COMMUTATIVE ALGEBRA, FALL 2018, A. KUSTIN, CLASS NOTES

1. Expectations

1.A. **What you should expect from me.** I am thinking of the course as a first graduate course. I hope that my students have some algebraic instincts (or are willing to develop some algebraic instincts) and maybe know a few words (group, ring, field, etc.). But I am not assuming that my students are already experts in the field. So I should define most of the words I am using! I should explain most of the techniques that I am using! I should give examples! etc. If it looks like I have forgotten any of this, you can

(a) ask me for more details, definitions, and/or examples,
(b) look the missing words or topics up,
(c) keep your head down and hope the storm passes quickly (and pick up what ever you can),
(d) or some combination of the above. In particular, if you decide to "sit this one out", but then notice that I seem to keep talking about it; it is legal at that point to ask me to start again at the beginning and say everything slowly.

1.B. **What do I expect from you?** The quick answer is something.

I'd like everybody to turn in some homework and/or speak about something in a seminar or something like that.

The point is: you will get more out of the course (and enjoy the course more) if you do something, rather than just watch me.

So, what should you do? Here are some ideas: (Any of them could be written-up-exercises or seminar talks.)

(a) I picked Eisenbud's book because it is full of interesting problems. Do some of his problems.
(b) Even though I promised that I would do everything thoroughly and completely, I am sure that there will be times that you will wonder, "So, what is the rest of the story?" or "What is the right way to say all of that?" Complete the lecture.
(c) I have made the website I used in 2013-2014 available to you. There is a huge list of problems and/or projects posted there.
(d) Find an interesting paper (maybe on the arXiv, maybe in a journal) and give a lecture on it (or write up a report on it).
(e) Maybe you have already done a commutative algebra project and you want to share it with the class.
(f) Maybe you want to experiment with Macaulay and produce evidence for a theorem or conjecture.

(g) Even if our course goes for a full year, we will cover only a small percentage of Eisenbud's book. You could present (or write up) some topic that we do not do.

1.C. **Further comments.**

(a) If we run a parallel seminar, it would be great if one the students (or a collection of students) organized it. My experience is that when somebody takes charge of something, most people respond by saying "Thank you for taking charge"; rather than "How dare you take charge."
(b) If you write something up, I prefer if you type it. You should take the time to express your thoughts in sentences, spell most words correctly, express complete ideas, define your words and notation. You should write most of the details. (If you think something is true, but do not yet know how to prove it, it is much better that state the real situation than to try to fake it.)
(c) You should acknowledge your sources!
(d) It is fun to do mathematics alone. It is fun to collaborate. Work either way. If you collaborate, you should mention this fact in your report. If you collaborate, I would like everybody involved to wrote up the results. (Of course, this is not what happens when one is finished with graduate school. My thought process is that this is one of the last opportunities for anyone to influence how you write mathematics.)
(e) I recognize that there are many demands on your time.
    (i) If this is your first year in graduate school, then the most important thing is for you the Qualifying Exam.
    (ii) If you have passed your Comprehensive Exam, then the most important thing is for you to write your dissertation.

    At any rate, I hope you enjoy my class; I hope you learn a lot; but you have other things to do too; and we both know that.

I plan to post notes at my website

`http://people.math.sc.edu/kustin/teaching/746/746.html`

The first section is about Expectations (what you should expect and what I expect.) You should read that. I do not want to talk about it.

I am always in my office TuTh 2:40–3:50. Most TuTh I can stay later, but you should warn me. For other days, you should schedule a meeting time.

In some sense, we will cover "A first course" as described in the Introduction to [3].

We get to work.

2. Ring, ideal, quotient ring, prime ideal, maximal ideal, module, Noetherian

This material "is" Chapter 0 and section 1.4 of [3].

2.1.

(a) (The word "*ring*" is "defined" in section 0.1 on page 11 of [3].) When I say ring, I mean **commutative ring with one**; furthermore, **the additive identity element** ("0") **is different than the multiplicative identity element** ("1").

(b) An *ideal* I in a ring R is a subgroup of $(R,+)$ which is closed under scalar multiplication.

(c) If I is a proper ideal in the ring R, then R/I is a new ring, called a *quotient* ring. (If one likes, R/I is the set of cosets $\{r+I | r\in R\}$, where

$$r+I=r'+I \iff r-r'\in I.$$

One checks that $r+I$ times $r'+I$ equals $rr'+I$ makes sense.)

Examples 2.2.

(a) Some of my favorite rings are $\mathbb{Z}$, a field $\boldsymbol{k}$, $\mathbb{Z}[x_1,\dots,x_n]$, $\boldsymbol{k}[x_1,\dots,x_n]$.

(b) Some of my favorite ideals are:

(i) (3) in $\mathbb{Z}$,

(ii) (x^2+1) in $\mathbb{Z}[x]$,

(iii) (x^2-y^3) in $\mathbb{R}[x,y]$, and

(iv) the ideal generated by the two by two minors of the matrix $M=\begin{bmatrix} x_0 & x_1\\ x_1 & x_2\\ x_2 & x_3\end{bmatrix}$ in the ring $\mathbb{C}[x_0,x_1,x_2,x_3]$.

(c) The corresponding quotient rings are:

(i) $\mathbb{Z}/(3)$,

(ii) the "Gaussian integers" $\mathbb{Z}[x]/(x^2+1)\cong\mathbb{Z}[i]$,

(iii) the coordinate ring $\mathbb{R}[x,y]/(x^2-y^3)\cong\mathbb{R}[t^2,t^3]$ of the singular plane curve $x^2=y^3$, which is parameterized by $t\mapsto(t^3,t^2)$, and

(iv) the homogeneous coordinate ring of the twisted cubic
$$[s:t] \mapsto [s^3 : s^2t : st^2 : t^3]$$
in projective 3-space, that is,
$$\frac{\mathbb{C}[x_0, x_1, x_2, x_3]}{(x_0x_2 - x_1^2, x_0x_3 - x_1x_2, x_1x_3 - x_2^2)}.$$

Definition 2.3.

- The ideal I in the ring R is *prime* if
$$r_1r_2 \in I \implies r_1 \in I \text{ or } r_2 \in I,$$
for r_1 and r_2 in R.
- The ideal I in the ring R is *maximal* if $I \neq R$ but the only ideal of R which properly contains I is R.

Exercise 2.4. Let I be an ideal in a ring R. Fill in the blanks and prove the resulting statement.

- The ideal I is prime if and only if the ring R/I is a _____.
- The ideal I is maximal if and only if the ring R/I is a _____.
- Which property of ideals (prime or maximal) implies the other?
- Give a chain of three ideals which satisfies one of the properties, but not the other.
- What property (prime or maximal) do each of the ideals of 2.2.(b) have? Can you give a larger ideal with the other property? (To prove my answer to (civ) I would establish an isomorphism from
$$\frac{\mathbb{C}[x_0, x_1, x_2, x_3]}{(x_0x_2 - x_1^2, x_0x_3 - x_1x_2, x_1x_3 - x_2^2)}$$
to $\mathbb{C}[s^3, s^2t, st^2, t^3]$. This is a fun exercise that you can do without any machinery.)

Definition 2.5. If R is a ring and M is an Abelian group, then M is an R-module if there is a function $R \times M \to M$ (written as $(r, m) \mapsto rm$) which satisfies:

- $r(m + m') =$,
- $(r + r')m =$,
- $(rr')m =$, and
- $1m =$.

Examples 2.6.

(1) A vector space is a module over a field.
(2) An Abelian group is a $\mathbb{Z}$-module.
(3) An ideal in the ring R is an R-submodule of R.

Class on August 28, 2018

Old business: The ideal $(x^2+1,3)$ is maximal ideal in $\mathbb{Z}[x]$. Indeed,

$$\frac{\mathbb{Z}[x]}{(x^2+1,3)} = \frac{\frac{\mathbb{Z}[x]}{(3)}}{\frac{(x^2+1,3)}{(3)}} = \frac{\frac{\mathbb{Z}}{(3)}[x]}{(x^2+1)}$$

Observe that $\frac{\mathbb{Z}}{(3)}$ is a field, $\frac{\mathbb{Z}}{(3)}[x]$ is a PID, and x^2+1 is an irreducible polynomial. Thus, $\frac{\frac{\mathbb{Z}}{(3)}[x]}{(x^2+1)}$ is a field.

