Commutative Algebra

Prof. Dr. Paul Nelson

Kevin Yeh

ETH Zürich, Autumn 2018

Contents

CURRENTLY MISSING NOTES FROM 25.09, 27.09, 26.11 (the first day after Completions, the continuation on Tor)
NEED CLARIFICATION: Example at the end of the section on Modules.
18.09.2018

1 Introduction and some Motivation

Definition 1.1. A *commutative ring (with unit)* is a set R together with two binary operations denoted $+$, and $\cdot$ (called "addition", and "multiplication"), satisfying the following axioms:

1. $(R, +)$ is an abelian group. We denote the neutral element in this group (called the additive neutral element) by 0.
2. Multiplication is associative.
3. Multiplication distributes over addition.
4. Multiplication is commutative.
5. There exists a multiplicative neutral element, denoted 1.

In this course, a ring means a commutative ring.

Example 1.2. $\mathbb{Z}$, k (which is also a field), $R[x_1, \dots, x_n]$.

Definition 1.3. An *ideal* I of a ring R is a subset of R, such that I is an additive subgroup, and $RI \subset I$.

Example 1.4. For any ring R, and $I \subset R$ an ideal, we can form the *qutient ring* R/I.

There are two main sources of motivation for the study of commutative algebra: algebraic geometry, and algebraic number theory.

1. Algebraic Geometry: The motivation comes particularly from the study of varieties.

   Definition 1.5. An *(affine) variety* or *(affine) zero-locus* (Note: most people distinguish between the two terms, with the definition given here belonging to that of a *zero-locus*, reserving the term *variety* for an irreducible zer-locus. Prof. Nelson uses both terms interchangeably to refer to a not necessarily irreducible zero-locus.) over an algebraically closed field k is the solution set to a system of polynomial equations. More precisely, given $n \geq 0$, and a subset $S \subset k[x_1, \dots, x_n]$, the *zero-locus* of S is the set

   $$Z(S) := \{a \in k^n : f(a) = 0 \quad \forall f \in S\}$$

   A set in k^n which is the zero-locus of some $S \subset k[x_1, \dots, x_n]$ is called an *algebraic set.*
   The study of varieties is closely related to the study of rings of the form

   $$k[x_1, \dots, x_n] \big/ I$$

   where I is an ideal in the polynomial ring $k[x_1, \dots, x_n]$.

2. Algebraic Number Theory: Examples include, how does a non-constant $f \in \mathbb{Z}[x]$ factor modulo a prime p? For example: $f(x) = x^2 + 1$ factors modulo an odd prime p if and only if $p \equiv 1 \pmod 4$. The study of this question is closely related to the ring

   $$\mathbb{Z}[x] \Big/ (f)$$

   and the ideal generated by p.

2 Hilbert Basis Theorem

Central Question : Can any zero-locus be defined by *finitely many* equations?

Example 2.1. Let $S = \{x^2 + y^2 - 1, y - \frac{1}{2}\} \subset k[x, y]$, where $k = \mathbb{C}$. Then we have

$$Z(S) = \left\{ (\frac{\sqrt{3}}{2}, \frac{1}{2}), (-\frac{\sqrt{3}}{2}, \frac{1}{2}) \right\}$$

Example 2.2. $S = \{x - 1, x^2 - 1, x^3 - 1, x^4 - 1, \dots\} \subset k[x]$. Then we have

$$Z(S) = Z(\{x - 1\})$$

since

$$x = 1, x^2 = 1, x^3 = 1, \cdots \iff x = 1$$

Theorem 2.3. *The answer to the Central Question is Yes: for all $S \subset k[x_1, \dots, x_n]$, there exists a finite set $\{f_1, \dots, f_n\} \subset k[x_1, \dots, x_n]$ such that*

$$Z(S) = Z(\{f_1, \dots, f_n\})$$

More precisely, given $f_1, f_2, \dots \in k[x_1, \dots, x_n]$, there exists $m \geq 1$ such that

$$Z(\{f_1, f_2, \dots\}) = Z(\{f_1, \dots, f_m\})$$

We will prove this Theorem in a bit.

Definition 2.4. Let R be a ring and $S \subset R$ a subset of R. We write (S) for the *ideal generated by S*, which is defined as such:

$$(S) := \left\{ \sum_{j=1,\dots,n} r_j s_j : r_j \in R, s_j \in S, n \in \mathbb{N} \right\}$$

That is, it is the set of all (finite) linear combinations of the elements in S.

Definition 2.5. We say that an ideal is *finitely-generated* if it can be written as the ideal generated by some finite set of elements.

Definition 2.6. We say that a ring R is *Noetherian* if every ideal in R is finitely-generated.

Remark. PID's are Noetherian.

Proposition 2.7. *Let $S \subset k[x_1, \dots, x_n]$, then $Z(S) = Z((S))$.*

Proof. Let $p \in Z(S)$. Then for all $f \in S$, by definition we have $f(p) = 0$. Therefore any linear combination of the elements in S must also vanish on p:

$$\left(\sum_{j=1}^{n} r_j f_j \right) (p) = \sum_{j=1}^{n} r_j(p) f_j(p) = 0$$

The other inclusion is trivial since $S \subset (S)$. □

Theorem 2.8 (Hilbert Basis Theorem). *If R is a Noetherian ring, so is the polynomial ring $R[x]$.*

Proof. Let $I \subset R[x]$ be an ideal. We want to show I is finitely generated. We may find elements

$$f_1 \in I \setminus \{0\}, f_2 \in I \setminus (f_1), \dots, f_{n+1} \in I \setminus (f_1, \dots, f_n), \dots$$

If I is to be finitely generated, then this process will terminate at some point, i.e. $I = (f_1, \dots, f_n)$ for some n; otherwise, it goes on forever. We may also assume moreover that for any n, we choose f_{n+1} to have minimal degree among the elements of $I \setminus (f_1, \dots, f_n)$. Let a_j be the leading coefficient of f_j. Since R is Noetherian, the ideal $J = (a_1, a_2, \dots)$ generated by all the leading coefficients is finitely generated. That means there is a finite set of a_i's that are generators of J. Let m be the first integer such that $a_1, \dots, a_m$ generate J.

Claim. $I = (f_1, \dots, f_m)$

Suppose the contrary. Then our process chooses an element f_{m+1}. Since J is finitely generated we may write $a_{m+1} = \sum_{j=1}^{m} u_j a_j$, for some $u_j \in R$. Since the degree of f_{m+1} is at least as great as the degree of any of the $f_1, \dots, f_m$, we may define a polynomial $g \in R$ having the same degree and initial term as f_{m+1} by the formula

$$g = \sum_{j=1}^{m} u_j f_j x^{\deg f_{m+1} - \deg f_j} \in (f_1, \dots, f_m)$$

The difference $f_{m+1} - g$ is in I but not in $(f_1, \dots, f_m)$, and has degree strictly less than the degree of f_{m+1}. This contradicts the choice of f_{m+1} as having minimal degree. This establishes the claim, and the Theorem. □

Corollary 2.9 (A special case of the Hilbert Basis Theorem)**.** *The polynomial rings $k[x_1, \dots, x_n]$ (where k is a field), and $\mathbb{Z}[x_1, \dots, x_n]$ are Noetherian.*

Now we are ready to prove our Central Question, Theorem 2.3

Proof. PROOF OF THEOREM 2.3: By Corollary 2.9, $k[x_1, \dots, x_n]$ is finitely generated, so the ideal (S) generated by S is finitely generated. That is, there exist $f_1, \dots f_m \in k[x_1, \dots, x_n]$ such that

$$(S) = (f_1, \dots f_m)$$

Then by Proposition 2.7 we have

$$Z(S) = Z((S)) = Z((f_1, \dots f_m)) = Z(\{f_1, \dots, f_m\})$$

as desired. □

20.09.2018

3 Hilbert's Nullstellensatz

Exercise 3.1. Let R be a ring, $S \subset R$ a subset such that (S) is finitely generated. Show that $(S) = (f_1, \dots, f_m)$ for some $f_1, \dots, f_m \in S$.

Question 3.2. *When is $Z(S_1) = Z(S_2)$?*

More precisely,

Question 3.3 (Motivating Question)**.** *For ideals $I_1, I_2 \subset k[x_1, \dots, x_n]$, when does $Z(I_1) = Z(I_2)$?*

Proposition 3.4. *$Z(k[x_1, \dots, x_n]) = Z(1) = Z((1)) = \emptyset$; $Z(0) = Z((0)) = Z(\emptyset) = k^n$.*

Proof. Trivial. □

Proposition 3.4 basically encodes the fact that nothing satisfies $1 = 0$, and everything satisfies $0 = 0$.

Question 3.5. *Given an ideal I, when does $Z(I) = \emptyset$? When does $Z(I) \neq \emptyset$?*

For $k = \mathbb{Q}$, it is an open question whether one can algorithmically compute this answer. The key being that $\mathbb{Q}$ is not algebraically closed. For our purposes we always assume k to be algebraically closed.

Example 3.6. For $n \geq 1$, define $I_n \coloneqq (x^n) \subset k[x]$. Then

$$Z(I_n) = \{a \in k : a^n = 0\} = \{0\}$$

Example 3.7. Any non-zero ideal $I \in k[x]$ has the form (f) for some $f \in R$ because $k[x]$ is a PID. Since we assume k to be algebraically closed, f splits in k, thus we can write

$$f = \prod_{j=1,\dots n} (x - a_i)^{\ell_i}$$

where $a_i \in k$ are the distinct roots of f, and $\ell_i \geq 1$. In this case the zero-locus of I is exactly the roots:

$$Z((f)) = \{a_1, \dots, a_n\}$$

Definition 3.8. For any subset $X \subset k^n$, the **vanishing ideal** of X, $I(X)$, are all the elements in $k[x_1, \dots, x_n]$ that vanish on every point of X:

$$I(X) := \{f \in k[x_1, \dots, x_n] : f(p) = 0 \quad \forall p \in X\}$$

As the name suggests, the vanishing ideal is indeed an ideal in $k[x_1, \dots, x_n]$.

Example 3.9. In dimension one, for a finite set of points $a_1, \dots, a_m \in k$, we have

$$I(\{a_1, \dots, a_m\}) = ((x - a_1) \cdots (x - a_m)) \subset k[x]$$

Moreover if a collection of points $X \subset k$ is infinite, i.e. $\mathrm{card}(X) = \infty$, then $I(X) = \{0\}$. This is because there exist no polynomial that has infinite distinct roots.

The notion of the vanishing deal is dual to the notion of a zero locus. We can now go from subsets of $k[x_1, \dots, x_n]$ to subsets of k^n via the zero-locus; and we can also go from subsets of k^n to subsets of $k[x_1, \dots, x_n]$ via the vanishing ideal:

The following are some immediate results connecting the two:

Lemma 3.10.

1. *If $X \subset X' \subset k^n$, then $I(X) \supset I(X')$.*
2. *If $S \subset S' \subset k[x_1, \dots, x_n]$, then $Z(S) \supset Z(S')$.*
3. *$X \subset Z(S)$ if and only if $S \subset I(X)$.*
4. *$I(Z(I(X))) = I(X)$.*
5. *$Z(I(Z(S))) = Z(S)$.*

Proof. 1., 2., 3. are trivial. For 4., first the inequality $X \subset Z(I(X))$ is clear by definition. Then by 1., we have $I(X) \supset I(Z(I(X)))$. Conversely, the inclusion $I(X) \subset I(Z(I(X)))$ is clear by definition. 5. □

The upshot of Lemma 3.10 is that the answer to Question 3.3 is the following:

$$Z(I_1) = Z(I_2) \iff I(Z(I_1)) = I(Z(I_2))$$

Proof. $(\Rightarrow)$ is clear. $(\Leftarrow)$ is a result of 5. of Lemma 3.10. □

In summary, our Motivating Question reduces to understanding

$$I(Z(\mathfrak{a}))$$

of an ideal $\mathfrak{a} \subset k[x_1, \dots, x_n]$.

