B/P \end{tikzcd}$$

We see that Ker $g = f^{-1}(P)$. So you get

$$A/f^{-1}(P) \hookrightarrow B/P$$

which identifies $A/f^{-1}(P)$ as a subring of B/P. But B/P is an integral domain, and any subring of an integral domain is an integral domain.

$\square$

The same result does not hold for maximal ideals, though. As intuition, we may try to replicate the proof above and conclude that

$$A/f^{-1}(M) \hookrightarrow B/M$$

identifying $A/f^{-1}(M)$ as a subring of the field B/M. But a subring of a field need not be a field itself, again taking $\mathbb{Z} \hookrightarrow \mathbb{C}$.

To see concretely why this does not hold, one can consider the usual counterexample of (0) under the inclusion $\mathbb{Z} \hookrightarrow \mathbb{C}$.

Example: $\mathbb{Z}[x] \hookrightarrow \mathbb{C}[x]$. If you think about it, $(x) \leftrightarrow (x)$. But (x) is maximal in $\mathbb{C}$ and not in $\mathbb{Z}$.

Theorem: *Every ring has a maximal ideal.*

Corollary: *If $I \subset A$ is a proper ideal, then I is contained in a unique maximal ideal.*

These proofs rely on Zorn's lemma.

Corollary: *x is not a unit iff x is contained in a maximal ideal.*

Proof: $\Leftarrow$: If x is contained in a maximal ideal, then x must not be a unit, otherwise the ideal which contains it will also contain 1, and thus not be maximal since it will equal the whole ring.
$\Rightarrow$: Consider the ideal $(x) \subsetneq A$, which is proper because x is not a unit. Then apply the above corollary to (x).

□

Definition: A ring A is called a local ring If it has exactly one maximal ideal.

Example: Any field has only two ideals, (0) and F, but F is not proper so there is only one maximal ideal, (0).

Example: Let p be a prime and define[1]

$$\mathbb{Z}_{(p)} := \left\{ \frac{a}{b} \mid a, b \neq 0 \in \mathbb{Z}, p \not| \, b \right\}$$

Claim that $\mathbb{Z}_{(p)}$ is a ring. This is an example of an operation on a ring called localization. And $(p) = \{$ non-units in $\mathbb{Z}_{(p)}\}$ is the unique maximal ideal.

Lemma: *If the non-units of a ring form an ideal, then A is a local ring.*

Proof: First we observe that if the non-units form an ideal, then that ideal must be maximal: If there is an ideal which contains it, it must have come from adding in units, which makes the ideal equal to A. So the non-units form a maximal ideal, and denote this as I. Suppose there is another maximal ideal, J which is not given by the set of all non-units.

[1] This concept tripped me up for quite some time. If you are familiar with the general notion of a localization of a ring, the definition of a localization at a prime ideal, is the general localization of a ring with respect to the compliment of the prime ideal, which is automatically a multiplicative set. In this ring, elements of (p) are not invertible, while for a general multiplicative set $S \subset A$, elements of S in $A_S \equiv S^{-1}A$ are invertible.

But every element of J must not be a unit, as we have argued before. Therefore $J \subset I$, a contradiction.

□

Definition: For a ring A, denote $Spec\ A$ as the set of all of its prime ideals.

Example: The ring of dual numbers, $\mathbb{C}[\epsilon]/\epsilon^2$ is an important ring in which one can do calculus from an algebraic perspective: The important object in calculus is a differential, something so small that its square is 0. This is the idea behind the taylor expansion. Such an object lives in the dual numbers.

Definition: The nilradical of A, $nilrad(A)$ or $rad(A)$, is the set of nilpotent elements of A.

Theorem:

$$rad(A) = \bigcap_i P_i$$

where P_i is a prime ideal of A.

CHAPTER 4

IV. Spectrum of a Ring

Lecture 4, Aug 22.

We will prove the theorem from last class:
Theorem:

$$rad(A) = \bigcap_i P_i$$

Proof: We will do double containment: $\subset$:

$$p \in rad(A) \Rightarrow p^k = 0$$
$$0 \in P_i \forall i \Rightarrow 0 \in \bigcap_i P_i$$
$$\Rightarrow p^k \in \bigcap_i P_i$$
$$\Rightarrow p^k \in P_i \; \forall \; i$$
$$\Rightarrow p \in P_i \; \forall \; i$$
$$\Rightarrow p \in \bigcap_i P_i$$
$$\Rightarrow rad(A) \subset \bigcap_i P_i$$

$\supset$: We will show the contrapositive: If $a \notin rad(A)$, then $a \notin \bigcap_i P_i$. If $a \notin rad(A)$, then $a^n \neq 0$ for any n. We need to find a prime ideal P which does not contain a. We will again need Zorn's lemma, since we have to create an ideal. Consider

$$\Sigma := \text{ set of ideals that do not contain } a^n \text{ for all } n$$

paritally ordered by inclusion. There exists a maximal element I by Zorn's lemma. Claim I is prime: If $x, y \notin I$, then $I + (x), I + (y) \in \Sigma \Rightarrow \exists n, m$ such that $a^n \in I + (x), a^m \in I + (y) \Rightarrow a^{nm} \in I + (xy) \Rightarrow xy \notin I$. Thus I is prime, and a^n is not in I for any n.