Resume the examples of modules.

(4) If F is an R-module, then any subgroup of $(F,+)$ which is closed under scalar multiplication is an R-module.
(5) If $N \subseteq M$ are R-modules, then M/N is an R-module. (One can think of M/N as a set of cosets (as described in 2.1.(c)). One must make sure that the induced multiplication makes sense.)
(6) My favorite R-modules are the finitely generated free R-modules:

R^n is equal to the set of column vectors with n entries from R.

Addition and scalar multiplication take place component wise.
(7) Let M and N be R-modules. A function $\phi : M \to N$ is an R*-module homomorphism* if

$$\phi(m+m') = \quad \text{and} \quad \phi(rm) =$$

for m, m' in m and $r \in R$.
(8) Every R-module homomorphism $R^m \to R^n$ is multiplication by an $n \times m$ matrix.
(9) If $\phi : M \to N$ is an R-module homomorphism, then $\ker \phi$ and $\operatorname{coker} \phi = \frac{N}{\operatorname{im} \phi}$ are R-modules.
(10) In a Noetherian ring R (see Observation 2.9 below), every finitely generated R-module is the cokernel of a matrix!
(11) If $\phi : R \to S$ is a ring homomorphism, then S and every S-module (say M) is an R-module, with rm defined to be $\phi(r)$ times m for $r \in R$ and $m \in M$.
(12) I am particularly fond of finitely generated modules because of (10). I usually figure that if one is thinking about a module which is not finitely generated that is because one is not thinking about the correct ring.

Observation 2.7. *Let M be a module over a ring R. The following two statements are equivalent.*

(a) *Every R-submodule of M is finitely generated.*
(b) *Every ascending chain of R-submodules of M stabilizes.* (*One says that the submodules of M satisfy the "Ascending Chain Condition".*)

Proof.
(a) $\implies$ (b). Let $M_1 \subseteq M_2 \subseteq \cdots$ be a chain of submodules of M. Observe that $\cup_i M_i$ is a submodule of M. Thus, $\cup_i M_i$ is finitely generated. All of the generators live in M_{i_0} for some i_0. Thus, $M_{i_0} = M_{i_0+1} = \cdots$.

(b) $\implies$ (a). Let N be a submodule of M. Pick $n_1 \in N$. If possible, pick $n_2 \in N \setminus (n_1)$. If possible, pick $n_3 \in N \setminus (n_1, n_2)$. etc. The chain $(n_1) \subsetneq (n_1, n_2) \subsetneq \cdots$ is finite. So, there exists $n_1, \cdots, n_{i_0}$ which generate N. □

Definition 2.8. If the conditions of Observation 2.7 hold for the R-module M, then M is called a *Noetherian R-module*. If the conditions of Observation 2.7 hold for the R-module R then R is called a *Noetherian ring*.

Observation 2.9. *If M is a finitely generated module over a Noetherian ring R, then M is a Noetherian R-module.*

Proof. It suffices to show that R^ℓ is Noetherian for each positive integer ℓ. (Indeed M is a quotient of R^ℓ for some ℓ. Every quotient of a Noetherian module is Noetherian. If $A \subseteq B$ are R-modules, then submodules of B/A all have the form C/A where C is a submodule of B which contains A. If B is a Noetherian module, then B/A is a Noetherian module.) Let N be a submodule of R^n. Consider the projection $\operatorname{proj} : R^\ell \to R$ which is given by

$$\operatorname{proj}\left(\begin{bmatrix} r_1 \\ \vdots \\ r_n \end{bmatrix}\right) = r_1.$$

Observe that $\operatorname{proj}(N)$ is an ideal of R; thus, $\operatorname{proj}(N)$ is finitely generated. It follows that there are elements $n_1, \ldots, n_\#$ in N so that $N = R(n_1, \ldots, n_\#) + N'$ where every element of N' has the form

$$\begin{bmatrix} 0 \\ * \\ \vdots \\ * \end{bmatrix}.$$

It follows by induction on ℓ that N' is finitely generated. Therefore, N is also finitely generated. □

Theorem 2.10. (Hilbert basis theorem) *If R is a Noetherian ring, then $R[x]$ is a Noetherian ring.*

Proof. Let J be an ideal of $R[x]$. The proof has two steps.

Step One. For each non-negative integer i, let J_i be the ideal of $R[x]$ which is generated by the elements of J of degree at most i. Prove by induction that each J_i is finitely generated. (This uses the same trick as 2.9. Suppose J_{i-1} is finitely generated. Consider the ideal in R which is generated by the leading coefficients of all polynomials of degree i in J. This ideal is finitely generated; so, we can find $f_1, \ldots, f_\#$ in J_j with $J_j = (f_1, \ldots, f_\#) + J_{j-1}$.)

Step Two.[1] Let

$$I_i = \{r \in R \mid r \text{ is the leading coefficient of a polynomial in } J \text{ of degree } i\}.$$

Notice that I_i is also equal to

$$\{r \in R \mid r \text{ is the leading coefficient of an element of } J_i\}.$$

Observe that

$$I_0 \subseteq I_1 \subseteq \cdots$$

is an ascending chain of ideals in the Noetherian ring R. So; there exists i_0 such that $I_{i_0} = I_k$, for all k with $i_0 \le k$.

Claim. $J_{i_0} = J$.

Proof of Claim.

It suffices to show that each element of J with degree bigger than i_0 is in J_{i_0}.

By induction, it suffices to show that if f is in J and $i_0 < \deg f$, then there exists $g \in J_{i_0}$ with $\deg(f - g) < \deg f$.

Let r be the leading coefficient of f. Thus, $r \in I_{\deg f} = I_{i_0}$. Thus there is an element h of J_{i_0} with $\deg h = i_0$ and the leading term of h is equal to r. Observe that

$$\deg(f - x^{\deg f - i_0} h) < \deg f.$$

This completes the proof of the claim.

The proof of the Theorem is also complete because we learned in step 1 that J_{i_0} is finitely generated. □

Examples 2.11.

(a) All of the rings of Example 2.2 are Noetherian. (The Hilbert basis theorem guarantees that if R is Noetherian, then $R[x_1, \dots, x_n]$ is Noetherian. If R is Noetherian, then the homomorphic image of R is Noetherian (because the ideals of R/I are all of the form J/I where J is an ideal of R which contains I). Maybe, I should point out also, that $\mathbb{Z}$ is Noetherian; indeed, every ideal can be generated by one element. One says $\mathbb{Z}$ is a PID (Principal Ideal Domain). If you don't know this already, then you should prove it.)

(b) The ring $\mathbb{Z}[x_1, x_2, \dots]$ is not Noetherian.

[1] This argument was repaired on August 30, 2018.

3. LOCALIZATION.

This material "comes from" Chapter 2 of [3].

Definition 3.1. A *local ring* is a ring with exactly one maximal ideal.

Examples 3.2.

(a) Every field is a local ring.
(b) The ring $\mathbb{Z}_{(2)} = \{\frac{a}{b} | a, b \in \mathbb{Z},\ b \notin (2)\}$ is a local ring. (View $\mathbb{Z}_{(2)}$ as a subring of the field of rational numbers $\mathbb{Q}$.)
(c) The ring of formal power series in one variable over a field $\boldsymbol{k}[[x]]$ is a local ring.

3.A. **Why should we study local rings?**

3.3. Many definitions are given for local rings. A local ring R is (Cohen-Macaulay, Gorenstein, regular) if xxxx. A ring R is (Cohen-Macaulay, Gorenstein, regular) if every localization of $R_\mathfrak{m}$ is (Cohen-Macaulay, Gorenstein, regular), where $\mathfrak{m}$ varies over the maximal ideals of R.

3.4. We will prove that if M is a module over a local ring, then M is zero if and only if $M_\mathfrak{m}$ is zero for all maximal ideals $\mathfrak{m}$ of R.