Example 3.11. In dimension one, we can write an ideal as $\mathfrak{a} = (f)$ for some $f \in k[x]$. As mentioned before, we can write $f = \prod_i^n (x - a_i)^{\ell_i}$, and thus $Z(\mathfrak{a}) = \{a_1, \dots, a_n\}$. Using Example 3.9

$$I(Z(\mathfrak{a})) = I\left(\prod (x - a_i)\right)$$

Definition 3.12. Let R be a ring, and $I \subset R$ an ideal. The **radical** of I is defined to be

$$\operatorname{rad}(I) \coloneqq \{f \in R : f^n \in I \quad \text{for some } n \geq 0\}$$

Lemma 3.13. *The radical of an ideal is an ideal.*

Proof. □

Theorem 3.14 (Hilbert's Nullstellensatz, Full-Blown, on Steroids Form)**.** *Let k be an algebraically closed field. If $\mathfrak{a} \subset k[x_1, \ldots, x_n]$ is an ideal, then*

$$I(Z(\mathfrak{a})) = \operatorname{rad}(\mathfrak{a})$$

Thus, the correspondences $\mathfrak{a} \mapsto Z(\mathfrak{a})$ and $X \mapsto I(X)$ induce a bijection between the collection of algebraic sets of $A_k^n = k^n$ and radical ideals of $k[x_1, \ldots, x_n]$.

Remark. A_k^n is the notation for the *affine n-space (over k)*, which is just k^n.

It is easy to see that the inclusion "$\supset$" holds: If $f \in \operatorname{rad}(\mathfrak{a})$, then $f^n \in \mathfrak{a}$ for some n, thus $f^n(p) = 0$ for all $p \in Z(\mathfrak{a})$, therefore $f \in I(Z(\mathfrak{a}))$. The other inclusion is more interesting. It says that if f is a polynomial that vanishes on $Z(\mathfrak{a})$, then $f^n \in \mathfrak{a}$ for some n.

Lemma 3.15. *Let $\mathfrak{a} \subset R$ be an ideal. Then* $\operatorname{rad}(\operatorname{rad}(\mathfrak{a})) = \operatorname{rad}(\mathfrak{a})$.

Proof. □

Proposition 3.16.

Corollary 3.17.

$$Z(\mathfrak{a}) = \emptyset \iff \mathfrak{a} = (1) = R$$

Proof. If $\mathfrak{a} = (1)$, then $Z(\mathfrak{a}) = \emptyset$ since the constant polynomial 1 never vanishes. Conversely, if $Z(\mathfrak{a}) = \emptyset$, then by the Strong Form of Nullstellensatz,

$$\operatorname{rad}(\mathfrak{a}) = I(Z(\mathfrak{a})) = I(\emptyset = (1)$$

which implies $\mathfrak{a} = (1)$. □

Corollary 3.18 (Hilbert's Nullstellensatz, Strong Form)**.** *Given polynomials $g, f_1, f_2, \ldots, f_m \in k[x_1, \ldots, x_n]$, the following are equivalent:*

1. *There exist no solution $p \in k^n$ to the system*

$$f_1(p) = f_2(p) = \cdots = f_m(p), \quad g(p) \neq 0$$

2. *There exists $N \geq 0$ and $q_1, \ldots, q_m \in k[x_1, \ldots, x_n]$ such that*

$$g^N = \sum q_j f_j$$

Proof. Let $\mathfrak{a} = (g, f_1, \ldots, f_m) \subset k[x_1, \ldots, x_n]$. Suppose 1. is true, then having no solution to the system means that $Z(\mathfrak{a}) = \emptyset$. Then by Theorem 3.17, we have

$$\mathfrak{a} = (1)$$

□

Corollary 3.19 (Hilbert's Nullstellensatz, Weak Form)**.**

4 Localization

5 Prime Ideals

6 Modules

6.1 Defintion and Basic Facts

I will begin with the definition given in A-M Chapter 2., which I find to be more approachable as a first introduction, and one that allows me to immediately think of examples to put the idea on a solid footing. In class Prof. Nelson gave th second definition first and showed it is equivalent to the first one.
Let R be a ring.

Definition 6.1. A *module M (over R)* or *R-module* is an additive abelian group $(M, +)$, on which R acts linearly. More precisely, it is a pair (M, μ), where M is an abelian group and $\mu : R \times M \to M$ is a mapping such that if we denote $axcoloneqq\mu(a, x)$, then the following axioms are satisfied:

$$a(x + y) = ax + ay \tag{1}$$

$$(a + b)x = ax + bx \tag{2}$$

$$(ab)x = a(bx) \tag{3}$$

$$1x = x \tag{4}$$

where $a, b \in R$, and $x, y \in M$.

Equivalently, we can define an R-module by the following definition:

Definition 6.2. A *module M (over R)* or *R-module* is an additive abelian group $(M, +)$ together with an action of R:

$$\begin{aligned} R \times M &\to M \\ (r, m) &\mapsto rm \end{aligned}$$

that defines a ring homomorphism:

$$\begin{aligned} R &\to \mathrm{End}(f) \\ r &\mapsto [m \mapsto rm] \end{aligned}$$

where $\mathrm{End}(M)$, the ring of endomorphisms (which are homomorphisms to itself) of the abelian group M is

$$\mathrm{End}(M) \coloneqq \{f : M \to M : f \text{ a homomoprhism } \} = \mathrm{Hom}(M, M)$$

Essentially, modules are generalized vector spaces. Whereas a vector space is defined over a space of scalars that is a field, a module is defined over a space of scalars that is a more general structure of a ring. We can still multiply “vectors” by scalars, and this distributes over addition of “vectors”. Analogous to linear transformations between vector spaces, we have the notion of a *module homomorphism* between modules, that preserves the module structure.

Definition 6.3. Let M, N be R-modules. A mapping $f : M \to N$ is an *R-module homomorphism* or an *R-linear map* if

$$f(x + y) = f(x) + f(y) \tag{5}$$

$$f(ax) = af(x) \tag{6}$$

for all $a \in R$, and all $x, y \in M$. Think of linear transformations between vector spaces when R is a field.

Definition 6.4. The set of all R-module homomorphisms between M and N is denoted:

$$\mathrm{Hom}(M,N) \coloneqq \{f : M \to N : f \text{ an } R\text{-module homomorphism}\}$$

This is naturally an R-module as well:

$$(r \cdot f)(x) \coloneqq r \cdot f(x) = f(rx)$$

and

$$(f+g)(x) \coloneqq f(x) + g(x)$$

for all $f, g \in \mathrm{Hom}(M,N)$, and $r \in R$.

Proposition 6.5. *Let M be an R-module. Then $\mathrm{End}(M) = \mathrm{Hom}(M,M)$. Furthermore, if we define:*

$$(f_1 f_2)(x) \coloneqq f_1(f_2(x))$$

we make $\mathrm{End}(M)$ into a ring.

Example 6.6. There is a mon-to-one correspondence:

$$\{\text{abelian groups}\} \longleftrightarrow \{\mathbb{Z}\text{-modules}\}$$

Suppose M is an abelian group, then there is a natural action of $\mathbb{Z}$ on M:

$$\begin{aligned} \mathbb{Z} \times M &\to M \\ (n,x) &\mapsto nx \coloneqq x + \cdots + x \quad (n \text{ times}) \end{aligned}$$

From which we can define a unique ring homomorphism

$$\begin{aligned} \mathbb{Z} &\to M \\ n &\mapsto [m \mapsto nx] \end{aligned}$$

Conversely, given a $\mathbb{Z}$-module, it is by definition an abelian group.

Example 6.7. If k is a field then k-modules equivalent to k-vector spaces. Morphism of k-modules are equivalent to k-linear maps.

As we can think of modules as generalized vector spaces, there is an equivalent notion of a module having a basis. Those of which are called *free modules.*

Definition 6.8. A *free module* over a ring R is a module that is isomorphic to a module of the following form:

$$R^{(I)} \coloneqq \{\text{sequences } (x_i)_{i\in I} : \text{ each } x_i \in R, x_i = 0 \text{ for all but finitely many } i\}$$

Where I is an arbitrary indexing set. This has to be a module over R, so we define for all $r \in R$,

$$(x)_{i\in I} + (y)_{i\in I} \coloneqq (x_i + y_i)_{i\in I}$$

and

$$r(x)_{i\in I} \coloneqq (rx_i)_{i\in I}$$

Or equivalently, a *free module* is a module that is isomorphic to a module of the form:

$$R^{(I)} \cong \bigoplus_{i\in I} M_i \text{ where each } M_i \cong R \text{ as an } R\text{-module}$$

See 6.15 for the definition of the direct sum of modules.

Proposition 6.9. *Let k be a field. The every k-module is free.*

Proof. This is just saying that every vector space has a basis. □

Proposition 6.10. *Over any ring R that is not a field, there are modules that are not free. Indeed, let $I \in R$ be an ideal other than $(0), (1)$. Then the module*

$$M \coloneqq {}^{R}/_{I}$$

is an R-module which is NOT free.

Example 6.11. $R = \mathbb{Z}$, $I = (2)$, $M = \mathbb{Z}/2\mathbb{Z}$.

We will give a proof to this Remark, but before that we introduce one definition.

Definition 6.12. For any R-module M, the *annihilator* of M is the set

$$\operatorname{Ann}(M) \coloneqq \{r \in R : rm = 0, \text{ for all } m \in M\} \subset R$$

That is, it is the set of elements in R that "hit every m into 0". It is also true that $\operatorname{Ann}(M)$ is an ideal of R.

Clearly, if M_1 isomorphic to M_2 as R-modules, then they have the same annihilator.
Now we give a proof of the Proposition above.

Proof. PROOF OF PROPOSITION 6.10: First, it is clear that R/I is an R-module. (in the most natural sense). It is also clear that $\operatorname{Ann}(R/I) = I$. In general, for a given free module $R^{(J)}$, the annihilator is:

$$\operatorname{Ann}(R^{(J)}) = \begin{cases} R & J = \emptyset \\ (0) & J \neq \emptyset \end{cases} \tag{7}$$

This is because $R^{(J)}$ is a set of R-sequences indexed by J such that all but finitely many of the entries are zero. Now if $J = \emptyset$, then it is vacuously true that every $r \in R$ is in the annihilator (actually, if we index with $\emptyset$, what exactly is $R^{(J)}$?). If $J \neq \emptyset$, if $r \in \operatorname{Ann}(R^{(J)}$, then in particular $r \cdot 1 = 0$ so it must be that $r = 0$. This establishes 7. In our case, since $\operatorname{Ann}(R/I) = I \neq R$ or (0), R cannot be free. □

Example 6.13. Let k be an algebraically closed field. Let $R = k[x_1, \ldots, x_n]/I$, where $I \subset k[x_1, \ldots, x_n]$ is a *radical* ideal in the multivariate polynomial ring. Furthermore, let J be another radical ideal such that $I \subset J \subset k[x_1, \ldots, x_n]$. Then the image $\overline{J} \subset R$ of J in the quotient is a radical ideal in R.
If we let $X = V(I)$, then $Y = V(J) \subset X$. The action of R on the module $M = R/\overline{J}$ is just multiplication of functions. This is somehow a consequence of the fac that

$$R \iff \{\text{functions } X \to k\}$$

and

$$R/\overline{J} \hookrightarrow \{\text{functions} Y \to k\}$$

NEED CLARIFICATION ON THIS EXAMPLE. O.K. THIS IS ALL VERY NICE BUT WHY DO WE CARE ABOUT MODULES AT ALL
04.10.2018

6.2 Properties of Hom

The first property is that given a module M the Hom module between the underlying ring and M is isomorphic to M itself (as R-modules).