□

Definition: Denote the spectrum of a ring A, $Spec(A)$, as the set of all prime ideals of A. Similarly the max spectrum, $mSpec(A)$ as the set of all maximal ideals. Clearly $mSpec(A) \subset Spec(A)$.

Example: $Spec(\mathbb{Z})$ is the set of prime ideals of $\mathbb{Z}$, which are all ideals of the form (p) for p a prime.

Proposition: *In a PID, all prime ideals different from* (0) *are maximal.*

Proof: Let A be a PID, (a) a prime ideal, and suppose $(a) \subset (b) \subset A$. Then $a = rb$ for some $b \in R \Rightarrow rb \in (a) \Rightarrow r \in (a)$ or $b \in (a)$. If $b \in (a)$, we are done. If $r \in (a)$, then $r = ax$ for some x. then $r = rbx \Rightarrow bx = 1 \Rightarrow b$ is a unit. We can cancel because we are in an ID.

□

Thus if $(f) \subset A$ is prime, for A a PID, then f must be an irreducible element, (non-unit).

Example: $Spec(\mathbb{C}[x]) = \mathbb{C}$. $\mathbb{C}[x]$ is a PID, so all primes look like (0) and (f) for f irreducible. But an irreducible complex polynomial must be degree one, by FTA. So all the primes are of the form $(x - b)$, for $b \in \mathbb{C}$, which contains all the polynomials which vanish at b.

Example: $Spec(\mathbb{R}[x])$. Primes still have the form (0) and (f), but now irreducible polynomials could be nonlinear, since $\mathbb{R}$ is not algebraically closed. We know f must have one complex root, c. If c is real, then $f \in (x - c)$. If c is not real, then $(x - c) \mid f$, and because complex roots of real polynomials come in pairs, $(x - \bar{c}) \mid f$. Thus

$$(x - c)(x - \bar{c}) \mid f$$
$$x^2 - (c + \bar{c})x + c\bar{c} \mid f$$

The above is a real polynoial, and f irreducible implies $f = x^2 - (c + \bar{c})x + c\bar{c}$. So $Spec(\mathbb{R}[x])$ contains two types of prime ideals $(x - c)$ and $(ax^s + bx + c)$, where $D \equiv b^2 - 4ac < 0$.

Theorem (Nullstellensatz):

$$mSpec\big(\mathbb{C}[x_1, \dots, x_n]\big) = \mathbb{C}^n$$

$$(x_1 - a_1, \dots, x_n - a_n) \mapsfrom (a_1, \dots, a_n)$$

Note that the inclusion $\supset$ is obvious. The work of the theorem is to prove all such maximal ideals have this form.

We would like to make $Spec(A)$ into a topological space[1] By Demorgan's law, it suffices

[1] This is laying the groundwork to define a scheme, although I don't believe we will be getting to this topic in this course.

to define a topology of closed subsets, and ensure that finite unions are closed, arbitrary intersections are closed, and the empty set and full space are closed. Define a subset of $Spec(A)$ to be closed if it can be written as $V(S) = \{P \mid P \supset S\}$, for S some ideal of A.

Exercise: Check that this does indeed define a topology.

Note the open sets of $Spec(A)$ are of the form $Spec(A) - V(I) = \{P \mid P \supsetneq I\} = \bigcup_{f \in I}\{P \,|f \notin P\}$. The sets being union'd over are referred to as the basic open sets.

Example: In $Spec(\mathbb{Z})$, closed sets have the form $V(m)$, for $m \in \mathbb{Z}$. Note that $P = (p) \supset (m) \rightarrow m \in (p) \Rightarrow p \mid m$. So for example $V(30) = \{(2), (3), (5)\}$ and $V(21) = \{(3), (7)\}$.

CHAPTER 5

V. Modules and Nakayama Lemma

Lecture 5, Aug 24.

Given an A-module M, there is a map $A \to End(M)$ given by $a \mapsto (m \mapsto am)$. One defn of M as an A-module is equivalent to saying that this map is a ring homomorphism for every a, where the ring structure on the right hand side is given by pointwise addition and composition.