MANY theorems are proven in the local case. A typical theorem says $X = Y$ where X and Y are submodules of some big module.

It suffices to prove $X = X + Y$ and $Y = X + Y$.

It suffices to prove $\frac{X+Y}{X} = 0$ and $\frac{X+Y}{Y} = 0$.

It suffices to prove $(\frac{X+Y}{X})_\mathfrak{m} = 0$ and $(\frac{X+Y}{Y})_\mathfrak{m} = 0$ for all maximal ideals $\mathfrak{m}$ of R.

3.B. **Why are local rings called local?** If you give me a geometric object, say

$$V = V(y - x^2) = \{(x_0, y_0) \in \boldsymbol{k}^2 \mid y_0 = x_0^2\},$$

then I immediately think of its coordinate ring

$$\frac{\boldsymbol{k}[x,y]}{(y - x^2)}.$$

This is the ring of polynomial FUNCTIONS which are defined in V. (Recall that two functions are equal precisely if they take the same value on each element in the domain.) If you give me a point, say $P_0 = (x_0, y_0)$ on V, then I might wonder about about the geometry of V near P_0. (Is P_0 a smooth point on V? If not, how singular is P_0? etc.) To do this, I would consider the ring of rational functions which make sense <u>locally</u> near P_0. This ring is the localization

$$\left(\frac{\boldsymbol{k}[x,y]}{(y - x^2)}\right)_{(x - x_0, y - y_0)}.$$

3.C. **The definition of localization.**

Plan 3.5. Let R be a ring and U be a multiplicatively closed subset of R which does not contain 0. We make a new ring $U^{-1}R$ in which all of the elements of U are units.

There are three typical choices for U.

(a) Let P be a prime ideal of the ring R and $U = R \setminus P$. (In this case, $U^{-1}R$ is usually written R_P. I have used this notation already numerous times.)
(b) Let u be an element of R which is not nilpotent and $U = \{1, u, u^2, \dots\}$. (In this case, $U^{-1}R$ is usually written R_u.)
(c) Let U be the set of non-zero divisors of R. In this case, $U^{-1}R$ is called the *total ring of fractions* of R or the *total quotient ring*. Do notice that if R is a domain, and U is the set of non-zero divisors of R, then $U^{-1}R$ is called the *fraction field* of R. It is the same as $R_{(0)}$ (as described in (a)) and maybe maybe you already built the fraction field of a domain (or built $\mathbb{Q}$ from $\mathbb{Z}$) in a previous course. The construction in general is very similar.

Definition 3.6. Let U be a multiplicatively closed subset of the ring R which does not contain 0. The localization of R at U is the ring

$$U^{-1}R = \frac{\{\frac{r}{u} | r \in R, u \in U\}}{\frac{r}{u} = \frac{r'}{u'} \iff \exists u'' \in U \text{ such that } u''(u'r - ur') = 0}.$$

Define addition and multiplication in the obvious manner

$$\frac{r}{u} + \frac{r'}{u'} = \frac{ru' + r'u}{uu'} \quad \text{and} \quad \frac{r}{u}\frac{r'}{u'} = \frac{rr'}{uu'}$$

and verify that these operations are indeed functions! (Remember that each element of $U^{-1}R$ has many names.)

Observation 3.7. *Let U be a multiplicatively closed subset of the ring R which does not contain 0. Then there is a bijection*

$$\begin{array}{ccc} \textit{the set of ideals of } R \textit{ disjoint from } U & \leftrightarrow & \textit{the set of proper ideals of } U^{-1}R \\ I & \longrightarrow & I(U^{-1}R) \\ \{r \in R | \frac{r}{1} \in \mathscr{I}\} & \longleftarrow & \mathscr{I}. \end{array}$$

Proof. This is easy. □

Corollary 3.8. *Let U be a multiplicatively closed subset of the ring R which does not contain 0. If R is Noetherian, then $U^{-1}R$ is Noetherian.*

3.D. $\mathrm{Hom}_R(M, N)$.

Let M and N be modules over the ring R.

- Define

$$\mathrm{Hom}_R(M, N) = \{\alpha : M \to N | \ \alpha \text{ is an } R\text{-module homomorphism}\}.$$

- Observe that $\mathrm{Hom}_R(M,N)$ is an Abelian group with
$$(\alpha+\beta)(m)=\alpha(m)+\beta(m)$$
for α and β in $\mathrm{Hom}_R(M,N)$.
- Observe that $\mathrm{Hom}_R(M,N)$ is an R-module with
$$(r\alpha)(m)=r(\alpha(m))$$
for α in $\mathrm{Hom}_R(M,N)$ and $r\in R$.
- Observe that $\mathrm{Hom}_R(M,-)$ is a covariant left exact functor. In other words, if
$$0\to A\xrightarrow{\alpha}B\xrightarrow{\beta}C$$
is an exact sequence of R-modules, then
$$0\to \mathrm{Hom}_R(M,A)\xrightarrow{\alpha_*}\mathrm{Hom}_R(M,B)\xrightarrow{\beta_*}\mathrm{Hom}_R(M,C)$$
is an exact sequence of R-modules, where α_* sends
$$M\to A \quad \text{to} \quad M\to A\xrightarrow{\alpha}B.$$
- Observe that $\mathrm{Hom}_R(-,N)$ is a contravariant left exact functor. In other words, if
$$A\xrightarrow{\alpha}B\xrightarrow{\beta}C\to 0$$
is an exact sequence of R-modules, then
$$0\to \mathrm{Hom}_R(C,N)\xrightarrow{\beta^*}\mathrm{Hom}_R(B,N)\xrightarrow{\alpha^*}\mathrm{Hom}_R(A,N)$$
is an exact sequence of R-modules, where α^* sends
$$B\to N \quad \text{to} \quad A\xrightarrow{\alpha}B\to N.$$

(None of the above assertion are completely obvious; but I think they are all fairly straightforward. You should check enough to get the idea of what is being asserted.)

3.E. **Tensor product.** Let R be a ring and M and N be R-modules. One can describe $M\otimes_R N$ using generators and relations; but if one does that, then $M\otimes_R N$ seems to be an arbitrary random object. I prefer to give the property satisfied by $M\otimes_R N$; this property is called the Universal Mapping Property (UMP). Only one module can satisfy the (UMP) up to (a very special) isomorphism. One still must prove that $M\otimes_R N$ actually exists. (This is where the generators and relations are introduced.) In my mind the (UMP) is significantly more important than the generators and relations. (I remember that when I was young, I had a hard time realizing this.)

Let L, M, N be R-modules. A function $h: M\times N\to L$ is called R-bilinear if
$$h(-,n): M\to L \quad \text{and} \quad h(m,-): N\to L$$
is an R-module homomorphism for each $n\in N$ and each $m\in M$. Bilinear homomorphisms are awkward, I'd rather only think about ordinary R-module homomorphisms. It turns out that it is possible to consider only ordinary R-module homomorphisms; but the cost is that the domain becomes more complicated.

Definition 3.9. Let M and N be modules over the ring R. The tensor product of M and N is an R-module $M \otimes_R N$, together with an R-bilinear function $M \times N \xrightarrow{b} M \otimes_R N$, which satisfies the following Universal Mapping Property. If L is an R-module and $h : M \times N \to L$ is an R-bilinear function, then there exists a unique homomorphism

$$\widetilde{h} : M \otimes_R N \to L$$

such that the diagram

$$\begin{tikzcd} M \times N \arrow[r, "b"] \arrow[d, "h"'] & M \otimes_R N \arrow[dl, dashed, "\exists! \widetilde{h}"] \\ L & \end{tikzcd}$$

commutes.

The image $b(m, n)$ of (m, n) in $M \otimes_R N$ is denoted $m \otimes n$.

Observation 3.10. (Uniqueness) *If $M \times N \xrightarrow{b} M \otimes_R N$ and $M \times N \xrightarrow{b'} (M \otimes_R N)'$ both satisfy the (UMP) for tensor product, then there is a unique isomorphism $\alpha : M \otimes_R N \to (M \otimes_R N)'$ for which the diagram*

$$\begin{tikzcd} & M \times N \arrow[dl, "b"'] \arrow[dr, "b'"] & \\ M \otimes_R N \arrow[rr, "\alpha", "\cong"'] & & (M \otimes_R N)' \end{tikzcd}$$

commutes.