Proposition 6.14. *Let M be an R-module. Then*

$$\operatorname{Hom}(R, M) \cong M$$

as R-modules.

Proof. Consider the module homomorphism:

$$\begin{aligned}\mu\colon \operatorname{Hom}(R, M) &\to M\\ \varphi &\mapsto \varphi(1)\end{aligned}$$

μ is indeed a bijection:
Surjectivity: Given $a \in M$, we can define $\varphi_{(a)}$ uniquely by

$$\varphi_{(a)}(x) \coloneqq x \cdot a$$

Then under the mapping μ we have $\mu(\varphi_{(a)}) = \varphi_{(a)}(1) = 1 \cdot a = a$.
Injectivity: We show injectivity by showing that $\ker(\mu) = \{0\}$ (the zero mapping). If $\varphi \in \ker(\mu)$, this means that $\mu(\varphi) = \varphi(1) = 0 \in M$, then for any $r \in R$, $\varphi(r) = \varphi(1 \cdot r) = r \cdot \varphi(1) = r \cdot 0 = 0$, showing φ is the zero mapping. □

We introduce some definitions to help us discuss further properties.

Definition 6.15 (Direct Sum of Modules)**.** Let $(M_i)_{i\in A}$ be an indexed family of R-modules. Their *direct sum* is defined to be:

$$\bigoplus_{i\in A} M_i \coloneqq \{\text{formal sums } \sum_{i\in A} m_i : m_i = 0 \text{ for a.e. } i\} = \{(m_i)_{i\in A} : m_i = 0 \text{ for a.e. } i\}$$

This is naturally an R-module, if we define both addition and multiplication (by a scalar) component-wise.

Remark. I find it more useful most of the time to think of them as tuples with “finite support” (), rather than “formal sums” which is sometimes a little misleading; this also makes the connection with the direct product clear.

Definition 6.16. Let $(M_i)_{i\in A}$ be an indexed family of R-modules. Their *direct product* is defined to be:

$$\prod_{i\in A} M_i \coloneqq \{(m_i)_{i\in A} : m_i \in M_i\}$$

Again, this is naturally an R-module, if we define both addition and multiplication (by a scalar) component-wise.

Remark. Notice that $\bigoplus_i M_i \subset \prod_i M_i$

Proposition 6.17. *Let M, N be R-modules. Then for any indexing set I,*

$$\operatorname{Hom}\left(\bigoplus_{i\in I} M_i, N\right) \cong \prod_{i\in I} \operatorname{Hom}(M_i, N)$$

as R-modules. This equivalence is given by the following isomorphism:

$$\begin{aligned}\alpha\colon \operatorname{Hom}\left(\bigoplus_{i\in I} M_i, N\right) &\to \prod_{i\in I} \operatorname{Hom}(M_i, N)\\ \phi &\mapsto (\phi \circ \kappa_i)_{i\in I}\end{aligned}$$

Where

$$\kappa_i : M_i \to \bigoplus_{i\in I} M_i$$

is the obvious map:

$$m \in M_i \mapsto (0, 0, 0, \dots, m\textit{(at the i-th position)}, 0, 0, \dots)$$

Proof. The map α is a well-defined morphism of modules. Indeed if $\varphi, \gamma \in \operatorname{Hom}\left(\bigoplus_{i \in I} M_i, N\right)$, then

$$\alpha(\varphi + \gamma) = ((\varphi + \gamma) \circ \kappa_i)_{i \in I} = (\varphi \circ \kappa_i + \gamma \circ \kappa_i)_{i \in I} = (\varphi \circ \kappa_i)_{i \in I} + (\gamma \circ \kappa_i)_{i \in I} = \alpha(\varphi) + \alpha + \alpha(\gamma)$$

Also, if $r \in R$, then

$$\alpha(r\varphi) = (r\varphi \circ \kappa_i)_{i \in I} = r(\varphi \circ \kappa_i)_{i \in I} = r\alpha(\varphi)$$

Now we want to show that α is a bijection.
Injectivity: If $\alpha(\phi) = (0)_{i \in I}$, then $\phi \circ \kappa_i = 0$ (the zero mapping) for every $i \in I$. This means for every $m \in M$,

$$\phi(\kappa_i(m)) = \phi((0, 0, 0, \dots, m(\text{at the } i\text{-th position}), 0, 0, \dots)) = 0$$

But this occurs precisely when $\phi : \bigoplus_{i \in I} M_i \to N$ is the zero mapping. Therefore $\ker(\alpha) = \{0\}$.
Surjectivity: Given $(\varphi_i)_{i \in I} \in \prod_i \operatorname{Hom}(M_i, N)$, we may define

$$\varphi \in \operatorname{Hom}\left(\bigoplus_i M_i, N\right)$$

by setting

$$\varphi((m_i)_{i \in I}) \coloneqq \sum_{i \in I} \varphi_i(m_i) \in N$$

for $(m_i)_{i \in I} \in \bigoplus_i M_i$. The sum on the right is well-defined because only finitely many m_i's are nonzero, therefore only finitely many $\varphi_i(m_i) \in N$ are nonzero in N. Then

Claim.

$$\varphi \circ \kappa_i = \varphi_i$$

Indeed we know the composition is a mapping

$$(\varphi \circ \kappa_i) : M_i \to N$$

Take $m_i \in M_i$, then

$$(\varphi \circ \kappa_i)(m_i) = \varphi(\kappa_i(m_i)) = \varphi(0, 0, \dots, m_i, 0, \dots) = \varphi_i(m_i)$$

thus the desired equality. □

Lemma 6.18.

$$\operatorname{Hom}\left(M, \prod_{i \in I} N_i\right) \cong \prod_{i \in I} \operatorname{Hom}(M, N_i)$$

$$\varphi \mapsto (\pi_i \circ \varphi)_i$$

where

$$\pi_i : N \to N_i$$

is the obvious map

Proof. Similar to previous lemma. □

Definition 6.19. A *submodule* of a module is a subgroup that is closed under multiplication by R. (think of a vector subspace)

Definition 6.20. Let M be an R-module and a $M' \subset M$ a submodule. The *quotient abelian group* $M'' \coloneqq M/M'$ is naturally a module with the action described below.
For all $r \in R$

$$r \cdot (x + M') \coloneqq rx + M'$$

Definition 6.21. Let $\varphi : M \to N$ be a module morphism. Then the *kernel* of φ is

$$\ker(\varphi) \coloneqq \{m \in M : \varphi(m) = 0\} \subset M$$

which is a submodule of M.

Definition 6.22. Let $\varphi : M \to N$ be a module morphism. Then the *cokernel* of φ is

$$\operatorname{coker}(\varphi) \coloneqq N \big/ \varphi(M)$$

which is an R-module, since the image $\varphi(M)$ is a submodule of N, and by Definition 6.20, quotienting by a submodule gives us another module.

The next property is the following fact: For any R-module M,

$$\operatorname{Hom}(M, -)$$

"preserves kernels". We make this more precise in the following proposition:

Proposition 6.23 (Hom$(M, -)$ Sends Kernel to Kernel)**.** *Let $\varphi : N_1 \to N_2$ be an R-module morphism. Let M be another R-module. Consider the induced map between "Hom spaces":*

$$\begin{aligned} \varphi_* \text{ or } \operatorname{Hom}(M, \varphi)\colon \operatorname{Hom}(M, N_1) &\to \operatorname{Hom}(M, N_2) \\ f &\mapsto \varphi \circ f \end{aligned}$$

The image $\varphi \circ f$ is called the pushforward of f by φ*. Then*

$$\ker(\varphi_*) \cong \operatorname{Hom}(M, \ker(\varphi))$$

Given by the mapping

$$(\ker(\varphi) \overset{i}{\hookrightarrow} N_1) \circ f \hookleftarrow f$$

Where i is the inclusion map.

Proof. We must verify the mapping

$$\begin{aligned} \Phi\colon \operatorname{Hom}(M, \ker(\varphi)) &\to \ker(\varphi_*) \\ f &\mapsto i \circ f \end{aligned}$$

is a bijective R-module morphism. Note that i is the inclusion morphism of $\ker(\varphi)$ into N_1:

$$i : \ker(\varphi) \hookrightarrow N_1$$

First we verify that Φ is indeed a module morphism: Let $f, g \in \operatorname{Hom}(M, \ker(\varphi)))$. Then for $m \in M$,

$$\begin{aligned} \Phi(f + g)(m) &= (i \circ (f + g))(m) \\ &= i(f(m) + g(m)) \\ &= i(f(m)) + i(g(m)) \quad \text{(since } i \text{ is a module morphism)} \\ &= (i \circ f)(m) + (i \circ g)(m) \\ &= \Phi(f)(m) + \Phi(g)(m) \end{aligned}$$

On the other hand, if $r \in R$, then

$$\begin{aligned} \Phi(rf)(m) &= (i \circ rf)(m) \\ &= i(rf(m)) \\ &= ri(f(m)) \quad \text{(since } i \text{ is a module morphism)} \\ &= r\Phi(f)(m) \end{aligned}$$

Thus Φ is indeed an R-module morphism. Now we need to show that it is bijective.
Injectivity: □

The dual notion to the *pushforward* is the *pullback*:

Definition 6.24. Let $\varphi : M_1 \to M_2$ be a module homomorphism and N another module.

Proposition 6.25 (Hom$(-, N)$ Sends Cokernel to Kernel)**.** *Let $\varphi : M_1 \to M_2$ be an R-module morphism. Let N be another R-module. Consider the induced map*

$$\begin{aligned} \varphi^* \textit{ or } \operatorname{Hom}(\varphi, N)\colon \operatorname{Hom}(M_2, N) &\to \operatorname{Hom}(M_1, N) \\ f &\mapsto f \circ \varphi \end{aligned}$$

The image $f \circ \varphi$ is called the pullback of f by φ*. Then*

$$\ker(\varphi^*) \cong \operatorname{Hom}(\operatorname{coker}(\varphi^*), N)$$

One may be able to prove Proposition 6.25 directly as we did for Proposition 6.23. However, we take this opportunity to introduce the notion of *exact sequences of module morphisms*, which we will use for the proof. This approach is more elegant.

Definition 6.26. A sequence of module morphisms

$$\ldots \xrightarrow{\varphi_{i-2}} M_{i-2} \xrightarrow{\varphi_{i-1}} M_{i-1} \xrightarrow{\varphi_i} M_i \xrightarrow{\varphi_{i+1}} M_{i+1} \xrightarrow{\varphi_{i+2}} M_{i+2} \xrightarrow{\varphi_{i+3}} \ldots$$

is *exact at M_i* if

$$\operatorname{Im}(\varphi_i) = \ker(\varphi_{i+1})$$

The entire sequence is called *exact* if it is exact at every M_i.

Example 6.27. The sequence

$$0 \to M \xrightarrow{\varphi} M' \to \ldots$$

is exact at M if and only if $\ker(\varphi) = \{0\}$. Thus the sequence is exact at M if and only if φ is injective.

Example 6.28. The sequence

$$0 \to M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \to 0$$

is exact if and only if α is injective, β is surjective, and $\operatorname{Im}(\alpha) = \ker(\beta)$.

The following to Lemmas encompasses the idea that "Hom is a left-exact functor".

Lemma 6.29. *If*

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C$$

is an exact sequence of modules (such a thing is called a left-exact sequence*) and M is any module, then the sequence of maps*

$$0 \to \operatorname{Hom}(M, A) \xrightarrow{f_*} \operatorname{Hom}(M, B) \xrightarrow{g_*} \operatorname{Hom}(M, C)$$

obtained by "pushing forward" is exact.

What we mean by "pushing forward" is the following: The map

$$\operatorname{Hom}(M, A) \xrightarrow{f_*} \operatorname{Hom}(M, B)$$

sends a map $\phi : M \to A$ to the pushforward of f by ϕ:

$$\phi \circ f : M \to B$$

which is an element of $\operatorname{Hom}(M, B)$. The definition of g_* is analogous.