Example: If $I \subset A$ is an ideal, then I and A/I are A-modules.

Remark: There is a category A-mod whose objects are A-modules and whose morphisms are module morphisms:

Definition: Given two A-modules M, N, an A-module homomorphism $M \to N$ is a group homomorphism such that $\varphi(am) = a\varphi(m)$. Note $Hom_{A-Mod}(A, B)$ is an abelian group.

Remark: The composition of A-module homomorphisms is an A-module homomorphism.

Definition: $N \subset M$, for M an A-module, is a <u>submodule</u> of M if N is a subgroup of M and closed under the action by A.

Lemma: *If $\varphi : M \to N$ is an A-module homomrphism, then $Im\varphi$ and $Ker\varphi$ are submodules of the appropriate A-module.*

□

Definition: If $N \subset M$ is a submodule, M/N is naturally an A-module, and a submodule of M. A priori it is an abelian group, and we equip it with the multiplication:

$$[a][b] = [ab]$$

Example: Every abelian group is a $\mathbb{Z}$-module.

Lemma: *If $\varphi : M \to N$ is an A-module homomorphism,*

$$M/Ker\varphi \cong Im\varphi$$

Proof: This statement already holds as abelian groups, and it is routine to check that the isomorphism used is also a ring isomorphism.

□

Theorem (Isomorphism Theorems): *Let $L \subset M \subset N$ be submodules. Then*

$$i) \qquad \frac{\left(\frac{N}{L}\right)}{\left(\frac{M}{L}\right)} \cong \frac{N}{M}$$

ii) $M + L \subset N$ is a submodule, and

$$(M + L)/L \cong M/M \cap L$$

Proof: The key here is to consider the right homomorphism, calculate the kernel, and apply the above lemma.
$i)$: Consider the homomorphism $N \to N/L \to (N/L)/(M/L)$.
$ii)$: Consider the homomorphism $M \to M + L \to M + L/L$.

□

Remark: If M_λ is a collection of A-modules, for $\lambda \in \Lambda$, then

$$\bigoplus_\lambda M_\lambda, \qquad \prod_\lambda M_\lambda$$

are also A-modules, with M_λ as a submodule for each λ. When Λ is finite, the two are isomorphic to each other: Each can be thought of as $|\Lambda|$-tuples of elements, with the λ component containing an element of M_λ. However the direct sum by definition requires cofinitely[1] many terms to be 0, while the direct product does not. For example, if M_λ is some fixed A-module M, and $\Lambda = \mathbb{Z}$, then for any $m \in M$, $(m, m, \dots)$ is in the direct product, but not the direct sum. In fact, the direct sum is a proper submodule of the direct product. This definition of direct sum and product of A-modules generalizes the definition of a direct sum of vector spaces and abelian groups by taking A to be a field or $A = \mathbb{Z}$, respectively.

Definition: For $m_\alpha \in M$, the set $\{m_\alpha\}$ generates M as an A-module if every $m \in M$ can be written as a finite sum $m = \sum_\alpha a_\alpha m_\alpha$, where $a_\alpha \in A$.

Remark: $\underbrace{A \oplus \cdots \oplus A}_{n \text{ times}}$ is generated by the set $\{e_\alpha\}$, where e_α is the element of the direct sum with a 1 in position α and 0 else.

[1] All but finitely many

Definition: An A-module M is finitely generated if it admits a finite set of generators.

Remark: By the above remark, $\underbrace{A \oplus \cdots \oplus A}_{n \text{ times}}$ is finitely generated for all n. We sometimes also denote this module as $A^{\oplus n}$ for brevity.

If M is a finitely generated A-module, then let $\{m_i\}$ be a finite set of generators. Then

$$A^{\oplus\ n} \to M$$

$$(a_i) \mapsto \sum a_i m_i$$

is surjective. It need not be injective, though.

Theorem (Nakayama Lemma):*If M is a finitely generated A-module and I is an ideal of A, then $M = IM \Rightarrow \exists\ x \equiv 1 \bmod I$ such that $xM = 0$.*

Example: If $A = \mathbb{Z}$ and $M = \mathbb{Z}/n\mathbb{Z}$, then I must have the form (m) for some $m \in \mathbb{Z}$. The condition $(m)M = M$ implies that $gcd(m,n) = 1$, so there exists a, b such that $am + bn = 1 \Rightarrow bn \equiv 1 \text{ mod } m$ and $(bn)(\mathbb{Z}/n\mathbb{Z}) = 0$.

To think about what the Nakayama lemma means, observe that the condition $M = IM \Rightarrow M = IM = I(IM) = I(I(IM)) = \ldots$. If we recall that maximal ideals of polynomial rings correspond to vanishing sets of functions, then we can think of the condition above as describing some functions which vanish to all orders. The only such function which should do that is the 0 function, and that is something like what happens here[2].

