# Math 771: Commutative Algebra

Jeffrey Ayers

Fall 2020

**About This Course**

This course was taken in the Fall of 2020 at UNC Chapel Hill taught by Professor Justin Sawon. We used Atiyah and Macdonald's text on Commutative Algebra. These notes were copied from the ones in my notebook, but heavily modified, and any mistakes are mine and not the lecturers.

# 1 Rings and Modules

## 1.1 Rings

Throughout this course, as the name would suggest, a "ring" means commutative with 1. For ring homomorphisms $f : A \to B$, we want $f(1_A) = 1_B$.

Recall we have the notion of an ideal, which is a special kind of subgroup of the additive group of the ring that absorbs elements: for each $r \in R$, $x \in I$ the product $rx \in I$. We have a proposition which we omit the proof of.

**Proposition.** Every proper ideal is contained in a maximal ideal

**Corollary.** Every nonunit of a ring $A$ is contained in a maximal ideal

We now get to the first major definition of this course:

**Definition.** A ring with exactly one maximal ideal $\mathfrak{m}$ is called a local ring, and $A/\mathfrak{m}$ us called the residue field of $A$.

**Example.** A field is a local ring with maximal ideal 0

**Proposition.**
1. Let $A$ be a local ring, then every element of $A - \mathfrak{m}$ is a unit
2. Coversely, if $A$ is a ring with an ideal $\mathfrak{m} \neq A$ such that every element of $A - \mathfrak{m}$ is a unit, then $A$ is a local ring with maximal ideal $\mathfrak{m}$
3. If $A$ is a ring with maximal ideal $\mathfrak{m}$, such that every element $1 + x$ for $x \in \mathfrak{m}$ is a unit, then $A$ is a local ring.

*Proof.*
1. Let $y \in A - \mathfrak{m}$ and consider $(y) \subset A$. As $y \notin \mathfrak{m}$, $(y) \notin \mathfrak{m}$ and as such we must have $(y) = A$, so $y$ is a unit.
2. If $\mathfrak{a} \subsetneq A$ is an ideal, then $\mathfrak{a}$ consists only of nonunits, thus $\mathfrak{a} \cap (A - \mathfrak{m}) = \emptyset$, which means that $\mathfrak{a} \subset \mathfrak{m}$ so $\mathfrak{m}$ is the only maximal ideal.
3. Let $x \in A - \mathfrak{m}$, because $\mathfrak{m}$ is maximal the ideal $M + (x) = A$, so there exists $y \in A, z \in \mathfrak{m}$ such that $z + xy = 1$ so $xy = 1 - z$ is a unit, hence $x$ is a unit. By part $ii$ $A$ is a local ring.

□

**Proposition.** The set $R$ of all nilpotent elements in a ring $A$ is an ideal, and $A/R$ has no nonzero nilpotent elements. We call $R$ the nilradical.

**Proposition.** The nilradical is the intersection of all the prime ideals in $A$

**Example.** $\mathbb{Z}/8\mathbb{Z}$, the nilradical, we claim, is $\{\overline{0}, \overline{2}, \overline{4}, \overline{6}\}$

We know that $\overline{1}, \overline{3}, \overline{5}, \overline{7}$ are all units, so the ideal generated by $\overline{2}$ is prime, and the only prime ideal, which is the nilradical

**Definition.** The Jacobson radical $J$ is the intersection of all maximal ideals (Fun fact: Jacobson was a mathematician at UNC!)

A somewhat obvious fact:

$$R = \bigcap \text{prime ideals} \subseteq \bigcap \text{maximal ideals} = J$$

**Proposition.** $x \in J$ if and only if $1 - xy$ is a unit for all $y \in A$, our ring.

*Proof.* We prove the contrapositive. First assume $1 - xy$ is not a unit. Then $1 - xy$ is contained in a maximal ideal $\mathfrak{m}$. If $xy \in \mathfrak{m}$, then $1 = (1 - xy) + (xy) \in \mathfrak{m}$, a contradiction. Hence $xy \notin \mathfrak{m}$. If $x \in J \subset \mathfrak{m}$ then $xy \in \mathfrak{m}$ a contradiction.
Next assume that $x \notin J$ so there is a maximal ideal $\mathfrak{m}$ with $x \notin \mathfrak{m}$. $A = (x) + \mathfrak{m}$, so $1 = xy + z$ for $z \in \mathfrak{m}$ thus $1 - xy = z \in \mathfrak{m}$ so $1 - xy$ is not a unit. □

We now look at some operations on ideals:

**Definition.** Given two ideals $\mathfrak{a}, \mathfrak{b}$ we can define

- Their sum $\mathfrak{a} + \mathfrak{b}$
- Their product $\mathfrak{ab} = \{\sum_{finite} xy : x \in \mathfrak{a}, y \in \mathfrak{b}\}$
- Intersection $\mathfrak{a} \cap \mathfrak{b}$
- Powers $\mathfrak{a}^n$

**Example.** In $\mathbb{Z}$ take the ideals $6\mathbb{Z}, 10\mathbb{Z}$, then

- $6\mathbb{Z} + 10\mathbb{Z} = 2\mathbb{Z}$ which is the gcd
- $6\mathbb{Z} \cdot 10\mathbb{Z} = 60\mathbb{Z}$
- $6\mathbb{Z} \cap 10\mathbb{Z} = 30\mathbb{Z}$ which is the lcm

In the ring $\mathbb{Z}$ we have that $(x)(y) = (x) \cap (y)$ if and only if gcd =1

**Example.** Let $\mathfrak{a} \subset \mathbb{Z}[x]$ consist of polynomials with even constant term. Then $2, x \in \mathfrak{a}$, so we then get $4, x^2 \in \mathfrak{a}^2$, hence $4 + x^2 \in \mathfrak{a}$. However $4 + x^2 \neq p(x)q(x)$ for any $p(x), q(x) \in \mathfrak{a}$

These operations on ideals satisy some expected rules: commutativity, associativity, distributive laws. Yet one needs to be careful:

$$\mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c}) \neq \mathfrak{a} \cap \mathfrak{b} + \mathfrak{a} \cap \mathfrak{c}$$

in general. This does hold in $\mathbb{Z}$, however. What we do always have is

$$\mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c}) \supseteq \mathfrak{a} \cap \mathfrak{b} + \mathfrak{a} \cap \mathfrak{c}$$

**Proposition.** $(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} \cap \mathfrak{b}) \subseteq \mathfrak{ab}$

**Definition.** $\mathfrak{a}$ and $\mathfrak{b}$ are called comaximal ideals or coprime ideals, if $\mathfrak{a} + \mathfrak{b} = A$

**Theorem** (Chinese Remainder Theorem)**.** Let $\mathfrak{a}_1, ..., \mathfrak{a}_n$ be ideals in $A$ then the map

$$\varphi : A \to A/\mathfrak{a}_1 \times \cdots A/\mathfrak{a}_n$$

$$x \mapsto (x + \mathfrak{a}_1, ..., x + \mathfrak{a}_n)$$

is a ring homomorphism with kernel $\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n$

If $\mathfrak{a}_i$ and $\mathfrak{a}_j$ are coprime for all $i, j$, then $\varphi$ is a surjective map and $\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n = \mathfrak{a}_1 \cdots \mathfrak{a}_n$. Thus we have

$$A/(\mathfrak{a}_1 \cdots \mathfrak{a}_n) \cong A/\mathfrak{a}_1 \times \cdots \times A/\mathfrak{a}_n$$

**Proposition.** Let $\mathfrak{p}_1, ..., \mathfrak{p}_n$ be prime ideals and let $\mathfrak{a}$ be an ideal contained in $\cup_{i=1}^n \mathfrak{p}_i$. Then $\mathfrak{a} \subseteq \mathfrak{p}_i$ for some $i$

**Proposition.** Let $\mathfrak{a}_1, ..., \mathfrak{a}_n$ be ideals an $\mathfrak{p}$ be a prime ideal containing the intersection of the $\mathfrak{a}_i$. Then $\mathfrak{a}_i \subseteq \mathfrak{p}$ for some $i$.

*Proof.* Suppose $\mathfrak{a}_i \not\subset \mathfrak{p}$ for all $i$. Then there is some $x_i \in \mathfrak{a}$ with $x_i \notin \mathfrak{p}$ for all $i$. Now

$$x = x_1 \cdots x_n \in \mathfrak{a}_1 \cdots \mathfrak{a}_n \subseteq \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n \subseteq \mathfrak{p}$$

But $x_1, ..., x_n \notin \mathfrak{p}$ so their product isn't either as $\mathfrak{p}$ is prime. Contradiction. □

**Definition.** If $\mathfrak{a}, \mathfrak{b}$ are ideals in $A$ their ideal quotient is

$$(\mathfrak{a} : \mathfrak{b}) = \{x \in A : x\mathfrak{b} \subseteq \mathfrak{a}\}$$