Proof. The (UMP) with $L = (M \otimes_R N)'$ yields a unique map α so that

$$\begin{tikzcd} M \times N \arrow[r, "b"] \arrow[d, "b'"] & M \otimes_R N \arrow[dl, dashed, "\exists! \alpha"] \\ (M \otimes_R N)' & \end{tikzcd}$$

commutes. The (UMP) with $L = M \otimes_R N$ yields a unique map β so that

$$\begin{tikzcd} & M \times N \arrow[r, "b"] \arrow[d, "b'"] \arrow[ddl, "b"'] & M \otimes_R N \arrow[dl, dashed, "\exists! \alpha"] \\ & (M \otimes_R N)' \arrow[dl, dashed, "\exists! \beta"] & \\ M \otimes_R N & & \end{tikzcd}$$

commutes. At this point $\beta \circ \alpha$ and $\mathrm{id}_{M \otimes_R N}$ both cause

$$\begin{tikzcd} M \times N \arrow[r, "b"] \arrow[d, "b"] & M \otimes_R N \arrow[dl, dashed, "\exists!"] \\ M \otimes_R N & \end{tikzcd}$$

to commute and $\alpha \circ \beta$ and $\mathrm{id}_{(M\otimes_R N)'}$ both cause

$$\begin{tikzcd} M \times N \arrow[r, "b'"] \arrow[d, "b'"] & (M \otimes_R N)' \arrow[dl, dashed, "\exists!"] \\ (M \otimes_R N)' \end{tikzcd}$$

to commute. Thus, $\beta \circ \alpha = \mathrm{id}_{M\otimes_R N}$ and $\alpha \circ \beta = \mathrm{id}_{(M\otimes_R N)'}$ and the proof is complete. $\square$

Remark. The proof that an object defined by a (UMP) is unique always goes this way. We probably will not write such a proof together again.

Observation 3.11. (Existence) *If M and N are modules over the ring R, then $M \otimes_R N$ exists.*

Proof. Let X equal the free R-module on the set $\{x_{(m,n)} \mid m \in M, \text{ and } n \in N\}$, Let Y be the R-submodule of X generated by

$$\begin{cases} \{x_{(m+m',n)} - x_{(m,n)} - x_{(m',n)} \mid m, m' \in M \text{ and } n \in N\} \\ \cup\{x_{(m,n+n')} - x_{(m,n)} - x_{(m,n')} \mid m \in M, \text{ and } n, n' \in N\} \\ \cup\{x_{(rm,n)} - r x_{(m,n)} \mid m \in M,\ n \in N, \text{ and } r \in R\} \\ \cup\{x_{(m,rn)} - r x_{(m,n)} \mid m \in M,\ n \in N, \text{ and } r \in R\}. \end{cases}$$

I claim that $M \times N \xrightarrow{b} \frac{X}{Y}$, given by $b(m,n) = \operatorname{cls} x_{(m,n)}$ satisfies the (UMP) of tensor product. Let L be an R-module and $h : M \times N \to L$ be an R-bilinear function.

- Observe first that b is an R-bilinear function of R-modules.
- Observe second that the only map $\alpha : \frac{X}{Y} \to L$ which has a chance of making

$$\begin{tikzcd} M \times N \arrow[r, "b"] \arrow[d, "h"'] & \frac{X}{Y} \arrow[dl, dashed, "\alpha"] \\ L \end{tikzcd}$$

  commute has to send $\operatorname{cls}(x_{(m,n)})$ to $h(m,n)$ for each $(m,n) \in M \times N$. Of course, X is a free R-module with basis $\{x_{(m,n)} \mid m \in M \text{ and } n \in N\}$; so $\widetilde{\alpha} : X \to L$ with $\widetilde{\alpha}(x_{(m,n)}) = h(m,n)$ is a well defined R-module homomorphism.
- Observe that $\widetilde{\alpha}(Y) = 0$. The first isomorphism theorem guarantees that $\widetilde{\alpha}$ induces $\alpha : \frac{X}{Y} \to L$ with $\alpha(\operatorname{cls}(x_{(m,n)}) = h(m,n)$.

Thus, $M \times N \xrightarrow{b} \frac{X}{Y}$ is a solution to the Universal Mapping Problem; and therefore

$$M \times N \xrightarrow{b} \frac{X}{Y}$$

is $M \times N \xrightarrow{b} M \otimes_R N$. $\square$

3.F. **Properties of tensor product.**

(a) If M is an R-module, then $R \otimes_R M = M$ and $R \times M \xrightarrow{b} R \otimes_R M$ is

$$R \times M \xrightarrow{\text{scalar multiplication}} M.$$

Proof. Observe that $R \times M \xrightarrow{\text{scalar multiplication}} M$ is an R-bilinear function. It suffices to show that $R \times M \xrightarrow{\text{scalar multiplication}} M$ is a solution of the Universal Mapping Problem. Let $h : R \times M \to L$ be an R-bilinear function. Observe that the only candidate for a homomorphism $\widetilde{h} : M \to L$ for which

(3.11.1)
$$\begin{tikzcd} R \times M \arrow[r, "\text{mult}"] \arrow[d, "h"'] & M \arrow[dl, "\widetilde{h}"] \\ L & \end{tikzcd}$$

commutes is $\widetilde{h}(m) = h(1, m)$ for $m \in M$; on the other hand, this choice does make (3.11.1) commute:

$$(\widetilde{h} \circ \text{mult})(r, m) = \widetilde{h}(rm) = h(1, rm) = rh(1, m) = h(r, m),$$

for $m \in M$ and $r \in R$. □

(b) If $f : M \to M'$ and $g : N \to N'$ are R-module homomorphisms, then there is a unique R-module homomorphism $M \otimes_R N \to M' \otimes_R N'$ which sends $m \otimes n$ to $f(m) \otimes g(n)$, for $m \in M$ and $n \in N$. (Of course, this homomorphism is called $f \otimes g$.)

Proof. Apply the (UMP) of tensor product. Observe that

$$M \times N \to M' \otimes_R N',$$

given by $(m, n) \mapsto f(m) \otimes g(n)$ is R-bilinear, for $m \in M$ and $n \in N$. □

(c) If M, N, and N' are R-modules, then

$$M \otimes_R (N \oplus N') \cong (M \otimes_R N) \oplus (M \otimes_R N').$$

Proof. Observe that

$$M \times (N \oplus N') \to (M \otimes_R N) \oplus (M \otimes_R N'),$$

with

$$(m, (n, n')) \mapsto (m \otimes n, m \otimes n')$$

is an R-bilinear function, for $m \in M$ and $n, n' \in N$. It follows that there is an R-module homomorphism

$$\phi : M \otimes_R (N \oplus N') \to (M \otimes_R N) \oplus (M \otimes_R N'),$$

with

$$\phi(m \otimes (n, n')) = (m \otimes n, m \otimes n'),$$

for $m \in M$ and $n, n' \in N$. Similarly,

$$M \times N \to M \otimes_R (N \oplus N'),$$

with

$$(m, n) \mapsto m \otimes (n, 0)$$

is an R-bilinear function, for $m \in M$ and $n \in N$; hence there is an R-module homomorphism

$$M \otimes_R N \to M \otimes_R (N \oplus N'),$$

with

$$m \otimes n \mapsto m \otimes (n, 0), \tag{3.11.2}$$

for $m \in M$ and $n \in N$. The same procedure produces an R-module homomorphism

$$M \otimes_R N' \to M \otimes_R (N \oplus N'),$$

with

$$m \otimes n' \mapsto m \otimes (0, n'), \tag{3.11.3}$$

for $m \in M$ and $n' \in N'$. Combine the legitimate R-module homomorphisms (3.11.2) and (3.11.3) to obtain a legitimate R-module homomorphism

$$\psi : (M \otimes_R N) \oplus (M \otimes_R N') \to M \otimes_R (N \oplus N'),$$

with

$$\psi(m \otimes n, m' \otimes n') = (m \otimes (n, 0)) + (m' \otimes (0, n'))$$

for all $m, m' \in M$, $n \in N$, and $n' \in N'$. In particular,

$$\psi(m \otimes n, m \otimes n') = (m \otimes (n, 0)) + (m \otimes (0, n')) = m \otimes \Big((n, 0) + (0, n')\Big) = m \otimes (n, n'),$$

for all $m \in M$, $n \in N$, and $n' \in N'$. Observe that ϕ and ψ are inverses of one another. $\square$

(d) If N is a module over the ring R, then $- \otimes_R N$ is a covariant right exact functor. In other words, if

$$A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$$

is an exact sequence of R-modules, then

$$A \otimes_R N \xrightarrow{\alpha \otimes 1} B \otimes_R N \xrightarrow{\beta \otimes 1} C \otimes_R N \to 0$$

is an exact sequence of R-modules.