The above didn't really make sense to me, so let's do a different example and follow the wiki page for Nakayama lemma:

BEGIN ASIDE:

Recall we found that the nilradical of A is the intersection over all prime ideals

Definition: For a ring A, the Jacobson radical, $J(A)$, is defined as the intersection over all maximal ideals of A:

$$J(A) := \bigcap_{\mathfrak{m} \in mSpec(A)} \mathfrak{m}$$

Note that for a local ring this is just the maximal ideal itself.

Example: $J(\mathbb{Z})$ is the intersection over all (p), where p is prime, so an element is in the intersection over all such if it is divisible by every prime. But such a number must be 0:

$$J(\mathbb{Z}) = (0)$$

[2] I'm not sure I understood/transcribed this intuition correctly. In the case of polynomials over a field, there are no non-trivial ideals I, so Nakayama lemma doesn't seem to have much to say.

Observe that this is equal to the nilradical because $\mathbb{Z}$ is a PID and thus $mSpec(\mathbb{Z}) = Spec(\mathbb{Z})$.

Proposition: *For any ring A, $J(A[x]) = nilrad(A[x])$.*

Proof: The inclusion $J(A[x]) \subset nilrad(A[x])$ is immediate and holds for any ring. Let $f \in nilrad(A[x])$, so that $f^k = 0$. Then if f is not in $J(A[x])$, there must exist some maximal ideal $\mathfrak{m}_0$ which does not contain f. Then $\mathfrak{m}_0 + (f) = A[x]$, so that there exist $m \in \mathfrak{m}_0$ and $r \in A[x]$ such that $m - rf = 1 \Rightarrow 1 + rf \in \mathfrak{m}_0 \Rightarrow 1 + rf$ must not be a unit. But the sum of a unit and a nilpotent is again a unit.

□

Something about the above proof must be wrong, but I can't figure out what it is. I didn't use anything about the ring $A[x]$ itself, and this result doesn't hold generally. If anyone reading this can figure it out let me know.

A corollary of Nakayama's lemma is:

Corollary: *If M is a f.g. module over A, then $J(A)M = M \Rightarrow M = 0$.*

Proof: For any x as in the statement of Nakayama, $x - 1 \in J(A)$ so x is invertible[3] so $M = 0$.

□

For N a submodule of M, M/N is also an A-module. So we can apply the above to this module, and get

Corollary: *If M is a f.g. module over A and N is a submodule, then $J(A)M + N = M \Rightarrow M = N$.*

Proof: Apply the above corollary to M/N. Then $J(A)(M/N) = J(A)\{m+N\} = \{J(A)m + N\} = J(A)M + N$, which equals M[4] iff $M/N = 0 \iff M = N$.

□

Finally we arrive at a statement useful in terms of geometry:

Corollary (Nakayama in terms of generators): *If M is a f.g. module over A and the images of the elements $m_1, \ldots, m_n$ of M in $M/J(A)M$ generate $M/J(A)M$ as an R-module, then $m_1, \ldots, m_n$ also generate M as an A-module.*

Proof: Consider the submodule of M generated by the m_i's, call this N. The condition $J(A)M + N = M$ is exactly equivalent to $[m_i]$ generating $M/J(A)M$. Then M is equal to the module generated by the m_i's.

[3] This is the converse of the statement that if x is nilpotent then $1 - x$ is a unit, which comes from the truncated Taylor series argument.

[4] Are we subtracting an N from the RHS?

□

Now we can actually apply this to say something about geometry: Given a module M over a local ring R, $M/\mathfrak{m}M$ is a vector space over $R/\mathfrak{m}$. Thus by Nakayama, any basis of $M/\mathfrak{m}M$ lift to a minimal set of generators of M. This is helpful because geometry is concerned with local rings: If $\mathcal{M}$ is a coherent sheaf of $\mathcal{O}_X$-modules over a scheme X, then the stalk at a point $p \in X$, $\mathcal{M}_p$, is a module over the local ring $(\mathcal{O}_{X,p}, \mathfrak{m})$.

Definition: The <u>residue field</u> of a local ring $(R, \mathfrak{m})$ is the field $R/\mathfrak{m}$.

Given a scheme X, we know that around any point x, there is a neighborhood $U \ni x$ such that $U = Spec(A)$ for A some ring, equipped with the structure sheaf $\mathcal{O}_U$. Then we can consider x as a prime ideal of A, and the stalk at x is the localization $A_{(x)} \equiv \mathcal{O}_{U,x}$.