Proof. We first show that f_* has trivial kernel: Suppose $\phi\circ : M \to B$ is the zero map. Since f has trivial kernel by assumption, ϕ must be the zero map from M to A, as desired.
Now we show $\mathrm{Im}(f_*) = \ker(g_*)$: Since A injects into B, we can regard A as a submodule of B. Moreover, since $A = \ker(g)$, by the First Isomorphism Theorem, $B/A \hookrightarrow C$, so we can regard B/A as a submodule of C.

Now we have the following commutative diagram:

$$\begin{tikzcd}
& B \arrow[dd, "g"] \arrow[dr, two heads, "\pi"] & \\
M \arrow[ur, "\gamma"] \arrow[dr, dotted, "g_*(\gamma)"'] & & {}^{B}/_{A} \arrow[dl, hook', "\eta"] \\
& C &
\end{tikzcd}$$

So

$$g_*(\gamma) = \gamma \circ \pi \circ \eta = 0 \quad \text{(the zero map)}$$

By injectivity of η, the above equation holds if and only if the image of M under γ is contained in A (regarding A as a submodule of B). This occurs if and only if $\gamma \in \mathrm{Im}(f_*)$ because of the following diagram:

$$\begin{tikzcd}
M \arrow[r] \arrow[dr, "\gamma"'] & A \arrow[d, hook, "f"] \\
& B
\end{tikzcd}$$

□

Lemma 6.29 gives us an alternative proof to Proposition 6.23 if we let $A = \ker(\varphi)$, $B = N_1$, and $C = N_2$. Then the results follows immediately. We will prove Proposition 6.25 in a similar fashion using the following analogous Lemma:

Lemma 6.30. *If*

$$A \xrightarrow{f} B \xrightarrow{g} C \to 0$$

is an exact sequence of modules (such a thing is called a right-exact sequence*), and N is any module, then*

$$0 \to \mathrm{Hom}(C, N) \xrightarrow{g^*} \mathrm{Hom}(B, N) \xrightarrow{f^*} \mathrm{Hom}(A, N)$$

obtained by "pulling back" is exact.

Proof. We first show that g^* has trivial kernel: Let $\gamma \in \ker(g^*)$. Using exactness, in particular that $\ker(g) = f(A)$, we have the following commutative diagram:

$$\begin{tikzcd}
C \arrow[r, "\gamma"] & N \\
B \arrow[u, two heads, "g"] \arrow[ur, "g^*(\gamma)"']
\end{tikzcd}$$

Suppose by contradiction that γ is not the zero map. Thus there exists some non-zero element $y \in C$ such that $\gamma(y) \neq 0$. Then consider the element $x := g^{-1}(y) \in B$. By assumption $g^*(\gamma)(x) = 0$, but $\gamma(g(x)) = \gamma(y) \neq 0$, commutativity of the diagram gives the contradiction.
We now show that $\mathrm{Im}(g^*) = \ker(f^*)$: □

6.3 Modules via Generators and Relations

(The following is taken from [Eis] page 17., since the description given in class was a little confusing). First, a motivating example. If we say that a module has one generator g and relations $f_1 g = f_2 g = \cdots = f_n g = 0$, for some elements $f_1, \dots, f_n \in R$, then the module is $R/(f_1, \dots, f_n)$. We make this more precise:

An element m of a module M corresponds to a homomorphism from R to M, sending 1 to m. Thus, giving a set of elements $\{m_\alpha\}_{\alpha \in A} \in M$ corresponds to giving a homomoprhism φ from a direct sum $G \coloneqq R^A$ of copies of R, indexed by A, sending the α-th basis element to m_α. If the m_α generate M, then φ is a surjection.

The relations on the m_α are the same as elements of the kernel of the map $G \to M$. A set of relations $\{n_\beta\}_{\beta \in B} \in G$ corresponds to a homomorphism ψ from a free module $F \coloneqq R^B$ to the kernel of φ (as before, sending the β-th basis element of R^B to $n_\beta \in R^A$). We say that the m_α generate M and the n_β generate the kernel, i.e. M is a module with generators $\{m_\alpha\}_{\alpha \in A}$ and relations $\{n_\beta\}_{\beta \in B}$ if and only if the sequence

$$F \xrightarrow{\psi} G \xrightarrow{\varphi} M \to 0$$

is exact. This sequence is called a *free presentation of* M. Notice that, by exactness, γ is surjective, so by the First Isomorphism Theorem we have

$$\begin{tikzcd}
F \arrow[r, "\psi"] & G \arrow[r, two heads, "\varphi"] \arrow[d, "\pi"] & M \arrow[r] & 0 \\
& G \big/ R \cdot \{n_\beta\}_{\beta \in B} \arrow[ur, "\cong"'] & &
\end{tikzcd}$$

Therefore we equivalently say that

$$M \coloneqq G \Big/ R \cdot \{n_\beta\}_{\beta \in B} = R^A \Big/ R \cdot \{n_\beta\}_{\beta \in B}$$

6.4 Tensor Product of Modules

Definition 6.31. Given two modules M and N, we define the *tensor product of* M *and* N, denoted $M \otimes N$, to be the module with generators

$$\{(m, n) : m \in M, n \in N\}$$

and relations

$$(m_1 + m_2, n) - (m_1, n) - (m_2, n)$$

$$(m, n_1 + n_2) - (m, n_1) - (m, n_2)$$

$$(am, n) - a(m, n)$$

$$(m, an) - a(m, n)$$

for any $m \in M$, $n \in N$, $a \in R$.

We denote $m \otimes n \in M \otimes N$ the image of (m, n) under the obvious mapping

$$M \times N \to M \otimes N$$

Definition 6.32. Let M, N, P be modules. A *bilinear or R-bilinear map*

$$f : M \times N \to P$$

is a map where for all $a, a', b, b' \in R$; $m, m' \in M$; and $n, n' \in N$, we have

$$f(am + a'm', bn + b'n') = abf(m, n) + a'bf(m'n) + ab'f(m, n') + a'b'f(m', n')$$

Example 6.33. The map

$$\begin{aligned} M \times N &\to M \otimes N \\ (m,n) &\mapsto m \otimes n \end{aligned}$$

is bilinear.

There is a natural one-to-one correspondence between bilinear mappings $M \times N \to P$ and R-linear mappings (i.e. R-module morphisms) $M \otimes N \to P$. More precisely:

Lemma 6.34. *For all modules M, N, P, we have*

$$\mathrm{Hom}(M \otimes N, P) \cong \{\textit{bilinear } f : M \times N \to P\}$$

via the identifications:
For $f \in \{\textit{bilinear } f : M \times N \to P\}$,

$$f \mapsto [m \otimes n \mapsto f(m,n)]$$

And for $\varphi \in \mathrm{Hom}(M \otimes N, P)$,

$$\varphi \mapsto \varphi \circ g$$

where g is the obvious bilinear map

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

Another way to say this is the follwing: Given any module P and any R-bilinear mapping $f : M \times N \to P$, there exists a unique A-linear mapping $f' : M \otimes N \to P$ such that $f = f' \circ g$ (in other words, every bilinear function on $M \times N$ factors through $M \otimes N$).

Moreover, if T' is some other module, and $g' : M \times N \to T'$ is a bilnear mapping with the same property, then there eixts a unique isomorphism $j : M \otimes N \to T'$ such that $j \circ g = g'$.

Proof. Will come back if there is time. The construction is somewhat not that important. □

09.10.2018
Below are some properties of the tensor product.

Proposition 6.35. *Let M be an R-module. Then*

$$R \otimes M \cong M$$

Proof. Consider the map

$$\begin{aligned} \alpha \colon R \otimes M &\to M \\ a \otimes m &\mapsto am \end{aligned}$$

We claim that α is a well defined R-module morphism. Indeed, consider the bilnear map

$$\begin{aligned} \tilde{\alpha} \colon R \times M &\to M \\ (a,m) &\mapsto am \end{aligned}$$

Then by Lemma 6.34, there is a unique corresponding R-linear map $\alpha \in \mathrm{Hom}(R \otimes M, M)$ such that

$$\alpha(a \otimes n) = \tilde{\alpha}(a,n) = am$$

This establishes that α is an R-linear morphism.
On the other hand, consider the map

$$\begin{aligned} \beta \colon M &\to R \otimes M \\ m &\mapsto 1 \otimes m \end{aligned}$$

We claim that β is a well definde R-module morphism as well. Indeed, if $m, m' \in M$, then

$$\beta(m+m') = 1 \otimes (m+m') = 1 \otimes m + 1 \otimes m'$$

And if $\lambda \in R$, then

$$\beta(\lambda m) = 1 \otimes \lambda m = \lambda(1 \otimes m)$$

This establishes that β is an R-linear morphism.

Claim.

$$\alpha \circ \beta = \beta \circ \alpha = \mathrm{id}$$

establishing the desired result.

PROOF OF CLAIM:
We first check that $\beta \circ \alpha = \mathrm{id}$: It suffices to check that this composition is indeed the identity on the generators $a \otimes m$ of $R \otimes M$. We have that

$$\beta \circ \alpha(a \otimes m) = \beta(am) = 1 \otimes am = a(1 \otimes m) = a \otimes m$$

as desired.
Now for the other composition. Let $m \in M$. Then we have

$$\alpha \circ \beta(m) = \alpha(1 \otimes m) = m$$

as desired.
END OF PROOF OF CLAIM. □

The next Proposition establishes the fact that "tensor product commutes with direct sum".

Proposition 6.36 (Tensor Product Commutes with Direct Sum). *Let $M = \bigoplus_{i \in I} M_i$ be a direct sum of modules. Then for any module N,*

$$M \otimes N \cong \bigoplus_{i \in I} (M_i \otimes N)$$

via the identifications

Proof. We give the proof for the case when M is the tensor product of two modules. It is then easy to extend the proof by induction. So suppose $M = M_1 \oplus M_2$.
First, we will construct a mapping α in the forward direction . Consider first the map

$$\begin{aligned} \tilde{\alpha} \colon M \times N &\to (M_1 \otimes N) \oplus (M_2 \otimes N) \\ ((m_1, m_2), n) &\mapsto ((m_1 \otimes n), (m_2 \otimes n)) \end{aligned}$$

which is easily seen to be bilinear and thus by the universal property of tensor product, there exists a unique module morphism

$$\alpha : M \otimes N \to (M_1 \otimes N) \oplus (M_2 \otimes N)$$

such that

$$\alpha((m_1, m_2) \otimes n) = \tilde{\alpha}((m_1, m_2), n) = ((m_1 \otimes n), (m_2 \otimes n))$$