Proof. I will show that $\ker(\beta \otimes 1) \subset \operatorname{im}(\alpha \otimes 1)$. The rest of the things that must be shown are fairly straightforward. Let $E = \operatorname{im}(\alpha \otimes 1)$. Observe that $E \subseteq \ker(\beta \otimes 1)$. Let $\bar{\beta}$ be the R-module homomorphism

$$\frac{B \otimes_R N}{E} \to C \otimes_R N,$$

which is induced by

$$B \otimes_R N \xrightarrow{\beta \otimes 1} C \otimes_R N.$$

We produce an inverse for $\bar{\beta}$ (and that will complete the proof). Observe that

$$C \times N \to \frac{B \otimes_R N}{E} \tag{3.11.4}$$

with $(c, n) \mapsto (b \otimes n) + E$, for some $b \in B$ with $\beta(b) = c$ is a well-defined FUNCTION, where $c \in C$ and $n \in N$ are arbitrary. (Indeed, if $b' \in B$ and $\beta(b')$ is also equal to c, then $b - b' \in \ker \beta = \operatorname{im} \alpha$ and $(b - b') \otimes n$ is in E.) Now observe that (3.11.4) is an R-bilinear function. It follows that there is an R-module homomorphism

$$\gamma : C \otimes_R N \to \frac{B \otimes_R N}{E},$$

with $\gamma(c \otimes n) = (b \otimes n) + E$, for some $b \in B$ with $\beta(b) = c$. Observe that γ and $\bar{\beta}$ are inverses of one another. □

(e) The right exactness of tensor product makes calculation possible. Indeed, if

$$R^b \xrightarrow{\phi} R^a \to M \to 0 \tag{3.11.5}$$

is an exact sequence of R-modules (where ϕ is an $a \times b$ matrix of scalars), then

$$N^b \xrightarrow{\phi} N^a \to M \otimes_R N \to 0$$

is an exact sequence of R-modules. (Of course, every finitely generated module over a Noetherian ring has a finite presentation like (3.11.5).)

(f) If M is an R-module and I is an ideal, then $\frac{R}{I} \otimes_R M \cong \frac{M}{IM}$.

Proof. Apply $- \otimes_R M$ to the exact sequence

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

to obtain the exact sequence

$$I \otimes_R M \to \underbrace{R \otimes_R M}_{M} \to R/I \otimes_R M \to 0$$

and the image of $I \otimes_R M$ in $R \otimes_R M = M$ is IM. □

(g) Let $\psi : R \to S$ be a ring homomorphism.

Every S-module is already an R module.

On the other hand, if M is an R-module, then $S \otimes_R M$ is the S-module that corresponds to M. (One says that $S \otimes_R M$ is obtained from M by *extension of scalars*).

In particular, if M is an R-module with finite presentation (3.11.5), then $S \otimes_R M$ is the S-module with presentation:

$$S^b \xrightarrow{\psi(\phi)} S^a \to S \otimes_R M \to 0.$$

If the entry in ϕ in row r and column c is $\phi_{r,c}$, then the entry in $\psi(\phi)$ in row r and column c is $\psi(\phi_{r,c})$.

(h) I want to point out that $-\otimes_R N$ is NOT always an exact functor. Let I and J be ideals of the ring R. Apply $-\otimes_R R/J$ to the exact sequence

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

to obtain the exact sequence

$$\underbrace{I \otimes_R (R/J)}_{I/IJ} \to \underbrace{R \otimes_R (R/J)}_{R/J} \to \underbrace{(R/I) \otimes_R (R/J)}_{\frac{R/I}{J(R/I)}=R/(I+J)} \to 0,$$

which we re-write as the exact sequence

$$\frac{I}{IJ} \to \frac{R}{J} \to \frac{R}{I+J} \to 0.$$

(Each map is the natural map $\operatorname{cls}\theta \mapsto \operatorname{cls}\theta$.) The kernel of the left-hand map is $\frac{I\cap J}{IJ}$. This module is often not zero. In particular, if $I = J$, then I/I^2 is usually not zero.

3.G. **Localization produces flat modules!**

Definition 3.12. Let R be a ring and M be an R-module. If $M \otimes_R -$ is an exact functor, then M is a *flat* R-module. (An exact functor carries short exact sequences to short exact sequences.)

Examples 3.13.

(a) Every free R-module is flat. (It is clear that R is flat. We proved that direct sum commutes with tensor product. Actually, we proved that finite direct sum commutes with tensor product; however, it is true that all direct sums commute with tensor product.)

(b) Every projective R-module is flat. (At this point, an R-module P is *projective* if P is a direct summand of a free R-module. Later, we will learn other equivalent characterizations of projective modules.) The proof that every projective R-module is flat is straightforward: Use the fact that if P is a projective module, then there is a module Q such that $P \oplus Q$ is free (hence flat) combined with the fact that direct sum commutes with tensor product.

Here are a few projective modules.

(i) If R is the ring $\frac{\mathbb{Z}}{(6)}$, then R is the internal direct sum of $I_1 \oplus I_2$, for $I_1 = (2)R$ and $I_2 = (3)R$. In other words, $I_1 + I_2 = R$ and $I_1 \cap I_2 = (0)$. The R-modules I_1 and I_2 are flat but not free. (Finitely generated free R-modules have a multiple of 6 elements.)

(ii) Here is a more interesting projective module which is probably not free. Let S be the polynomial ring $\boldsymbol{k}[x,y,z]$ localized at the element $u = x^2 + y^2 + z^2$. That is $S = \boldsymbol{k}[x,y,z]_u$, where $\boldsymbol{k}$ is an arbitrary field. Consider the S-module homomorphisms

$$S \xrightarrow{i=\begin{bmatrix} x \\ y \\ z \end{bmatrix}} S^3 \xrightarrow{\pi=\begin{bmatrix} x & y & z \end{bmatrix}} S.$$

Observe that the composition $\pi \circ i$ is multiplication by a unit. It follows that $S^3 = \operatorname{im} i \oplus \ker \pi$ as an internal direct sum. Thus, $\operatorname{im} i$ and $\ker \pi$ are both projective S-modules. It is clear that $\operatorname{im} i$ is a free S-module (isomorphic to S). I am fairly certain that $\ker \pi$ is not a free S-module, but I do not have a proof. See, for example, [3, Example 19.8] where a topological argument is offered to prove that a module similar to $\ker \pi$ is not free.

(iii) Every ideal in a Dedekind domain D is a projective D-module, but not all of these ideals are free. One large family of Dedekind Domains comes from Algebraic Number Theory. Let K be a field which is a finite dimensional vector space over $\mathbb{Q}$ (such fields are called algebraic number fields) and let D be the set of all elements of K which satisfy a monic polynomial with integer coefficients. This set D forms a ring, called the ring of algebraic integers in K. Furthermore, D is a Dedekind domain. One example of a Dedekind domain is $D = \mathbb{Z}[\sqrt{-5}]$. In D, there are two factorizations of 6 into irreducible factors:

$$2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

This lack of unique factorization into irreducibles gives rise to the ideal

$$(2, 1 + \sqrt{-5})D,$$

which is a projective D-module that is not free. (In order to be free, the ideal would have to be principal.)