Proposition: *For any ring A, the localization at a prime, $A_\mathfrak{p}$ is a local ring with unique maximal ideal $\mathfrak{p}A_\mathfrak{p}$.*

Proof:

$$A_\mathfrak{p} = \left\{ \frac{a}{b} \mid a \in A, b \notin \mathfrak{p} \right\}$$

Note that for any $\frac{a}{b} \in A_\mathfrak{p}$, $a \notin \mathfrak{p} \iff \frac{b}{a} \in A_\mathfrak{p} \iff \frac{a}{b}$ is invertible. $a \notin \mathfrak{p} \iff \frac{a}{b} \notin \mathfrak{p}A_\mathfrak{p}$. So a fraction in $A_\mathfrak{p}$ is a unit iff it is not contained in $\mathfrak{p}A_\mathfrak{p}$, characterizing $\mathfrak{p}A_\mathfrak{p}$ as the set of non-units in $A_\mathfrak{p}$. Thus $\mathfrak{p}A_\mathfrak{p}$ is the unique maximal ideal: Maximality is clear, and uniqueness comes because any other maximal ideal must consist only of non-units. But then it must be contained in $\mathfrak{p}A_\mathfrak{p}$, and thus must be equal to it.

□

Definition: For x a point of a scheme X, the <u>residue field of x</u>, $k(x)$, is the residue field of $A_{(x)} \equiv \mathcal{O}_{X,x}$.

Example: Letting $X = Spec(k[t])$, for k algebraically closed, say we want to compute the residue field over some point $x \in X$. We know what all the non-zero prime ideals look like: $(t-a)$, for some $a \in k$. Then the residue field is

$$k[t]_{(t-a)}/(t-a)k[t]_{(t-a)}$$

To see what field this is, define the map

$$ev_a : k[t]_{(t-a)} \to k$$

$$\frac{p(t)}{q(t)} \mapsto \frac{p(a)}{q(a)}$$

Notice this is a ring homomorphism and is well defined because the denominator cannot vanish. The kernel of this map is $(t-a)k[t]_{(t-a)}$, so

$$k(x) = k\Big((t-a)\Big) \equiv k[t]_{(t-a)}/(t-a)k[t]_{(t-a)} \cong k$$

Note for a non-affine scheme, to define the residue field we had to choose a particular affine neighborhood, but this definition is independent of that choice. It is easy to check that $k\big((0)\big) = k(t)$.

Definition: For a coherent sheaf, $\mathcal{F}$, on a scheme X, the (geometric?) fiber over a point $x \in X$ is defined as

$$\mathcal{F}(p) := \mathcal{F}_x \otimes_{\mathcal{O}_{X,x}} k(x)$$

This makes sense because a coherent sheaf on a scheme is defined to be a sheaf of $\mathcal{O}_X$ modules, among other conditions, so the stalks are $\mathcal{O}_{X,x}$ modules, and $k(x)$ is a quotient of $\mathcal{O}_{X,x}$. So this is a tensor product of rings.

Back in the affine scheme setting, we can rewrite $k(x) = \mathcal{O}_{X,x}/(x)\mathcal{O}_{X,x}$, so we are looking at something of the form $R/I \otimes M$, for M an R-module. To see what this is, recall that the tensor product of modules is right-exact, and examine the exact sequence

$$0 \to I \to R \to R/I$$

which implies

$$I \otimes M \to R \otimes M = M \to R/I \otimes M \to 0$$

is exact, $\Rightarrow$ $R/I \otimes M \cong M/IM$, since the image of $I \otimes M \to M$ is IM. Thus the fiber over p is given by $\mathcal{F}_x/\mathfrak{m}_x\mathcal{F}_x$. Let's return to our original Nakayama setup, copied here for convenience:[5]

If $\mathcal{M}$ is a coherent sheaf of $\mathcal{O}_X$-modules over a scheme X, then the stalk at a point $p \in X$, $\mathcal{M}_p$, is a module over the local ring $(\mathcal{O}_{X,p}, \mathfrak{m}_p)$. We now understand that the fiber over p is given by $\mathcal{M}_p/\mathfrak{m}_p\mathcal{M}_p$, and Nakayama's lemma (the final corollary in terms of generators) says that any basis of $\mathcal{M}_p/\mathfrak{m}_p\mathcal{M}_p$ lifts to a minimal set of generators of $\mathcal{M}_p$.

In terms of geometry, if $\mathcal{M}$ is a locally free sheaf of $\mathcal{O}_X$ modules[6], we may view it as being associated to some vector bundle[7]. The fiber of $\mathcal{M}$, we now know is the vector space $\mathcal{M}_p/\mathfrak{m}_p\mathcal{M}_p$. Nakayama's lemma says that any basis of this vector space lifts to a set of minimal generators of $\mathcal{M}_p$, which in this case is interpreted as germs of sections of the vector bundle associated to $\mathcal{M}$ around the point p. So in this way, any basis of the fiber of a coherent sheaf comes from a basis of local sections of its associated vector bundle.