For the mapping in the reverse direction, which we will call β, consider two bilinear maps:

$$\begin{aligned} \tilde{\phi_1} \colon M_1 \times N &\to M \otimes N \\ (m_1, n) &\mapsto (m_1, 0) \otimes n \end{aligned}$$

$$\begin{aligned} \tilde{\phi_2} \colon M_2 \times N &\to M \otimes N \\ (m_2, n) &\mapsto (0, m_2) \otimes n \end{aligned}$$

thus they induce unique module morphisms ϕ_1 and ϕ_2 as such:

$$\begin{tikzcd}
M_1 \otimes N \arrow[dr, "\tilde{\phi_1}"] & & M_2 \otimes N \arrow[dl, "\tilde{\phi_2}"] \\
& M \otimes N &
\end{tikzcd}$$

such that

$$\tilde{\phi_1}(m_1 \otimes n) = \phi_1(m_1, n) = (m_1, 0) \otimes n$$

and

$$\tilde{\phi_2}(m_2 \otimes n) = \phi_1(m_2, n) = (0, m_2) \otimes n$$

Therefore the map

$$\beta : (M_1 \otimes N) \oplus (M_2 \otimes N) \to M \otimes N$$

defined as

$$\beta(m_1 \otimes n_1, m_2 \otimes n_2) \coloneqq \tilde{\phi_1}(m_1 \otimes n_1) + \tilde{\phi_2}(m_2 \otimes n_2) = (m_1, 0) \otimes n_1 + (0, m_2) \otimes n_2$$

is a well defined module morphism. Now we need to show

$$\alpha \circ \beta = \mathrm{id} = \beta \circ \alpha$$

For the first equality, let $(m_1 \otimes n_1, m_2 \otimes n_2) \in (M_1 \otimes N) \oplus (M_2 \otimes N)$. Then we have

$$\begin{aligned}
\alpha \circ \beta((m_1 \otimes n_1, m_2 \otimes n_2) &= \alpha((m_1, 0) \otimes n_1 + (0, m_2) \otimes n_2) \\
&= \alpha((m_1, 0) \otimes n_1 + (0, m_2) \otimes n_2) \\
&= \alpha((m_1, 0) \otimes n_1) + \alpha((0, m_2) \otimes n_2) \\
&= ((m_1 \otimes n_1), (0 \otimes n_1)) + ((0 \otimes n_2), (m_2 \otimes n_2)) \\
&= ((m_1 \otimes n_1), 0) + (0, (m_2 \otimes n_2)) \\
&= (m_1 \otimes n_1, m_2 \otimes n_2)
\end{aligned}$$

as desired.
For the second equality, it suffices to show that the composition is the identity on generators $(m_1, m_2) \otimes n \in M \otimes N$. Then we have

$$\begin{aligned}
\beta \circ \alpha((m_1, m_2) \otimes n) &= \beta((m_1 \otimes n), (m_2 \otimes n)) \\
&= (m_1, 0) \otimes n + (0, m_2) \otimes n \\
&= ((m_1, 0) + (0, m_2)) \otimes n \\
&= (m_1, m_2) \otimes n
\end{aligned}$$

as desired.
Note: on second thought, induction may not be enough to extend to general case of I being an uncountable indexing set. However, one can still reproduce the proof for the general case by just using indexes, irregardless of countability. □

Proposition 6.37.

some more stuff about tensor products.... skip for now

6.5 Localization of Modules

We can generalize localization of a ring R at a multiplicatively closed subset $U \subset R$ to modules. More precisely, given an R-module M, we can define $M[U^{-1}]$ as such

Definition 6.38. Let M be an R-module and $U \subset R$ a multiplicatively closed subset of R. The *localization of M at U* is:

$$M[U^{-1}] := \{\tfrac{m}{u} : m \in M, u \in U\} /_{\sim}$$

where the equivalence relation is defined analogous as before, where we declare $\frac{m}{s} \sim \frac{n}{t}$ if there exists an element $u \in U$ such that

$$u(sn - tm) = 0$$

To make this a module, as before, we define

$$\frac{m}{s} + \frac{n}{t} := \frac{tm + sn}{st}$$

and for $a \in R$,

$$a \cdot \frac{m}{s} := \frac{am}{s}$$

The localization of modules can be described in terms of tensor products:

Lemma 6.39. *The natural map*

$$\alpha \colon R[U^{-1}] \otimes M \to M[U^{-1}]$$
$$\frac{r}{u} \otimes m \mapsto \frac{rm}{u}$$

is an isomorphism.

We claim that the map

$$\beta \colon M[U^{-1}] \to R[U^{-1}] \otimes M$$
$$\frac{m}{u} \mapsto \frac{1}{u} \otimes m$$

is the inverse to α. First we need to show that β is well-defined in the sense that it is independent of the choice of equivalence class. So let $\frac{m}{u} \sim \frac{m'}{u'}$ be equivalent elements in $M[U^{-1}]$. That is, there exists an element $v \in U$ such that $v(m'u - u'm) = 0$, that is, $vm'u = vu'm$. Therefore

$$\frac{1}{vuu'} \otimes vm'u = \frac{1}{vuu'} vu'm$$

thus

$$\frac{vu}{vuu'} \otimes m' = \frac{vu'}{vuu'} m$$

so

$$\frac{1}{u'} \otimes m' = \frac{1}{u} \otimes m$$

which is equivalent to $\beta(\frac{m'}{u'}) = \beta(\frac{m}{u})$, as desired. Now we show that

$$\alpha \circ \beta = \mathrm{id}_{M[U^{-1}]}$$

and

$$\beta \circ \alpha = \mathrm{id}_{R[U^{-1}] \otimes M}$$

First Equality: Let $\frac{m}{u} \in M[U^{-1}]$. Then

$$\begin{aligned} \alpha \circ \beta \left(\frac{m}{u}\right) &= \alpha\left(\frac{1}{u} \otimes m\right) \\ &= \frac{m}{u} \end{aligned}$$

Second Equality: As usual, it suffices to check the result on generators. Let $\frac{n}{u} \otimes m \in R[U^{-1}] \otimes M$. Then

$$\begin{aligned} \beta \circ \alpha \left(\frac{n}{u} \otimes m\right) &= \beta\left(\frac{nm}{u}\right) \\ &= \frac{1}{u} \otimes nm \\ &= \frac{n}{u} \otimes m \end{aligned}$$

6.6 Flat Modules

11.10.2018

6.7 Noetherian Modules

6.8 Localization of a Module at a Prime Ideal

Let $\mathfrak{p}$ be a prime ideal of R and M an R-module. We can localize M at the multiplicatively closed set

$$U_{\mathfrak{p}} \coloneqq R \setminus \mathfrak{p}$$

We denote this localiztion

$$M_{\mathfrak{p}} \coloneqq M[U_{\mathfrak{p}}^{-1}]$$

Lemma 6.40. *Let M be an R-module. Let $x \in M$. Then $x = 0$ if and only if for all $\mathfrak{p} \in \operatorname{Spec}(R)$, the image $x_{\mathfrak{p}} \in M_p$ of x under the canonical mapping satisfies $x_p = 0$.*

Proof. The forward direction is trivial: if $x = 0$, then $x_{\mathfrak{p}} = 0$ in the localization. For the reverse direction, suppose $x_{\mathfrak{p}} = 0$. Then for some $a \in U_{\mathfrak{p}}$, we have $ax = 0$. This is because in $M_{\mathfrak{p}}$, we have

$$\frac{x}{1} \sim \frac{0}{1}$$

implying that there exists some $a \in U_{\mathfrak{p}}$ such that $(x \cdot 1 - 1 \cdot 0) = ax = 0$. This means that there is some element in $U_{\mathfrak{p}}$ that annihilates x. Therefore we must have

$$\operatorname{Ann}(x) \cap U_{\mathfrak{p}} \neq \emptyset \tag{8}$$

thus

$$\operatorname{Ann}(x) \not\subset \mathfrak{p} \tag{9}$$

for any prime ideal $\mathfrak{p}$ (if this were not the case then $\operatorname{Ann}(x) \subset \mathfrak{p} \cap U_{\mathfrak{p}} = \emptyset$ contradicting (8)). We want to show that $x = 0$, so aiming for a contradiction suppose $x \neq 0$ in M. Since

$$\operatorname{Ann}(x) = (1) = R \iff x = 0$$

The annihilator of x must be a proper ideal of R, and so there exists a maximal ideal P containing it:

$$\operatorname{Ann}(x) \subset P \subsetneq R$$

But maximal ideals are prime, so this contradicts (9). Therefore we have the desired result. □

There is another formulation of the result of the previous Lemma:

Proposition 6.41. *Let M be an R-module. Then the following are equivalent:*

1. *$M = 0$*
2. *$M_{\mathfrak{p}} = 0$ for all prime ideals $\mathfrak{p}$ of R.*
3. *$M_{\mathfrak{m}} = 0$ for all maximal ideals $\mathfrak{m}$ of R.*

Proof. The implications 1. ⇒ 2. ⇒ 3. ⇒ are clear. Now suppose 3. is satisfied, and by contradiction suppose $M \neq 0$. Thus there exists a non-zero element $0 \neq x \in M$. Thus $\operatorname{Ann}(x) \subsetneq (1)$ is a proper ideal. Thus it is contained in a maximal ideal $\mathfrak{m}$. Now consider the localization $M_{\mathfrak{m}}$, and the image of x: $\frac{x}{1} \in M_{\mathfrak{m}}$. Since $M_{\mathfrak{m}} = 0$, $\frac{x}{1} = 0$. By definition this means there exists an element $u \in A \setminus \mathfrak{m}$ such that $ux = 0$. That is, there is an element of $\operatorname{Ann}(x)$ in $A \setminus m$. But this is impossible since we have established that $\operatorname{Ann}(x) \subset \mathfrak{m}$. □

Corollary 6.42. *If $K \subset M$ is a submodule, then $K = 0$ if and only if $K_{\mathfrak{p}} = 0$ for all prime ideal $\mathfrak{p}$.*

Proof. Follows immediately from the previous Proposition. □

Proposition 6.43. *Let $\phi : M \to N$ be an R-module morphism. Then the following are equivalent:*

1. *ϕ is injective.*
2. $$\begin{aligned}\phi_{\mathfrak{p}} : M_{\mathfrak{p}} &\to N_{\mathfrak{p}} \\ \frac{m}{u} &\mapsto \frac{\phi(m)}{u}\end{aligned}$$ *is injective for each prime ideal $\mathfrak{p}$.*
3. $$\begin{aligned}\phi_{\mathfrak{m}} : M_{\mathfrak{m}} &\to N_{\mathfrak{m}} \\ \frac{m}{v} &\mapsto \frac{\phi(m)}{v}\end{aligned}$$ *is injective for each maximal ideal $\mathfrak{m}$.*

Similarly with "injective" replaced by "surjective" throughout.

Proof. □

7 Associated Primes of Ideals

In this section, let R be a Noetherian ring and M a finitely generated R-module, which we know from before implies that M is a Noetherian module.

Definition 7.1. A prime $\mathfrak{p} \subset R$ is said to be *associated to M* if there exists a non-zero element $0 \neq f \in M$ such that
$$\mathfrak{p} = \text{Ann}(f) = \{a \in R : af = 0\}$$
And we denote the set of associated primes of M:
$$\text{Ass}_R(M) = \text{Ass}(M) = \{\mathfrak{p} : \mathfrak{p} \subset R,\ \mathfrak{p} \text{ associated prime of } M\}$$

Lemma 7.2. *For all $f \in M$, we have*
$$R \big/ \text{Ann}(f) \cong R \cdot f$$
where $R \cdot f$ is the submodule of M generated by f.

Proof. Consider the module morphism
$$\begin{aligned}\phi \colon R &\to R \\ r &\mapsto rf\end{aligned}$$
Then we have
$$\ker(\phi) = \text{Ann}(f)$$
Thus by the First Isomorphism Theorem, we have
$$R \big/ \ker(\phi) = R \big/ \text{Ann}(f) \cong \text{Im}(\phi) = R \cdot f$$
□

This enables us to give the following Proposition:

Proposition 7.3. *A prime ideal $\mathfrak{p} \subset R$ is associated to M if and only if M contains a submodule isomorphic to $R/\mathfrak{p}$.*

Proof. Suppose there exists a submodule $S \subset M$ such that S is isomorphic to $R/\mathfrak{p}$. Then and non-zero element $f \in S$ has the property that

$$\mathrm{Ann}(f) = \mathfrak{p}$$

Indeed, let $\tilde{f} \in R$ be represent $f \in S = R/\mathfrak{p}$ (i.e. an element in f, which is an equivalence class). Then $\tilde{f} \notin \mathfrak{p}$ since f is chosen to be non-zero. If $a \in R$ satisfies $af = 0$ (i.e. $a \in \mathrm{Ann}(f)$), then $a\tilde{f} \in \mathfrak{p}$. By primality, $a \in \mathfrak{p}$. Thus

$$\mathrm{Ann}(f) \subset \mathfrak{p}$$

The other inclusion is trivial since, $\mathfrak{p}$ annihilates all of $R/\mathfrak{p}$, so in particular it annihilates f. This shows that $\mathfrak{p}$ is indeed associated to M.
On the other hand, if we assume that $\mathfrak{p}$ is associated to M, i.e. $\mathfrak{p} = \mathrm{Ann}(f)$ for some $0 \neq f \in M$. Then by Lemma 7.2, we have

$$R\big/\mathfrak{p} = R\Big/\mathrm{Ann}(f) \cong R \cdot f$$

And $R \cdot f$ is indeed a submodule of M. □

Definition 7.4. Let $I \subset R$ be any ideal. We say that a prime ideal $\mathfrak{p} \subset R$ is a *minimal prime of (or over) I* if $I \subset \mathfrak{p}$ and there exists no prime ideal $\mathfrak{q}$ such that

$$I \subset \mathfrak{q} \subsetneq \mathfrak{p}$$

We will show later that in fact a prime $\mathfrak{p}$ is associated to M if and only if $\mathfrak{p}$ is a minimal prime over $\mathrm{Ann}(f)$ for some $0 \neq f \in M$. We now give some examples of associated primes for some modules.