The purpose of this subsection is to prove Proposition 3.16 which states that if R is a ring and U is a multiplicatively closed subset of R which does not contain 0, then $U^{-1}R$ is a flat R-module.

First we make sense of the localization of a module $U^{-1}M$ with out making any reference to tensor product. Then we prove $U^{-1}R \otimes_R M = U^{-1}M$. Then we prove $U^{-1}R$ is a flat R-module.

Definition-Observation 3.14. Let R be a ring, U be a multiplicatively closed subset of R which does not contain 0, and M be an R-module. Define the set

$$U^{-1}M = \frac{\{\frac{m}{u} | m \in M, u \in U\}}{\frac{m}{u} = \frac{m'}{u'} \iff \exists u'' \in U \text{ such that } u''(u'm - um') = 0}.$$

Define addition and scalar multiplication by $U^{-1}R$ in the obvious manner:

$$\frac{m}{u} + \frac{m'}{u'} = \frac{mu' + m'u}{uu'} \quad \text{and} \quad \frac{r}{u}\frac{m}{u'} = \frac{rm}{uu'}$$

and verify that these operations are indeed functions! (Remember that each element of $U^{-1}R$ and each element of $U^{-1}M$ has many names.)

Lemma 3.15. *Let R be a ring, U be a multiplicatively closed subset of R which does not contain 0, and M be an R-module. Then multiplication*

$$U^{-1}R \otimes_R M \to U^{-1}M$$

is an isomorphism of $U^{-1}R$-modules.

Proof. Observe that multiplication

$$U^{-1}R \times M \to U^{-1}M$$

is an R-bilinear function. Thus,

$$\text{mult} : U^{-1}R \otimes_R M \to U^{-1}M \tag{3.15.1}$$

is also a legitimate R-module homomorphism. One easily sees that (3.15.1) is also a legitimate $U^{-1}R$-module homomorphism.

Now we define an inverse

$$\alpha : U^{-1}M \to U^{-1}R \otimes_R M$$

to (3.15.1). If $m \in M$ and $u \in U$, then we hope to send $\frac{m}{u}$ to $\frac{1}{u} \otimes m$. Suppose $\frac{m}{u} = \frac{m'}{u'}$ in $U^{-1}M$, for some $u' \in U$ and $m' \in M$. Then there exists $u'' \in U$ with $u''u'm = u''um'$ in M. It follows that

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

in $U^{-1}R \otimes_R M$. The must recent equation is the same as

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

in $U^{-1}R \otimes_R M$ because elements of R are allowed to slide over the tensor product symbol. Thus, $\alpha(\frac{m}{u}) = \frac{1}{u} \otimes m$ is a legitimate function. It is not hard to check that α is a $U^{-1}R$-module homomorphism and is the inverse of (3.15.1). ☐

Proposition 3.16. *If R is a ring and U is a multiplicatively closed subset of R which does not contain 0, then $U^{-1}R$ is a flat R-module.*

Proof. It suffices to prove that if $\alpha : N \to M$ is an injective R-module homomorphism, then $1 \otimes \alpha : U^{-1}R \otimes_R N \to U^{-1}R \otimes_R M$ is an injective $U^{-1}R$-module homomorphism. It suffices to show that if $N \subseteq M$, then $U^{-1}N \subseteq U^{-1}M$. This is obvious. If $n \in N$ and $u \in U$ with $\frac{n}{u} = 0$ in $U^{-1}M$, then there exists $u' \in U$ with $u'n = 0$ in M. It follows that $u'n = 0$ in N and $\frac{n}{u} = 0$ in $U^{-1}N$. ☐

Observation 3.17. *If M is a finitely generated R-module, then $M_P \neq 0$ if and only if* $\operatorname{ann} M \subseteq P$.

Proof. Suppose $M_P = 0$. The module M is finitely generated; say by $m_1, \dots, m_N$ for some integer N. For each m_i, there is an element $u_i \in R \setminus P$ with $u_i m_i = 0$ in M. Observe that $\prod_{i=1}^{N} u_i \in \operatorname{ann} M \setminus P$.

Suppose $u \in \operatorname{ann} M \setminus P$. Then u is a unit in R_P and $uM_P = 0$. Thus $M_P = 0$. ☐

Observation 3.18. *If M is an R-module then*

$$M = 0 \iff M_{\mathfrak{m}} = 0 \textit{ for all maximal ideals } \mathfrak{m} \textit{ of } R.$$

Proof. One direction is obvious. We prove $(\Leftarrow)$. Suppose $M_{\mathfrak{m}} = 0$ for all maximal ideals $\mathfrak{m}$ of R. Let $m \in M$. It follows (say from the flatness of localization) that $(m)_{\mathfrak{m}} = 0$ for all $\mathfrak{m}$. Apply Observation 3.17 to say that $\operatorname{ann}(m)$ is not contained in any maximal ideal of R. Thus, $\operatorname{ann}(m) = R$ and $m = 0$. Thus, every element of M is zero; hence, $M = 0$. $\square$

Proposition 3.19. *Let R be a ring, S be a flat R-algebra, and M and N be R-modules with M finitely presented. Then*

$$S \otimes_R \operatorname{Hom}_R(M, N) \cong \operatorname{Hom}_S(S \otimes_R M, S \otimes_R N).$$

Corollary 3.20. *Let R be a Noetherian ring, U be a multiplicatively closed subset of R not containing 0, and M and N be R-modules with M finitely generated. Then*

$$U^{-1} \operatorname{Hom}_R(M, N) \cong \operatorname{Hom}_{U^{-1}R}(U^{-1}M, U^{-1}N).$$

Proof of Proposition 3.19. Apply $\operatorname{Hom}_R(-, N)$ followed by $S \otimes_R -$ to the exact sequence

$$R^b \xrightarrow{\phi} R^a \to M \to 0 \tag{3.20.1}$$

to obtain the exact sequences

$$0 \to \operatorname{Hom}_R(M, N) \to \operatorname{Hom}_R(R^a, N) \xrightarrow{\phi^*} \operatorname{Hom}_R(R^b, N)$$

and

$$0 \to S \otimes_R \operatorname{Hom}_R(M, N) \to \underbrace{S \otimes_R \operatorname{Hom}_R(R^a, N) \xrightarrow{S \otimes_R \phi^*} S \otimes_R \operatorname{Hom}_R(R^b, N)}_{(S \otimes_R N)^a \xrightarrow{\psi(\phi^{\mathrm{T}})} (S \otimes_R N)^b}. \tag{3.20.2}$$

Apply $S \otimes_R -$ followed by $\operatorname{Hom}_S(-, S \otimes_R N)$ to the exact sequence (3.20.1) to obtain the exact sequences

$$S \otimes_R R^b \to S \otimes_R R^a \xrightarrow{S \otimes \phi} S \otimes_R M \to 0$$

and

(3.20.3)

$$0 \to \operatorname{Hom}_S(S \otimes_R M, S \otimes_R N) \to \underbrace{\operatorname{Hom}_S(S \otimes_R R^a, S \otimes_R N) \xrightarrow{(S \otimes \phi)^*} \operatorname{Hom}_S(S \otimes_R R^b, S \otimes_R N)}_{(S \otimes_R N)^a \xrightarrow{\psi(\phi^{\mathrm{T}})} (S \otimes_R N)^b}$$

Compare (3.20.2) and (3.20.3). There is a natural homomorphism

$$S \otimes_R \operatorname{Hom}_R(M, N) \to \operatorname{Hom}_S(S \otimes_R M, S \otimes_R N),$$

which sends $s \otimes \phi$ to $s \otimes \phi$. Observe that

$$\begin{tikzcd}
0 \arrow[r] & S \otimes_R \operatorname{Hom}_R(M, N) \arrow[r] \arrow[d] & (S \otimes_R N)^a \arrow[r, "\psi(\phi^{\mathrm{T}})"] \arrow[d, "\cong"] & (S \otimes_R N)^b \arrow[d, "\cong"] \\
0 \arrow[r] & \operatorname{Hom}_S(S \otimes_R M, S \otimes_R N) \arrow[r] & (S \otimes_R N)^a \arrow[r, "\psi(\phi^{\mathrm{T}})"] & (S \otimes_R N)^b
\end{tikzcd}$$

is a commuting diagram with exact rows. This is enough to guarantee that the left most map is an isomorphism. (There is probably a fancy way to say this. It is also easy to check the assertion by hand.) □

3.H. **Ideals which are maximal with respect to any plausible property are prime.**

Observation 3.21. *Let U be a multiplicatively closed subset of the ring R. If I is an ideal of R which is maximal among the ideals of R which are disjoint from U, then I is a prime ideal of R.*

Proof. This proof is by contradiction. Suppose I is not a prime ideal of R. Then there exist a and b in $R \setminus I$ with $ab \in I$. The ideals (I, a) and (I, b) meet U; so there exist i_1, i_2 in I and r_1, r_2 in R with $X = i_1 + r_1 a$ and $Y = i_2 + r_2 b$ in U. Observe that $XY \in I \cap U$, which is a contradiction. □

The next result is very important in the unit on Primary Decomposition, Section 4.