[5] This aside took place over like an entire week, so even I am losing track of what's happening.

[6] For all $x \in X$, there exists an open set $U \ni x$ such that $\mathcal{M}|_U \cong \bigoplus_I \mathcal{O}_X|_U$, as an $\mathcal{O}_X|_U$ module, i.e. $\mathcal{M}(U)$ is an $\mathcal{O}_X(U)$ module, and the condition is it must be a free module. Note this implies $\mathcal{M}$ is quasi-coherent. Also note that $\mathcal{O}_X$ is trivially free.

[7] This is in fact an equivalence, but it is not easy to see. One direction is clear, unfortunately the direction we do not need: Given a vector bundle, define the sheaf of local sections. This is locally free, since the sections over U are functions $U \to U \times \mathbb{R}^n$, which is identified with a direct sum of n copies of functions on U. The sheaf is free if the vector bundle is globally trivial. But the other direction, how to see every locally free sheaf as the sections of a vector bundle, is not trivial.

One thing to note: In general, for a ringed space, locally free of finite rank does not imply coherent. It holds iff the structure sheaf itself is coherent. In particular, for any scheme this holds, hence the above exchange of locally free with coherent[8]

END ASIDE:

[8] I believe they left out the finite rank assumption.

CHAPTER 6

VI. The Topology on Spec(A)

Lecture 6, Aug 24.

Definition: If I is an ideal of A,

$$rad(I) = \{a \in A \mid A^n \in I \text{ for some } n\}$$

this is also sometimes denoted as $\sqrt{I}$.

Observe that $nilrad(A) = rad((0))$. Then in general

$$\begin{aligned} \sqrt{I} &= \{a \in A \mid \bar{a}^n = 0 \in A/I\} \\ &= f^{-1}(nilrad(A/I)), \qquad f : A \to A/I \\ &= f^{-1}\left(\bigcap_{\bar{P} \in Spec(A/I)} \bar{P}\right) \\ &= \bigcap_{\bar{P} \in Spec(A/I)} f^{-1}(\bar{P}) \\ &= \bigcap_{P \in Spec(A)} P, \qquad I \subset P \end{aligned}$$

where we have applied the correspondence of prime ideals under $A \to A/I$ in the final equality.

Definition: For $f \in A$, define the basic open sets

$$X_f := \{P \in Spec(A) | \, f \notin P\}$$

Note $X_f \cap X_g = \{P \mid f \notin P, g \notin P\} \Rightarrow \{P \mid fg \notin P\} \equiv X_{fg}$.

Definition: A topological space X is quasi-compact if any open cover of X admits a finite subcover. Note that from basic topology, it suffices to check that the basis admits a finite subcover.

Proposition: *Every affine scheme is quasi-compact.*

Proof: Suppose $X = Spec(A)$ has an open cover by the basic open sets:

$$X = \bigcup_{q \in I} X_{f_q} = \bigcup_{q \in I} \{P \mid f_q \notin P\}$$

If P is a prime in A, then it belongs to this union, and thus does not contain some f_q. So each P misses some f_q. If the ideal generated by all the f_q's does not equal A, then it is contained in some maximal ideal $\mathfrak{m}$. But

$$\begin{aligned} (f_q)_{q \in I} &\subset \mathfrak{m} \\ \Rightarrow (f_q) &\subset \mathfrak{m} \qquad \forall\, q \\ \Rightarrow \mathfrak{m} &\notin \bigcup_{q \in I} X_{f_q} \end{aligned}$$

The last implication holds because elements of $\bigcup_{q \in I} X_{f_q}$ must miss at least one of the f_q's. Of course the last line is a contradiction because $\mathfrak{m} \in X$.

□

Example: The inclusion $\mathbb{R}[x] \to \mathbb{C}[x]$ induces a map $Spec(\mathbb{C}[x]) \to Spec(\mathbb{R}[x])$ by taking the preimage. We've shown before that taking the preimage of a prime ideal is prime. So in general, a map $f : A \to B$ induces a map $f^* : Spec(B) \to Spec(A)$. Under the above example,

$$\mathfrak{m}_a \in Spec(\mathbb{C}[x]) = mSpec(\mathbb{C}[x]) \mapsto \{f \in \mathbb{R}[x] \mid f(a) = 0\}$$

CHAPTER 7

VII. Homological Algebra

Lecture 7, Aug 29.