**Example.** $A = \mathbb{Z}$, $\mathfrak{a} = (60), \mathfrak{b} = (126)$ then

$$(\mathfrak{a} : \mathfrak{b}) = \{x \in \mathbb{Z} : 126x \in (60) \implies 2 \cdot 5 = 10 | x\}$$

So the ideal quotient is $(10) = (60/\gcd(60, 126))$

**Proposition.**

- $\mathfrak{a} \subseteq (\mathfrak{a} : \mathfrak{b})$
- $(\mathfrak{a} : \mathfrak{b})\mathfrak{b} \subseteq \mathfrak{a}$
- $((\mathfrak{a} : \mathfrak{b}) : \mathfrak{c}) = (\mathfrak{a} : \mathfrak{b}\mathfrak{c}) = (\mathfrak{a} : \mathfrak{c}\mathfrak{b}) = ((\mathfrak{a} : \mathfrak{c}) : \mathfrak{b})$
- $(\cap_i \mathfrak{a}_i : \mathfrak{b}) = \cap_i (\mathfrak{a}_i : \mathfrak{b})$

**Definition.** The radical of an ideal $\mathfrak{a}$ is

$$r(\mathfrak{a}) = \{x \in A : x^n \in \mathfrak{a} \text{ for some } n > 0\}$$

**Proposition.**

- $r(\mathfrak{a}) \supset \mathfrak{a}$
- $r(r(\mathfrak{a})) = r(\mathfrak{a})$
- $r(\mathfrak{a}\mathfrak{b}) = r(\mathfrak{a} \cap \mathfrak{b}) = r(\mathfrak{a}) \cap r(\mathfrak{b})$
- $r(\mathfrak{a}) = A \iff \mathfrak{a} = A$
- $r(\mathfrak{a} + \mathfrak{b}) = r(r(\mathfrak{a}) + r(\mathfrak{b}))$
- if $\mathfrak{p}$ is prime, then $r(\mathfrak{p}^n) = \mathfrak{p}$

**Proposition.** Let $\mathfrak{a}, \mathfrak{b} \in A$ be ideals such that $r(\mathfrak{a}), r(\mathfrak{b})$ are coprime, then the ideals $\mathfrak{a}, \mathfrak{b}$ are coprime

*Proof.* $r(\mathfrak{a} + \mathfrak{b}) = r(r(\mathfrak{a}) + r(\mathfrak{b})) = r(A) = A$ So $\mathfrak{a} + \mathfrak{b} = A$ □

We'll now look at something called extension and contraction of a ring.

**Definition.** Let $f : A \to B$ be a ring homomorphism with $\mathfrak{b} \subset B$ an ideal. We define the contraction as $\mathfrak{b}^c = f^{-1}(\mathfrak{b})$, which is an ideal in $A$

If $\mathfrak{b}$ is prime, the contraction is also prime. If $f$ is a surjection then by the isomorphism theorems we have

$$f : A \to B \cong A/\ker(f)$$

So we have a one-to-one correspondence:

$$\{\text{ideals of } A \text{ containing } f\} \leftrightarrow \{\text{ideals of } B\}$$

$$\{\text{prime ideals of } A \text{ containing } f\} \leftrightarrow \{\text{prime ideals of } B\}$$

**Definition.** If $\mathfrak{a} \subset A$ is an ideal then

$$\mathfrak{a}^e = Bf(\mathfrak{a}) = \left\{\sum y_i f(x_i) : x_i \in \mathfrak{a}, y_i \in B\right\}$$

is called the extension

**Example.** If $f$ is injective the situation can be very complicated. Consider

$$\mathbb{Z} \hookrightarrow \mathbb{Z}[i]$$

Then for a prime $p$, we have $(p)$, what is $(p)^e$? It depends on the prime.

- $(2)^e = (1+i)(1-i) = (1+i)^2$
- If $p \equiv 3 \mod 4$ then $(p)^e$ is prime.
- If $p \equiv 1 \mod 4$ then $(p)^e$ is a product of two distinct prime ideals in the Gaussian integers.

## 1.2 Modules

We take a detour from Rings to talk about Modules.

**Definition.** An $A$-module $M$ is an abelian group with an $A$-action such that for $a \in A, x, y \in M$

- $a(x+y) = ax + ay$
- $(a+b)x = ax + bx$
- $(ab)x = a)bx$
- $1x = x$

**Example.** We have lots of examples of modules cause they're cool:

- Ideals
- If $A$ is a field $k$, then a $k$-module is a vector space
- If $A = \mathbb{Z}$ then a $\mathbb{Z}$-module is an abelian group
- $A = k[x]$, a $k$-module is a vector space $V$ over $k[x]$ and an endomorphism $T : V \to V$ which is the action of $x$.