Example 7.5. There are no associated primes for a zero module: $\mathrm{Ass}(\{0\}) = \emptyset$.

Example 7.6. $\mathrm{Ass}(R/\mathfrak{p}) = \{\mathfrak{p}\}$ (viewing $R/\mathfrak{p}$ as a module), for any prime $\mathfrak{p}$. This follows from the proof of Proposition 7.3, where we showed that every non-zero element $f \in R/\mathfrak{p}$ has the property that $\mathrm{Ann}(f) = \mathfrak{p}$. thus establishing that $\mathfrak{p}$ is an associated prime.

Example 7.7. Let $n \geq 1$, p a prime number. Consider $\mathbb{Z}/p^n\mathbb{Z}$ as a $\mathbb{Z}$-module. Then

$$\mathrm{Ass}_{\mathbb{Z}}\left(\mathbb{Z}\big/p^n\mathbb{Z}\right) = \{(p)\}$$

Proof. Consider a non-zero element $0 \neq \overline{f} \in \mathbb{Z}/p^n\mathbb{Z}$. Then its representative may be written as

$$f = kp^n = up^m$$

NEED CLARIFICATION □

Lemma 7.8. *Let P be a maximal element among the following set of ideals*

$$\{\mathrm{Ann}(f) : 0 \neq f \in M\}$$

Then P is a prime ideal (and thus belongs to $\mathrm{Ass}(M)$*).*

Proof. Suppose $P = \mathrm{Ann}(f)$, $0 \neq f \in M$. Then P is a proper ideal of R since f is non-zero. Suppose $ab \in P$. Then $ab \in \mathrm{Ann}(f)$ which means $abf = 0$. Thus $a \in \mathrm{Ann}(bf)$. We have the inclusion $P = \mathrm{Ann}(f) \subset \mathrm{Ann}(bf)$ just by definition; together with the maximality of P forces the equality

$$\mathrm{Ann}(bf) = \mathrm{Ann}(f)$$

Thus $a \in \mathrm{Ann}(f) = P$. Thus establishing that P is prime. □

Note that we were alowed to choose a maximal element by the Noetherian assumption (on R?). An important Corollary that any non-zero module has non-empty set of associated prime follows:

Corollary 7.9. *If $M \neq \{0\}$, then* $\mathrm{Ass}(M) \neq \emptyset$*.*

Proof. Since M is non-zero, the set $\{\mathrm{Ann}(f) : 0 \neq f \in M\}$ is non-empty, and by the previous Lemma, there exists a prime ideal that belongs to $\mathrm{Ass}(M)$. □

Lemma 7.10. *Let*

$$0 \to M' \xrightarrow{\phi} M \xrightarrow{\gamma} M'' \to 0$$

be an exact sequence of modules. Then

$$\mathrm{Ass}(M') \subset \mathrm{Ass}(M) \subset (\mathrm{Ass}(M') \cup \mathrm{Ass}(M''))$$

Proof. First Inclusion: Let $\mathfrak{p} \in \mathrm{Ass}(M')$. By Proposition 7.3, M' contains a submodule isomorphic to $R/\mathfrak{p}$, that is, there is an injection

$$R \big/ \mathfrak{p} \hookrightarrow M'$$

Thus we have, from the exact sequence,

$$R \big/ \mathfrak{p} \hookrightarrow M' \overset{\phi}{\hookrightarrow} M$$

Composition of injections is an injection, therefore $R/\mathfrak{p}$ is isomorphic to its image in M, which is a submodule of M. Therefore the other direction of Proposition 7.3 implies that $\mathfrak{p}$ is an associated prime of M, os $\mathfrak{p} \in \mathrm{Ass}(M)$.

Second Inclusion: It suffices to show that if $\mathfrak{p} \in \mathrm{Ass}(M)$ and $\mathfrak{p} \notin \mathrm{Ass}(M')$, then we have $\mathfrak{p} \in \mathrm{Ass}(M'')$. Take $\mathfrak{p}$ with those assumed properties. thus there exists some $f \in M$ such that $\mathfrak{p} = \mathrm{Ann}(f)$. Now by Proposition 7.3, $R/\mathfrak{p}$ is isomorphic to a submodule of $R/\mathfrak{p} \hookrightarrow M$. In particular, if we go back to the proof of the Proposition, we have

$$S := R \cdot f \cong R \big/ \mathfrak{p} \hookrightarrow M$$

From the proof of the Proposition we also know that any non-zero element of S has annihilator $\mathfrak{p}$. By the exact sequence we can regard M' as a submodule of M, so we can consider the intersection of submodules (of M):

$$S \cap M' = \{0\}$$

whici is $\{0\}$, otherwise there exists some element in M' which also has $\mathfrak{p}$ as its annihilator, contradicting the assumption that $\mathfrak{p} \notin \mathrm{Ass}(M')$. By the exact sequence, $\ker(\gamma) = \mathrm{Im}(\phi) = M'$. Therefore the kernel of the composition

$$S \hookrightarrow M \xrightarrow{\gamma} M''$$

is $S \cap M' = \{0\}$. Thus the composition is injective, implying that $S = R/\mathfrak{p}$ is isomorphic to a submodule of M''. Therefore $\mathfrak{p} \in \mathrm{Ass}(M'')$. □

Lemma 7.11. *Any finitely generated module M over a Noetherian ring R admits a filtration of submodules of the following form:*

$$\{0\} = M_0 \subsetneq M_1 \cdots \subsetneq M_n = M$$

such that

$$M_j \Big/ M_{j-1} \cong R \Big/ \mathfrak{p}_j$$

for prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \subset R$

Proof. If $M = \{0\}$, then the assertion is trivially true. Else, $\mathrm{Ass}(M)$ is non-empty by Corollary 7.9. So take an element $\mathfrak{p}_1 \in \mathrm{Ass}(M)$. By Proposition 7.3, we have

$$R \big/ \mathfrak{p}_1 \cong M_1 \subset M$$

for some submodule M_1 of M. If in fact $M_1 = M$, then we are done. Else, $M/M_1 \neq \{0\}$, therefore the set of associated primes is again non-empty, thus we can take an element $\mathfrak{p}_2 \in \mathrm{Ass}(M/M_1)$. Then we have

$$R \big/ \mathfrak{p}_2 \cong \overline{M_2} \subset M \big/ M_1 \tag{10}$$

for some submodule $\overline{M_2}$ in M/M_1. Let $M_2 \subset M$ be the preimage of $\overline{M_2}$ under the projection $M \twoheadrightarrow M/M_1$. Then M_2 is a submodule of M. Furthermore, since $\mathfrak{p}_2 \neq R$ by definition of prime ideal, (10) implies that $\overline{M_2} \neq 0$ in M/M_1. Therefore we must have $M_1 \subsetneq M_2$ in M. Moreover, we have

$$ {}^{M_2}\big/_{M_1} \cong \overline{M_2} \cong {}^{R}\big/_{\mathfrak{p}_2} $$

Repeating this process, we must terminate at some $M_n = M$ since by assumption M is finitely generated and R is Noetherian, thus M is Noetherian. Thus the ascending chain of submodules M_i must terminate. □

Corollary 7.12. *With notation as the above Lemma, we have that*

$$ \mathrm{Ass}(M) \subset \{\mathfrak{p}_1, \dots, \mathfrak{p}_n\} $$

Proof. Induct on n. First, the base case of $n = 1$. Then $M \cong R/\mathfrak{p}_1$. Then for any $\mathfrak{q} \in \mathrm{Ass}(M)$, we must have $R/\mathfrak{q}$ as a submodule of M:

$$ {}^{R}\big/_{\mathfrak{q}} \hookrightarrow M = {}^{R}\big/_{\mathfrak{p}_1} $$

this means that

$$ \mathfrak{q} \supset \mathfrak{p}_1 $$

On the other hand, if we write $\mathfrak{q} = \mathrm{Ann}(\tilde{f})$ for some $\tilde{f} \in M = R/\mathfrak{p}_1$, then we see

$$ \mathfrak{q} = \mathrm{Ann}(\tilde{f}) \subset \mathfrak{p}_1 $$

Thus we must have $\mathbb{Q} = \mathfrak{p}_1$.
Induction Hypothesis: Suppose the assertion is true for $n = k$.
We construct the short exact sequence

$$ 0 \to M_1 \to M \to {}^{M}\big/_{M_1} \to 0 $$

By Lemma 7.10 we have

$$ \mathrm{Ass}(M_1) \subset \mathrm{Ass}(M) \subset \mathrm{Ass}(M_1) \cup \mathrm{Ass}\left({}^{M}\big/_{M_1}\right) \tag{11} $$

By Lemma 7.11, we have the filtration

$$ 0 \subsetneq M_1 \subsetneq M_2 \subsetneq \cdots \subsetneq M $$

If we mod out M_1 on this filtration we get

$$ 0 \subsetneq \overline{M_2} \subsetneq \cdots \subsetneq {}^{M}\big/_{M_1} $$

where $\overline{M_j} := M_j/M_1$. By the Induction Hypothesis,

$$ \mathrm{Ass}\left({}^{M}\big/_{M_1}\right) \subset \{\mathfrak{p}_2, \dots, \mathfrak{p}_n\} $$

and from the base case we know $\mathrm{Ass}(M_1) \subset \{\mathfrak{p}_1\}$. Therefore (11) implies

$$ \mathrm{Ass}(M) \subset \{\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_n\} $$

as desired. □

Corollary 7.13. *If*

$$ M = M_1 \oplus \cdots \oplus M_n $$

then

$$ \mathrm{Ass}(M) = \bigcup_i^n \mathrm{Ass}(M_i) $$

Proof. Induct on i. Base case: if $M = M_1 \oplus M_2$, then we can construct the short exact sequence of modules:

$$0 \to M_1 \xrightarrow{f} M \xrightarrow{g} M_2 \to 0$$

where

$$\begin{aligned} f\colon M_1 &\to M \\ x &\mapsto (x, 0) \end{aligned}$$

and

$$\begin{aligned} g\colon M &\to M_2 \\ (m_1, m_2) &\mapsto m_2 \end{aligned}$$

Then be Lemma 7.10, we must have

$$\operatorname{Ass}(M) \subset \operatorname{Ass}(M_1) \cup \operatorname{Ass}(M_2)$$