Corollary of Nakayama's Lemma: If $(A, \mathfrak{m})$ is a local ring then $\mathfrak{m}M = 0 \Rightarrow M = 0$.

This is because if $x \notin \mathfrak{m}$, then it must be a unit, since it is not contained in *any* maximal ideal.

Proposition (Characterization of local rings): Let I be an ideal of A. Then I is the unique maximal ideal of A iff the complement of I is exactly given by the set of units in A (iff the set of non-units is given by I).

Proof: $\Rightarrow$: trivial.
$\Leftarrow$: Clearly if all elements outside of I are units then I must be maximal. However, why should it be the unique maximal ideal? If there is some other maximal ideal, it must consist only of non-units, otherwise it is not proper. Therefore it is contained in I. By maximality it is equal to I.

□

Example: Let $k[[x]]$ be the ring of formal power series. To show it is local, guess a unique maximal ideal of the form $(x) = \{a_0 = 0\}$. Suffices to show any $f(x) \notin (x)$ is invertible. WLOG let $a_0 = 1$. Then the inverse is given by

$$f^{-1} = (1 - xg(x))^{-1} = 1 + xg(x) + x^2g^2(x) + \cdots \in k[[x]]$$

where

$$g(x) = a_1 + a_2x + a_3x^2 + \ldots$$

There is something subtle going on here though. Note that the element

$$1 + (1 + x) + (1 + x)^2 + (1 + x)^3 + \ldots$$

is *not* an element of $k[[x]]$, since, for example, the constant term is infinite. The problem is in each degree, the coefficient is adding up infinitely many positive terms. Elements of the formal power series ring are allowed to have infinite degree, but the coefficients still need to all be elements of k. However our choice of f^{-1} has only finitely many contributions in each degree, so each coefficient is finite. For example, the constant term is determined by the first term in the sum, which is 1: all subsequent terms in the sum have degree at least 1. The linear term is determined by the first two terms in the sum: all subsequent terms have degree at least 2, and so on. Thus $k[[x]]$ is a local ring with unique maximal ideal (x).

We are now going to get into some homological algebra. Many of these proofs are quite involved diagram chases. I'm not going to include these proofs as I don't think there is much value to gain from watching or reading someone else doing a diagram chase. This is one of those things you really have to do yourself, and they are often very awkward or unnecessarily long winded to write down.

Definition: Suppose you have a sequence of A-modules, M_i and A-module homomorphisms $f_i : M_{i-1} \to M_i$. This sequence, presented as

$$\dots \to M_{i-1} \to M_i \to M_{i+1} \to \dots$$

is called a complex if $f^2 = 0$, where square means subsequent compositions. Note this implies $ker(f_{i+1}) \subset im(f_i)$.

Definition: The sequence above is exact at M_i if $ker(f_{i+1}) = im(f_i)$. The sequence is exact if it is exact at every M_i.

Example:
i)

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

is exact at M' iff $M' \to M$ is injective.

ii)

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

is exact at M iff $M' \to M$ is surjective.

iii)

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

is exact if $M' \cong M$. To see this, combine i) and ii) to show that $M' \to M$ is an isomorphism. It's not an immediate application, since you don't have an exact sequence of the form i) or ii), so you can't just say this holds by i) and ii). But you apply the exact same arguments.

iv)

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

is exact iff $M' \to M$ is injective, $M \to M''$ is surjective and $M'' \cong M/M'$.

Definition: An exact sequence which has only 5 terms, the first and last being 0, is called a short exact sequence (SES).

Example:

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

is exact. An SES of this type[1] is referred to as a split exact sequence. There is a section (right inverse) $M'' \to M' \oplus M''$. In general, this is equivalent to being split.

Example:

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

is exact, where the map $\mathbb{Z} \to \mathbb{Z}$ is given by multiplication by 2. But it is not split: If it was, then $\mathbb{Z} \cong \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, which is obviously not possible because the right hand side has torsion while the left hand side does not.

Example: If $A = k$, then any sequence of A-modules (vector spaces) splits. This is just the rank-nullity theorem from linear algebra.

Lemma: *If*

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

is an exact sequence, then

$$0 \to Hom_A(M, N') \to Hom_A(M, N) \to Hom_A(M, N'')$$

is exact. In such a case, we say the functor $Hom_A(M, -)$ is left exact.

Proof: Exercise (diagram chase). If you need the proof and can't get it, look it up or email me.

From a similar argument, $Hom_A(-, M)$ is right exact.

Example: But $Hom_A(M, -)$ may not be exact. Take the sequence

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

Then apply $Hom_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, -)$:

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

which is not exact, since the kernel of the third map is 0, while the image of the 4th map is $\mathbb{Z}/2\mathbb{Z}$.