Observation 3.22. *Let R be a ring and M be an R-module. Consider the following set of ideals*

$$\mathscr{S} = \{\operatorname{ann}(m) \mid m \in M \setminus \{0\}\}.$$

If I is a maximal element of $\mathscr{S}$, then I is a prime ideal of R.

Proof. The ideal I is equal to $\operatorname{ann} m$ for some non-zero element m of M. Suppose that a, b are in R with $ab \in I$ and $a \notin I$. We prove $b \in I$.

The hypothesis that $a \in I = \operatorname{ann} m$ ensures that $am \neq 0$. On the other hand,

$$I = \operatorname{ann}(m) \subseteq \operatorname{ann}(am),$$

with $\operatorname{ann}(am) \in \mathscr{S}$, and I is a maximal element of $\mathscr{S}$. It follows that $I = \operatorname{ann}(am)$. The hypotheses $ab \in I = \operatorname{ann}(m)$, ensures $b \in \operatorname{ann}(am) = I$ and the proof is complete. □

3.I. **Rings and modules of finite length.**

3.23. Why do we care?

(a) Rings of finite length are precisely the rings of Krull dimension zero. The main goal of this course is to understand Krull dimension. The best place to start is Krull dimension zero.

(b) One reason to study Commutative Algebra is that it provides a precise way to measure geometric phenomenon; like, for example, intersection multiplicity. (Draw some secant lines converging to a tangent line at a smooth point. Play the "same game" at a singular point.) This precise measure is almost always given by the length of some module.

Definition 3.24. An R-module N is *simple* if the only submodules of N are N and (0).

Example 3.25. If $\mathfrak{m}$ is a maximal ideal in the ring R then $R/\mathfrak{m}$ is a simple R-module.

Definition 3.26. The R-module M has *finite length* if there exists a finite chain of submodules of M of the form:

$$M = M_0 \supsetneq M_1 \supsetneq M_2 \supsetneq \cdots \supsetneq M_n = 0, \tag{3.26.1}$$

for some non-negative integer n, such that M_i/M_{i+1} is a simple R-module for $0 \le i \le n-1$. In this case, the chain of modules (3.26.1) is called a *composition series* of M. The length of (3.26.1) is n (the number of inclusions) and the *length of* M, denoted $\ell(M)$, is the length of the shortest composition series of M.

Proposition 3.27. [3, 2.13] *If M is an R-module of finite length, then every composition series has the same length.*

Proof. The argument has two steps.

Step 1. If N is a proper submodule of M, then $\ell(N) < \ell(M)$. Let

$$M = M_0 \supsetneq M_1 \supsetneq M_2 \supsetneq \cdots \supsetneq M_n = 0,$$

be a composition series for M with $n = \ell(M)$. Intersect this chain with N to obtain

$$N = (M \cap N) = (M_0 \cap N) \supseteq (M_1 \cap N) \supseteq (M_2 \cap N) \supseteq \cdots \supseteq (M_n \cap N) = 0. \tag{3.27.1}$$

Use the isomorphism theorem

$$\frac{A+B}{B} \cong \frac{A}{A \cap B}$$

to see

$$\frac{M_i}{M_{i+1}} \supseteq \frac{(M_i \cap N) + M_{i+1}}{M_{i+1}} = \frac{A+B}{B} \cong \frac{A}{A \cap B} = \frac{M_i \cap N}{(M_i \cap N) \cap M_{i+1}} = \frac{M_i \cap N}{M_{i+1} \cap N}.$$

The i^{th} factor in (3.27.1) is either (0) or naturally isomorphic to $\frac{M_i}{M_{i+1}}$.

Claim. Some factor must be (0).

Proof of this claim. Otherwise, by induction one proves that $N = M$. Indeed, if

$$\frac{M_{n-1} \cap N}{M_n \cap N} = \frac{M_{n-1}}{M_n},$$

then $M_{n-1} \cap N = M_{n-1}$; hence $M_{n-1} \subseteq N$. If $\frac{M_{n-2} \cap N}{M_{n-1} \cap N}$ is also equal to $\frac{M_{n-2}}{M_{n-1}}$, then

$$M_{n-2} \cap N = M_{n-2}$$

Proceed in this manner to see that $M \subseteq N$. □

At this point one deletes enough terms from (3.27.1) to remove the zero factors. One obtains a composition series for N which has length less than $\ell(M)$. Hence,

$$\ell(N) \le \text{ the length of this composition series } < \ell(M).$$

Step 2. Let

$$M = N_0 \supsetneq N_1 \supsetneq N_2 \supsetneq \cdots \supsetneq N_k$$

be a chain of submodules of M. We prove (by induction on $\ell(M)$) that $k \le \ell(M)$.

If $\ell(M) = 0$, then $M = 0$; hence $k = 0$.

If $1 \le \ell(M)$, then $k-1 \le \ell(N_1)$ by induction and $\ell(N_1) \le \ell(M)-1$ by Step 1; hence $k \le \ell(M)$. $\square$

Definition 3.28. The ring R is *Artinian* if every descending chain of ideals of R stabilizes. That is, if

$$I_0 \supseteq I_1 \supseteq I_2 \supseteq I_3 \supseteq \cdots$$

are ideals of R, the there exists i_0 such that $I_{i_0} = I_{i_0+k}$ for all positive integers k. (One says that the ideals of R satisfy the *Descending Chain Condition* (DCC).)

Examples 3.29.

(a) The ring $\mathbb{Z}/(n)$ is Artinian for any integer n with $2 \le n$.
(b) Any ring which contains a field $\boldsymbol{k}$ and is finite dimensional as a vector space over $\boldsymbol{k}$ is Artinian.
(c) The rings $\mathbb{Z}$ and $\boldsymbol{k}[x]$ are not Artinian.

Thursday, October 4. Last time we thought about the following issues:

(1) A module M has finite length if it has a composition series:
$$M = M_0 \supsetneq M_1 \supsetneq M_2 \supsetneq \cdots \supsetneq M_n = 0,$$
with M_i/M_{i+1} a simple module for each i.
(2) If M has finite length then every composition series for M has the same length.
(3) If M has one composition series, then there is an absolute bound on the length of strictly descending chains of submodules of M, namely $\ell(M)$. (This was step two of the proof that every composition series has the same length.) This last remark deserves further discussion. It says that if M has finite length, then the submodules of M satisfy the descending chain condition! It also says that, if M has finite length, then the submodules of M satisfy the ascending chain condition!

Observation 3.30. *Let R be a ring and*

$$0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$$

be a short exact sequence of R-modules. Then

(a) *B has finite length if and only if A and C have finite length, and*
(b) *if B has finite length, then*
$$\ell(B) = \ell(A) + \ell(C).$$

One says that "length is additive on short exact sequences."

Proof. It suffices to prove the result when $A \subseteq B$ and $C = B/A$ because A is isomorphic to the image of α and C is isomorphic to $B/\operatorname{im}\alpha$. In this case, we consider

$$B \supseteq A \supseteq (0).$$

(a) If A and B/A have finite length, then they have composition series. Paste these composition series together to get a composition series for B. Conclude that B has finite length.

If B has finite length, then we proved (in Step 2 of Proposition 3.27) that every strictly descending chain of submodules of B has length at most $\ell(B)$; hence A and B/A have finite length.