For the other inclusion, let $\mathfrak{p} \in \operatorname{Ass}(M_1) \cup \operatorname{Ass}(M_2)$. We can consider both M_1 and M_2 as submodules of M because they both can be injected in to M. WOLOG, say $\mathfrak{p} \in \operatorname{Ass}(M_1)$, then we can write $\mathfrak{p} = \operatorname{Ann}(f)$ for some $f \in M_1$. But then $f \in M$ as well so $\mathfrak{p} \in \operatorname{Ass}(M)$. Thus we have the equality

$$\operatorname{Ass}(M) = \operatorname{Ass}(M_1) \cup \operatorname{Ass}(M_2)$$

Induction Hypothesis: Suppose the assertion holds for all i up to some $i = k > 2$. Let $A \coloneqq \bigoplus_{i=1}^{k-1} M_i$. Then by the induction hypothesis we have

$$\operatorname{Ass}(A) = \bigcup_{i=1}^{k-1} \operatorname{Ass}(M_i)$$

Now we have $M = A \oplus M_n$, so we can again construct the short exact sequence:

$$0 \to A \to M \to M_n \to 0$$

and using the same process obtain that

$$\operatorname{Ass}(M) = \operatorname{Ass}(A) \cup \operatorname{Ass}(M_n)$$

Thus by the Principle of Mathematical Induction, we have the desired result. □

Associated primes behave well with respect to localization:

Lemma 7.14. *The formation of the set* $\operatorname{Ass}(M)$ *commutes with localization at an arbitrary multiplicatively closed set* U*, in the sense that*

$$\operatorname{Ass}_{R[U^{-1}]}(M[U^{-1}]) = (\operatorname{Spec} R[U^{-1}]) \cap \operatorname{Ass}_R(M)[U^{-1}]$$

Proof. We can try to interpret this equlity by looking at the two inclusions separately.

$$\operatorname{Ass}_{R[U^{-1}]}(M[U^{-1}]) \supset (\operatorname{Spec} R[U^{-1}]) \cap \operatorname{Ass}_R(M)[U^{-1}]$$

says the following: Take a prime in the right hand side: $Q \in (\operatorname{Spec} R[U^{-1}]) \cap \operatorname{Ass}_R(M)[U^{-1}]$. First, $Q \in \operatorname{Spec}(R[U^{-1}])$. But we know that a prime in the localization is in bijection (via "localizing") with primes "upstairs" which do not intersect U. That is, $Q = \mathfrak{p}[U^{-1}]$ for some $\mathfrak{p} \in \operatorname{Spec} R$. Second, $Q \in \operatorname{Ass}_R(M)[U^{-1}]$, so Q is the localization of some associated prime, thus we must have $\mathfrak{p} \in \operatorname{Ass}_R(M)$. Therefore, this inclusion says that if $\mathfrak{p} \in \operatorname{Ass}_R(M)$, where $\mathfrak{p} \cap U = \emptyset$, then

$$\mathfrak{p}[U^{-1}] \in \operatorname{Ass}_{R[U^{-1}]}(M[U^{-1}])$$

To show this, we notice that the assumption indicates that we have

$$R/\mathfrak{p} \hookrightarrow M$$

as a submodule. Since localization preserves kernels (Proposition ????), we have

$$\left(R/\mathfrak{p}\right)[U^{-1}] \hookrightarrow M[U^{-1}]$$

□

Theorem 7.15. *Suppose R is Noetherian and $M \neq \{0\}$ a finitely generated R-module. Then $Ass(M)$ is non-empty, finite, and contains all the minimal primes of* $\mathrm{Ann}(M)$*. Moreover,*

$$\{\textit{zero divisors on } M\} = \bigcup_{0 \neq f \in M} \mathrm{Ann}(f) = \bigcup_{p \in \mathrm{Ass}(M)} \mathfrak{p}$$

Proof. Non-emptiness is Corollary 7.9. Finiteness is Corollary 7.12. Now let $\mathfrak{p}$ be a prime ideal minimal over $\mathrm{Ann}(M)$. We want to show that it is in $\mathrm{Ass}(M)$. Since by assumption $M \neq 0$ so $\mathfrak{p} \neq 0$. Therefore by Proposition ¿¿¿ the localization $M_\mathfrak{p} \neq 0$. Let $p \coloneqq \mathfrak{p}_\mathfrak{p} \subset R_\mathfrak{p}$ denote the image of $\mathfrak{p}$ in the localization, i.e. the unique maximal ideal in the localization. □

8 Primary Decomposition

Definition 8.1.

9 Integrality

10 Primes in Integral Extentions

11 Proving Hilbert's Nullstellensatz

We have already mentioned various versions of Hilbert's Nullstellensatz, which are all equivalent. We are now ready to prove them. For clarity the following illustrates the process:

$$\begin{tikzcd}
\text{Full-Blown Nullstellensatz} \arrow[r, leftrightarrow] & \text{Classic Nullstellensatz} \arrow[r, leftrightarrow] & \text{Weak Nullstellensatz} \\
 & \text{Zariski's Lemma} \arrow[u] & \\
\text{Direct Proof with 4 Sublemmas} \arrow[ur] & \text{Noether Normalization} \arrow[u] & \text{Jacobson Rings} \arrow[ul]
\end{tikzcd}$$

As we can see, Zariski's Lemma is central to all of this. We state it here.

Theorem 11.1 (Zariski's Lemma)**.** *Let Ω/k be a field extension where Ω is at the same time a finitely generated k-algebra (in particular if $k = \overline{k}$ then $\Omega = k$). Then*

$$[\Omega : k] < \infty$$

i.e. Ω/k is a finite field extension.

We will have three ways to prove Zariski's Lemma.

11.1 Zariski's Lemma by Direct Proof

There are exactly four "sublemmas" needed to prove Zariski's Lemma directly.

Lemma 11.2 (Zariski's Sublemma 1.)**.** *Let k be a field. Suppose $f \in k[x]$ is a non-zero polynomial. Then there exists a finite field extension L/k, and $\alpha \in L$ such that $f(\alpha) \neq 0$.*

Proof. Take $\alpha \in \overline{k}$ such that $f(\alpha) \neq 0$, and let $L := k(\alpha)$. □

Lemma 11.3 (Zariski's Sublemma 2.)**.** *Let k be a field. Suppose $f \in k[x_1, \dots, x_n]$ for $n \geq 1$ is a non-zero (multivariate) polynomial. Then there exists a field extension L/k and a set of elements $\{\alpha_1, \dots, \alpha_n\} \in L$ such that $f(\alpha_1, \dots, \alpha_n) \neq 0$.*

Proof. Not sure. □

Lemma 11.4 (Zariski's Sublemma 3.)**.** *Let k be a field. Suppose $f \in k[x_1, \dots, x_n]$ for $n \geq 1$ is a non-zero polynomial. Then the ring*

$$R := k\left[x_1, \dots, x_n, \frac{1}{f}\right]$$

is not a field.

Proof. Suppose by contradiction that R is a field. Then choosing the field extension L and $\alpha = \{\alpha_1, \dots, \alpha_n\}$ as in Lemma 11.3 (Zariski's Sublemma 2.), we get an injective map of k-algebras:

$$\phi : R \to L$$

$$x_i \mapsto \alpha_i$$
$$\frac{1}{f} \mapsto \frac{1}{f(\alpha)}$$

This is injective because the kernel only contains the zero polynomial. Since L is a finite extension of k, i.e. L is a finite dimensional vector space over k. Thus we have $\dim_k(L) < \infty$. However, the dimension of R as a vector space over k is infinite (why?). Thus this is a contradiction since we cannot inject an infinite dimensional vector space into a finite dimensional vector space. There is a nother proof in Eis. Section 4.6. □

Lemma 11.5. *Let Ω be a field, $R \subset \Omega$ a subring such that the following are satisfied:*

1. *Ω is algebraic over $K := \mathrm{Frac}(R)$.*
2. *Ω is a finitely generated R-algebra.*

Then there exists a non-zero $f \in R$ such that Ω is finite over $R[f^{-1}]$.

Proof. Suppose $x_1, \dots, x_n \in \Omega$ are the generators of Ω as an R-algebra. Then using that Ω is algebraic over K, we have for any $j = 1, \dots, n$:

$$x_j^{N(j)} + c_{j,1}x_j^{N(j)-1} + \cdots + c_{j,N(j)} = 0$$

where $c_{j,k} \in K$ and $N(j)$ is a natural number dependent on j. We can write each $c_{j,k}$ as a fraction $\frac{a_{j,k}}{b_{j,k}}$, $a_{j,k}, b_{j,k} \in R$. Then multiplying by the denominator of the leading coefficient we get

$$\lambda_j x_j^{N(j)} + \cdots = 0$$

where $\lambda_j \in R$ and $\lambda \neq 0$. Then this implies that x_j is integral over $R[lambda^{-1}]$. Now define

$$f := \lambda_1 \cdots \lambda_n$$

Then notice that $R[\lambda_j^{-1}] \subset R[f^{-1}]$ for any j. Indeed if $\frac{r}{\lambda_j} \in R[\lambda_j^{-1}]$, then we have the equivalence

$$\frac{r}{\lambda_j} \sim \frac{r\prod_{i \neq j} \lambda_j}{\lambda_j \prod_{i \neq j} \lambda_i} \quad \text{in } R[f^{-1}]$$

Thus the inclusion implies that each x_j is in particular integral over $R[f^{-1}]$. Therefore Ω is finite over $R[f^{-1}]$. □

Now we can state the proof of Zariski's Lemma:

Proof. PROOF OF ZARISKI'S LEMMA: Since Ω is a finitely generated k-algebra, and Ω and k both being fields means $\Omega = k(S)$ for some finite set $S \subset \Omega$. Then we know by Theorem ??????, there must exist a finite transcendence basis $\{x_1, \ldots, x_n\}$ for Ω/k. Let $R \coloneqq k[x_1, \ldots, x_n]$ and $K \coloneqq \mathrm{Frac}(R) = k(x_1, \ldots, x_n)$. Then Ω is algebraic over K (Why???). Also, since Ω is finitely generated as a k-algebra hence it is also finitely generated as an R-algebra. Now it suffices to show that $n = 0$, which would imply $K = k$. Then Ω is algebraic over k and finitely generated over k, therefore finite over k which is equivalent to $[\Omega : k] < \infty$. To that end we assume otherwise that $n \geq 1$. Then by Sublemma 4. we have that there exists a non-zero $f \in R$ such thtat Ω is finite over $R[f^{-1}]$, which is equivalent to Ω being integral over $R[f^{-1}]$. Thus by Lemma ?? since Ω is a field be know $R[f^{-1}]$ is a field. This contradicts Sublemma 3. □

11.2 Noether Normalization

Lemma 11.6 (Noether's Normalization Lemma)**.** *Let k be a field and A a finitely generated k-algebra. Then there exists a nonnegative integer d and algebraically independent elements $\{y_1, \ldots, y_d\} \subset A$ such that A is finite over the polynomial ring $k[y_1, \ldots, y_d]$.*

Proof. TOO FUCKING HARD. □

Proof. PROOF OF ZARISKI'S LEMMA: By Noether's Normalization Lemma, there exists a nonnegative integer d and algebraically independent elements $\{y_1, \ldots, y_d\} \subset \Omega$ such that Ω is a finitely generated module over $k[y_1, \ldots, y_d]$.

Claim. $d = 0$.

PROOF OF CLAIM: Since Ω is a field, ... ???
Thus we have Ω is a finitely generated module over k, i.e. $[\Omega : k] < \infty$. □

11.3 Jacobson Rings

Definition 11.7. A ring R is called a *Jacobson ring* is every prime ideal is the intersection of maximal ideals. Equivalently, for any prime ideal $\mathfrak{p} \subset R$, we have

$$\mathfrak{p} = \bigcap_{m \supset \mathfrak{p}, m \text{ maximal ideal}} m$$

And equivalently, for any prime ideal $\mathfrak{p}$,

$$\mathrm{Jac}\left({}^{R}/_{\mathfrak{p}}\right) = 0$$

(Recall that the Jacobson radical is defined to be the intersection of all maximal ideals)

Theorem 11.8. *Let R be a Jacobson ring and S a finitely generated R-algebra. Then S is Jacobson and for all maximal ideal $n \subset S$, the ideal $m \coloneqq R \cap n$ is maximal. Furthermore, S/n is a finite field extension of R/m.*

We first show that this Theorem implies Zariski's Lemma:

Proof. PROOF OF ZARISKI'S LEMMA: If $R = k$ is a field, then R is Jacobson. If Ω is a finitely generated R-algebra and is also a field. Then Theorem 11.8 implies that Ω is Jacobson (which actually follows also from Ω being a field). More importantly, since $\{0\}$ is a (the only) maximal ideal of Ω, we have

$$\Omega = {}^{\Omega}/_{0}$$

is a finite extension of $k/0 = k$, as desired.