Note that in general, if we have an additive functor $F : A \to B$ between abelian categories,

[1] I believe "of this type" is supposed to mean isomorphic as a chain complex, which is given by the obvious commutative diagram condition.

there is a canonically induced functor from chain complexes in A to chain complexes in B by applying F to each object and morphism:

$$Ch(F) : Ch(A) \to Ch(B)$$

The only thing to check is that this sequence of objects and morphisms satisfies $d^2 = 0$, which follows from F being an additive functor.

So given an exact sequence, applying any additive functor will return a chain complex, but it does not necessarily preserve exactness.

Definition: In the category R-mod, for a morphism $g : M \to N$, define $coker\ g := N/im\ g$. For example, if g is surjective, $coker\ g = 0$.

Lemma (Snake): *Given a commutative diagram*

$$\begin{tikzcd}
0 \arrow[r] \arrow[d] & M' \arrow[r] \arrow[d, "f"] & M \arrow[r] \arrow[d, "g"] & M'' \arrow[r] \arrow[d, "h"] & 0 \arrow[d] \\
0 \arrow[r] & N' \arrow[r] & N \arrow[r] & N'' \arrow[r] & 0
\end{tikzcd}$$

with exact rows, there is an exact sequence

$$\begin{tikzcd}
0 \arrow[r] & ker\ f \arrow[r] & ker\ g \arrow[r] & ker\ h \arrow[dll] & \\
 & coker\ f & coker\ g \arrow[r] & coker\ h \arrow[r] & 0
\end{tikzcd}$$

CHAPTER 8

VIII. Tensor product on A-Mod

Lecture 8, Aug 31.

Definition: If M, N, P are A-modules, a bilinear map $M \times N \to P$ is a map which is linear in both components.

Example: $M \times A \to M$ with $(m, a) \mapsto am$ is bilinear.

Theorem[1] **(Tensor product):** *For $M, N \in A - Mod$, there exists a pair (T, g) with $T \in A - Mod$ and $g : M \times N \to T$ bilinear which satisfies the universal property: If (T', g') is another pair satisfying the above conditions, then there is a unique A-linear map $T \to T'$ such that*

$$\begin{tikzcd} M \times N \arrow[rr, "g"] \arrow[dr, "g'"'] & & T \arrow[dl, dashed, "\exists!"] \\ & T' & \end{tikzcd}$$

commutes.

Remark: As always, an object characterized by a universal property is unique up to unique isomorphism.

Proof: We will construct such a pair (T, g). Define

$$T := Fr_{A-Mod}((m,n)) \Big/ \{\text{tensor product relations}\}$$

So we consider the cartesian product $M \times N$ and the free A-module generated by all such. Then we quotient by the ideal generated by the tensor product relations, which is

[1] In this course, we bypassed all the involvement of the A-balanced maps rather than A-bilinear, which is something I still have never read about. Is it necessary to consider to construct the tensor product of modules? Maybe the need is eliminated when A is commutative, as in our case? I have no idea what that whole story is about.

the ideal generated by elements of the form

$$\begin{gathered}(m_1 + m_2, n) - (m_1, n) - (m_2, n) \\ (m, n_1 + n_2) - (m, n_1) - (m, n_2) \\ (rm, n) - r(m, n) \\ (m, rn) - r(m, n)\end{gathered}$$

which can be thought of as the appropriate things to quotient in order to make the tensor product in the quotient bilinear. The image of (m, n) through this quotient map is denoted as $m \otimes n$. Then we define the map

$$g : M \times N \to T$$

by first defining a map $g : M \times N \to Fr_{A-Mod}((m, n))$. Send

$$(m, n) \mapsto 1 \cdot (m, n)$$

the trivial sum. Then the induced map $(m, n) \mapsto 1 \cdot [m, n] \equiv m \otimes n$ is bilinear: respecting the quotient is the same as killing the tensor relations, which is the same as g being bilinear. This shows why this construction is the "right one": We kill exactly the relations necessary to force g to be bilinear, and no more, making T the "most general target for a bilinear map". So (T, g) is a pair. Now we need to show that it satisfies the universal property. If (T', g') is another such pair, define a map

$$T \to T'$$

by sending $m \otimes n \mapsto g'(m, n)$. That this map is well defined wrt the quotient on T is exactly equivalent to the bilinearity of g'. Clearly this uniquely defines the map as well, since any other such map would agree on the generators of T.

□

Example: i) $M \otimes_A A \cong M$
ii) $(M \oplus N) \otimes P \cong (M \otimes P) \oplus (N \otimes P)$ These isomorphisms are shown using the universal property.

CHAPTER 9

VIII.

Lecture 8, Sept 2.