**Definition.** $f : M \to N$ is an $A$-module homomorphism if $f(x+y) = f(x) + f(y)$, $f(ax) = af(x)$. We can make the set of module homomorphisms into an $A$-module: $\mathrm{Hom}_A(M, N)$

**Definition.** $(N : P) = \{a \in A : aP \subseteq N\} \subset A$ The annihilator module can be defined as $(0, M) = \{a \in A : aM = 0\}$

Because every element of the annihilator acts trivially on $M$ we can think of $M$ as an $A/\text{Ann}(M)$ module.

**Definition.** We can define the Cartisian and Direct products of modules:

$$\bigoplus_{i \in I} M_i = \{(x_i) : x_i \in M, x_i = 0 \text{ for all but finitely many } i\}$$

$$\prod_{i \in I} M_i = \{(x_i) : x_i \in M_i\}$$

**Definition.** A free module is $M = \bigoplus M_i$ with $M_i \cong A$, which is to say $A^n = A \oplus \cdots \oplus A$. It's a module with a basis.

$M$ is finitely generated if it has a finite set of generators

$$M = \sum Ax_i = \left\{\sum a_i x_i : a_i \in A\right\}$$

**Proposition.** $M$ is finitely generated $\iff$ $M$ is a quotient of $A^n$ for some $n > 0$

Next comes a super-duper important lemma in Commutative Algebra:

**Lemma** (Nakayama's Lemma)**.** Let $M$ be a finitely generated $A$-module, and $J$ be the Jacobson radical. Then

- If $JM = M$ then $M = 0$
- If $N \subseteq M$ is a submodule, and $M = JM + N$ then $M = N$

Remark: $2 \implies 1$ is trivial, take $N = 0$. For $1 \implies 2$ consider $M/N$ then $J(M/N) = J(M + N)/N = M/N$ which implies $M/N = 0$ so $M = 0$

*Proof.* So prove 1, we suppose $M \neq 0$, let $x_1, ..., x_n$ be a basis of $M$. Then $x_n \in M = JM$ which means that

$$x_n = a_1 x_1 + \cdots + a_n x_n$$

for $a_i \in J$ Hence

$$(1 - a_n)x_n = a_1 x_1 + \cdots a_{n-1} x_{n-1}$$

but $a_n \in J$ so $1 - ya_n$ is a unit for all $y \in A$. Hence $1 - a_n$ is a unit. Which means

$$x_n = (1 - a_n)^{-1}(a_1 x_1 + \cdots a_{n-1} x_{n-1})$$

Contradicting the minimality of the set of generators □

Here's an application: Let $A$ be a local ring with maximal ideal $\mathfrak{m}$. Then $J = \mathfrak{m}$. Let $M$ be a finitely generated $A$-module. We can think of $M/\mathfrak{m}$ as an $A/\mathfrak{m}$ module, where $A/\mathfrak{m}$ is the residue field of $A$. In other words $M/\mathfrak{m}$ is a vector space. If $x_1, ..., x_n \in M$, then $\overline{x_1}, ..., \overline{x_n}$ generate $M/\mathfrak{m}M$ then $x_1, ..., x_n$ generate $M$ as an $A$-module.

**Lemma.** $M$ finitely generated over $A$, $\mathfrak{a}$ an ideal, and $\phi$ an endomorphism such that $\phi(M) \subset \mathfrak{a}M$. Then $\phi$ satisfies

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

*Proof.* Cayley-Hamilton □

We now turn our attention to discussing an important concept, and a foundational aspect of a field called Homological Algebra: Exact Sequences

**Definition.** A sequence of $A$-modules and homomorphisms

$$\cdots \longrightarrow M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \longrightarrow \cdots$$

Is exact at $M_i$ if $\text{im}(f_i) = \ker(f_{i+1})$. The sequence is exact if it's exact everywhere.

**Example.** Consider

$$0 \xrightarrow{0} M_1 \xrightarrow{f} M_2$$

Is exact at $M_1 \iff 0 = \text{im } 0 = \ker f \iff f$ is injective

Similarly we have

$$M_2 \xrightarrow{g} M_3 \xrightarrow{0} 0$$

Is exact at $M_3 \iff \text{im } g = \ker 0 = M_3 \iff g$ is surjective

Then combining these we get that

$$0 \xrightarrow{0} M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \xrightarrow{0} 0$$

Is a short exact sequence if $f$ is injective, $g$ is surjective and $\text{im } f = \ker g$. Or equivalently: $g$ induces an isomorphism

$$M_2/M_1 \simeq M_2/\text{im } f = M_2/\ker g \simeq M_3$$

We can show that Hom preserves exactness of the sequence:

**Proposition.** We have

$$M_1 \xrightarrow{f} M_2 \xrightarrow{f} M_3 \longrightarrow 0$$

is exact if and only if for $A$-modules $N$ we have that

$$0 \longrightarrow \text{Hom}(M_1, N) \xrightarrow{\tilde{g}} \text{Hom}(M_2, N) \xrightarrow{\tilde{f}} \text{Hom}(M_3, N)$$

Is exact. Note: $\tilde{g}$ is defined by $\alpha \in \text{Hom}(M_3, N)$ then

$$\tilde{g}(\alpha): \quad M_2 \xrightarrow{g} M_3 \xrightarrow{\alpha} N$$

Similarly for $\tilde{f}$

Likewise we get that

$$0 \longrightarrow N_1 \xrightarrow{f} N_2 \xrightarrow{g} N_3$$

is exact if and only if for $A$-modules $M$ we have that

$$0 \longrightarrow \mathrm{Hom}(M, N_1) \xrightarrow{\tilde{f}} \mathrm{Hom}(M, N_2) \xrightarrow{\tilde{g}} \mathrm{Hom}(M, N_3)$$

Is exact.

**Definition.** We say that $\mathrm{Hom}(M, -)$ is a covariant left exact functor, and $\mathrm{Hom}(-, N)$ is a contravariant left exact functor.

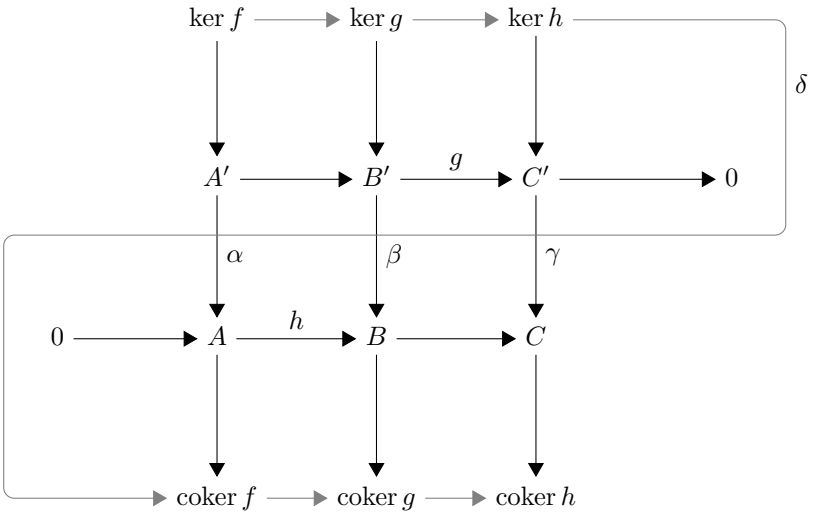
**Lemma** (Snake Lemma)**.** Suppose we have a commutative diagram with exact rows

$$\begin{array}{ccccccccc} & & A' & \xrightarrow{f} & B' & \xrightarrow{g} & C' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & A & \xrightarrow{h} & B & \xrightarrow{j} & C & & \end{array}$$

Then there exists an exact sequence

$$\ker \alpha \xrightarrow{\tilde{f}} \ker \beta \xrightarrow{\tilde{g}} \ker \gamma \xrightarrow{\delta} \operatorname{coker} \alpha \xrightarrow{\tilde{h}} \operatorname{coker} \beta \xrightarrow{\tilde{j}} \operatorname{coker} \gamma$$

Such that the following diagram commutes:




Sketch of proof: Define $\delta$ via diagram chase. Let $x \in \ker \gamma$, then $g$ surjective implies that there is a $y \in B'$ such that $g(y) = x$. Consider $\beta(y) \in B$. Then $j(\beta(y)) = \gamma(g(y)) = \gamma(x) = 0$ as $x \in \ker \gamma$. So $\beta(y) \in \ker j = \text{im}h$, so there is a $z \in A$ such that $\beta(y) = h(z)$. Define $\delta(x) = \overline{z} \in A/\text{im}\alpha = \operatorname{coker} \alpha$

TENSOR PRODUCTS OF MODULES———

# 2 Rings of Fractions

**Definition.** A mulitplicativly closed subset $S \subset A$ is such that $1 \in S$ and closed under multiplication

Define an equivalence on $A \times S$ by $(a, s)$ $(b, t)$ if and only if $(at - bs)u = 0$ for some $u \in S$