□

11.4 Zariski's Lemma Implies Nullstellensatz

Now we show how Zariski's Lemma implies the Classic Nullstellensatz. This will be sufficient for the other versions of Nullstellensatz as we showed before they are all equivalent.

Proof. PROOF OF THE CLASSIC NULLSTELLENSATZ: □

12 Filtrations and Artin-Rees Lemma

13 Tor and Flatness

14 Completion

15 Dimension Theory

Throughout this section we assume R is a Noetherian ring.

Definition 15.1.

$$\dim(R) \coloneqq \sup_n \{n : \mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_n : \mathfrak{p}_i \text{ prime ideals in } R\}$$

In particular $\dim(R) = 0$ if and only if there are no prime in R that contain some other (distinct) prime.

Proposition 15.2. *Suppose R is an integral domain. Then* $\dim(R) = 0$ *if and only if R is a field.*

Proof. Notice that R being an integral domain implies that (0) is a prime ideal. Suppose $\dim(R) = 0$, then there cannot exist any other prime ideals, otherwise we will be able to form a chain of length $1 > 0$. Therefore there cannot be any other maximal ideal other than (0), so R is a field. The converse is obvious since the only ideals are (0) and (1). □

Proposition 15.3. *Suppose R is an integral domain. Then* $\dim(R) \leq 1$ *if and only if every non-zero prime ideal $\mathfrak{p}$ is a maximal ideal.*

Proof. Suppose $\dim(R) \leq 1$. For the case $\dim(R) = 0$ we have already shown that R is a field so there are no non-zero prime ideals thus the assersion is vacuously true. For the case $\dim(R) = 1$, suppose by contradiction that there exists some prime ideal $\mathfrak{p} \neq (0)$ that is non maximal. We can then form the chain of prime ideals $(0) \subsetneq \mathfrak{p} \subsetneq m$ for some maximal ideal m. This contradicts $\dim(R) = 1$. For the other direction, suppose that every non-zero prime ideal is maximal, then there cannot be any chain of prime ideals of length greater than or equal to 2. Therefore $\dim(R) \leq 1$. □

15.1 Zero-Dimensional Rings

Here we list some examples of rings whose dimension is zero.

Example 15.4. A field has dimension zero.

Example 15.5. $R \coloneqq k[x]/(x^n)$, which has exactly one prime ideal $\mathfrak{p} = (x)$.

Example 15.6. $R \coloneqq k[x^2, x^3]/(x^n)$ for large n. Notice that $x \notin k[x^2, x^3]$ but every other power of x is in $k[x^2, x^3]$. R has exactly one prime $\mathfrak{p} = (x^2, x^3)$.

Example 15.7. Multivariate generalizations of $k[x, y]/(x, y^n)$. (???)

Recall that a module M is *Noetherian* if it satisfies the ACC on submodules. A ring R is likewise Noetherian if it satisfies the ACC on ideals. There is a related definition:

Definition 15.8. A module/ring is called *Aritnian* or *Artin* if it satisfies the DCC on submodules/ideals.

Lemma 15.9. *If*

$$0 \to M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \to 0$$

is a short exact sequence of modules, then M is Artinian if and only if M' and M'' are Artinian.

Proof. Same proof as the one in the Noetherian case. We show here the case for a module (it's really the same thing for rings). Suppose M is Artinian. Suppose $\{L_n\}_{n\geq 1}$ is a descending chain in M', and $\{K_n\}_{n\geq 1}$ is a descending chain in M''. Then $\{\alpha(L_n)\}_{n\geq 1}$ is a descending chain in M and $\{\beta^{-1}(K_n)\}_{n\geq 1}$ is a descending chain in M. Therefore these two chains terminate, and mapping them to the respective modules gives the result. Conversely, suppose M' and M'' are Artinian. Let $\{L_n\}_{n\geq 1}$ be a descending chain in M. Then $\{\alpha^{-1}\}_{n\geq 1}$ is a descending chain in M'. Similarly $\{\beta(L_n)\}_{n\geq 1}$ is a descending chain in M''. For large enough n, both chains terminate in M' and M'' respectively. That is, for large enough n we have

$$\alpha^{-1}(L_n) = \alpha^{-1}(L_{n+1})$$

and

$$\beta(L_n) = \beta(L_{n+1})$$

We want to show that $L_n = L_{n+1}$. The inclusion $L_n \supset L_{n+1}$ is by assumption so we show the other inclusion. Suppose $x \in L_n$. Then $\beta(x) \in \beta(L_n) = \beta(L_{n+1})$. By the surjectivity of β, there exists some $y \in L_{n+1}$ such that $\beta(y) = \beta(x)$. Thus $x - y \in \ker(\beta) = \operatorname{Im}(\alpha)$. Thus there exists some $z \in M'$ such that $\alpha(z) = x - y$. Since $x - y \in L_n$ (because both are in L_n), $z \in \alpha^{-1}(L_n) = \alpha^{-1}(L_{n+1})$. Therefore $\alpha(z) = x - y \in L_{n+1}$ and therefore $x \in L_{n+1}$ since $y \in L_{n+1}$, as desired. □

Lemma 15.10. *Let R be an Aritinian integral domain. Then R is a field.*

Proof. Let $x \in R$ be a non-zero element. We want to show that x has a multiplicative inverse. Consider the descending chain of ideals:

$$(x) \supset (x^2) \supset (x^3) \supset \dots$$

Since R is Artinian, this chain stabilizes, so $(x^n) = (x^{n+1} = \dots$ for some n. Thus $x^n \in (x^{n+1})$, so $x^n = yx^{n+1}$ for some $y \in R$. Therefore $x^n = yxx^n$. Thus

$$x^n - yxx^n = 0$$

$$x^n(1 - yx) = 0$$

since $x^n \neq 0$ since in an integral domain there does not exist non-zero divisors. Therefore we must have $1 - yx = 0$, i.e. $yx = 1$, as desired. □

Proposition 15.11. *Let R be an Artinian ring and $\mathfrak{p} \subset R$ a prime ideal. Then $R/\mathfrak{p}$ is an Artinian ring.*

Proof. R being an Artinian ring is equivalent to R being an Artinian module over itself. We can regard $\mathfrak{p}$ as a submodule of R. Then we can construct the short eaxact sequence of R-modules:

$$0 \to \mathfrak{p} \to R \to R/\mathfrak{p} \to 0$$

Then by Lemma 15.9, $R/\mathfrak{p}$ is an Artinian R-module. We can then further regard $R/\mathfrak{p}$ as an Artinian $R/\mathfrak{p}$-module, but this is again equivalent to $R/\mathfrak{p}$ being Artinian as a ring. □

Corollary 15.12. *Let R be an Aritnian ring. Then every prime ideal $\mathfrak{p}$ of R is a maximal ideal.*

Proof. Apply Lemma 15.10 to the Artinian integral domain $R/\mathfrak{p}$ (this is Artinian by the preceding Proposition) to get that $R/\mathfrak{p}$ is a field. Thus $\mathfrak{p}$ is maximal □

Corollary 15.13. *If R is an Artinian ring, then* $\operatorname{Nil}(R) = \operatorname{Jac}(R)$.

Proof. By Corollary 15.12, every prime ideal is maximal, so

$$\operatorname{Nil}(R) = \bigcap_{\mathfrak{p}\text{ prime}} \mathfrak{p} = \bigcap_{m\text{ maximal}} m = \operatorname{Jac}(R)$$

□

Corollary 15.14. *Let R be an Artinian ring. Then* $\dim(R) = 0$*.*

Proof. By Corollary 15.12, and ideal $I \subset R$ is prime if and only if it is maximal. Therefore any chain of prime ideals is of length 0, i.e. $\dim(R) = 0$. □

Recall that ACC is equivalent to the so-called *Maximal Condition*: every non-empty collection of submodules/ideals has a maximal element. Similarly, DCC is equivalent to the *Minimal Condition*: every non-empty collection of submodules/ideals has a minimal element.
The following Lemma appears in A-M Chapter 1., which we will need for the Lemma that follows it.

Lemma 15.15. *Let R be a ring and $I_1, \dots, I_n$ a finite collection of ideals. Suppose $\mathfrak{p}$ is a prime ideal such that $\mathfrak{p} \supset I_1 \cap \dots \cap I_n$. Then $\mathfrak{p} \supset I_j$ for some j.*

Proof. By contradiction assume $\mathfrak{p} \supset I_j$ for all j. Then there exists $x_j \in I_j \setminus \mathfrak{p}$ for all j. Since $\mathfrak{p}$ is prime, the product $x_1 \cdots x_n \notin \mathfrak{p}$. But we also have that

$$x_1 \cdots x_n \in I_1 \cdots I_n \subset I_1 \cap \dots \cap I_n \subset \mathfrak{p}$$

which is a contradiction. □

Lemma 15.16. *If R is an Artinian ring, then* $\operatorname{card}(\operatorname{Spec}(R)) < \infty$*.*

Proof. Let $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \dots$ be distinct prime ideals in R. Then the descending chain

$$\mathfrak{p}_1 \supset \mathfrak{p}_1\mathfrak{p}_2 \supset \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3 \supset \dots$$

satisfies the DCC. By the minimal condition, there exists an ideal I that is minimal among all finite intersections of maximal ideals in R. Thus $I = \mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_n$ for some maximal ideals $\mathfrak{p}_i$ (we know prime ideals are maximal in an Artinian ring). Let P be any prime ideal. By minimality of I,

$$(P \cap \mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_n) \supset (\mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_n)$$

implying that $P \supset I = \mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_n$.

Claim. $P \supset \mathfrak{p}_j$ for some $1 \leq j \leq n$.

PROOF OF CLAIM: Use Lemma 15.15.
The Claim, together with the fact that $\mathfrak{p}_j$ is a maximal ideal gives us that $P = \mathfrak{p}_j$. Therefore any arbitrary prime ideal is one of the $\mathfrak{p}_i$'s. Therefore

$$\operatorname{Spec}(R) = \{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}$$

which is a finite set. □

We will eventually prove that any Artinian ring is Noetherian. But for now, we do not assume that.

Theorem 15.17. *Let R be an Artinian ring. Let $N := \operatorname{Nil}(R)$ be the nilradical of R. Then N is nilpotent, i.e. $N^k = (0)$ for some k.*

Proof. By definition

$$N = \bigcap_{\mathfrak{p} \in \operatorname{Spec}(R)} \mathfrak{p} = \mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_n$$

where we know this is a finite intersection by Lemma 15.16. An equivalent definition of the nilradical gives $N = \{x \in R : x^k = 0 \text{ for some } k\} = \{\text{nilpotent elements of } R\}$ Now consider the descending chain

$$N \supset N^2 \supset N^3 \supset \dots$$

Then by DCC we must have $N^k = N^{k+1} = N^{k+2} = \dots$ for some k .Define

$$I := N^k = N^{k+1} = \dots$$

Notice in particular that any power of I is equal to itself. ....???? □

Theorem 15.18. *The R be a ring. Then the following are equivalent:*

1. *R is Artin.*
2. *R is Noetherian and* $\dim(R) = 0$*.*

Proof. (1. $\Rightarrow$ 2.): Suppose R is Artinian. We have already showed that $\dim(R) = 0$. Let $\operatorname{Spec}(R) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$. By Theorem 15.17, we have □