Finally, one composition series for B is obtained by pasting together a composition series for A and a composition series for B/A. All composition series for B have the same length. It follows that $\ell(B) = \ell(A) + \ell(B/A)$. □

Theorem 3.31. [3, 2.14] *The following statements about the ring R are equivalent*:

(a) *R is Noetherian and all prime ideals of R are maximal ideals;*
(b) *R has finite length as an R-module; and*
(c) *R is Artinian.*

Remark. The Krull dimension of a ring R is the longest length of a chain

$$P_0 \subsetneq P_1 \subsetneq P_2 \subsetneq \cdots \subsetneq P_d$$

of prime ideals in R. Consequently Theorem 3.31 also gives that if R is a Noetherian ring, then R has finite length if and only if R has Krull dimension zero.

Proof.
$(a) \implies (b)$ We prove that if R is Noetherian but not of finite length, then there exists some prime ideal of R which is not a maximal ideal.

Consider the set of ideals I of R such that R/I does not have finite length. This set is non-empty because it contains the zero ideal. The ring R is Noetherian, so we select a maximal element I of this set. Suppose $a \notin I$. The ideal (I, a) is strictly larger than I; so, $R/(I, a)$ has finite length. Consider the short exact sequence

$$0 \to R/(I : a) \xrightarrow{a} \underbrace{R/I}_{\text{not finite length}} \to \underbrace{R/(I,a)}_{\text{finite length}} \to 0.$$

Length is additive on short exact sequences. It follows that $R/(I : a)$ does not have finite length. But $I \subseteq (I : a)$ forces $I = (I : a)$. Hence I is prime. The ideal I is not maximal because fields have finite length.

$(b) \implies (c)$ This is clear.

$(c) \implies (a)$ The main intermediate result is

3.31.1. If R is Artinian, then 0 is the product of a finite collection of maximal ideals of R.

Assume (3.31.1) for now and finish the proof. Let $0 = \mathfrak{M}_1 \cdots \mathfrak{M}_n$, with each $\mathfrak{M}_i$ a maximal ideal of R (repetitions are allowed). Consider the descending chain of submodules (i.e., ideals):

$$R \supseteq \mathfrak{M}_1 \supseteq \mathfrak{M}_1\mathfrak{M}_2 \supseteq \cdots \supseteq \mathfrak{M}_1 \cdots \mathfrak{M}_n.$$

The factor

$$\frac{\mathfrak{M}_1 \cdots \mathfrak{M}_{s-1}}{\mathfrak{M}_1 \cdots \mathfrak{M}_{s-1}\mathfrak{M}_s} \tag{3.31.2}$$

is a vector space over $R/\mathfrak{M}_s$. The ring R is Artinian and subspaces of (3.31.2) correspond to ideals of R; hence, the vector space (3.31.2) is finite dimensional. Thus, this vector space has a composition series; and therefore, R has composition series. Thus, R has finite length. (It follows that R is Noetherian. We proved in 3.27, Step 2, that if $\ell(R) < \infty$, then $\ell(R)$ is an absolute bound on the length of strictly descending chains of submodules (i.e., ideals) of R. No strictly ascending chain of ideals can have length exceeding this absolute bound either; because one can turn an ascending chain of ideals into a descending chain of ideals.)

If P is a prime ideal of R, then

$$\mathfrak{M}_1 \cdots \mathfrak{M}_n = 0 \subseteq P;$$

hence $\mathfrak{M}_i \subseteq P$ for some i and $P = \mathfrak{M}_i$, which is a maximal ideal of R.

• Now we prove 3.31.1.

Let J be minimal among the set of ideals in R which are equal to a product of maximal ideals of R. We prove $J = 0$. Suppose $J \neq 0$.

Well J^2 is also a product of maximal ideals and $J^2 \subseteq J$. It follows that $J^2 = J$.

Let I be minimal among all ideals of R which do not annihilate J. Observe that

$$0 \neq IJ = IJ^2;$$

so IJ does not annihilate J and $IJ \subseteq I$. It follows that $IJ = I$.

There must be an element $f \in I$ with $fJ \neq 0$. Again $(f) \subseteq I$; (f) has a property; and I is minimal among the ideals with this property. Thus, $(f) = I$.

Observe that $(f)J = (f)$. Thus, there is an element $g \in J$ with $fg = f$. In other words, $f(1-g) = 0$. The element g is in every maximal ideal of R (because if $\mathfrak{M}$ is a maximal ideal of R, then $J\mathfrak{M}$ is a product of maximal ideals and $J\mathfrak{M} \subseteq J$; hence $J\mathfrak{M} = J$ and in particular, $\mathfrak{M} \supseteq J$.) At any rate, $1-g$ is not in any maximal ideal of R; that is $1-g$ is a unit of R. Thus, $f = 0$, which is a contradiction. □

Remark 3.32. One consequence of the proof of Theorem 3.31 is that Artinian rings only have a finite number of maximal ideals. (If $\mathfrak{M}$ is a maximal ideal of R, then $\mathfrak{M}_1 \cdots \mathfrak{M}_n = (0) \subseteq \mathfrak{M}$; hence, $\mathfrak{M} = \mathfrak{M}_i$ for some i.)

Proposition 3.33. [3, 2.16] *Every Artinian ring is the direct product of local Artinian rings.*

Proof.

Key idea. If R is an Artinian ring and $\mathfrak{M}$ and $\mathfrak{M}'$ are maximal ideals of R, then

$$(R_{\mathfrak{M}})_{\mathfrak{M}'} = \begin{cases} R_{\mathfrak{M}}, & \text{if } \mathfrak{M} = \mathfrak{M}', \text{ and} \\ 0 & \text{if } \mathfrak{M} \neq \mathfrak{M}'. \end{cases}$$

Assume the Key idea for the time being. Finish the proof.

Let R be an Artinian ring. Recall from Remark 3.32 that R only has a finite number of maximal ideals $\mathfrak{M}_1, \dots, \mathfrak{M}_n$. Let

$$\alpha : R \to \bigoplus_i R_{\mathfrak{M}_i}$$

send 1 to $(1, \dots, 1)$. Let C be the cokernel of α and K be the kernel of α. So

$$0 \to K \to R \xrightarrow{\alpha} \bigoplus_i R_{\mathfrak{M}_i} \to K \to 0$$

is an exact sequence of R-modules. The Key idea tells us that

$$\alpha_{\mathfrak{M}} : R_{\mathfrak{M}} \to (\bigoplus_i R_{\mathfrak{M}_i})_{\mathfrak{M}} = R_{\mathfrak{M}}$$

is an isomorphism for each maximal ideal $\mathfrak{M}$ of R. Localization is exact; thus, $K_{\mathfrak{M}} = 0$ and $C_{\mathfrak{M}} = 0$ for each maximal ideal $\mathfrak{M}$ of R. Recall from Observation 3.18 that if a module is locally zero, then the module is zero. Thus, α is an isomorphism.

• Proof of the Key idea.

It is clear that $(R_{\mathfrak{M}})_{\mathfrak{M}} = R_{\mathfrak{M}}$. We focus on $(R_{\mathfrak{M}})_{\mathfrak{M}'}$ with $\mathfrak{M} \neq \mathfrak{M}'$. We show that if $\mathfrak{M}$ is a maximal ideal of the Artinian ring R, then $R_{\mathfrak{M}}$ is also Artinian and each factor in a composition series for $R_{\mathfrak{M}}$ is $R/\mathfrak{M}$. This is enough because $(R/\mathfrak{M})_{\mathfrak{M}'} = 0$ since some element of $\mathfrak{M}$ is not in $\mathfrak{M}'$. (This element acts like a unit on $(R/\mathfrak{M})_{\mathfrak{M}'}$ and also annihilates $(R/\mathfrak{M})_{\mathfrak{M}'}$.)

The ring R is Artinian; so R has a composition series

$$R = I_0 \supsetneq I_1 \supsetneq I_2 \supsetneq \cdots \supsetneq I_n = 0;$$

and each factor is $R/\mathfrak{M}_i$ for some maximal ideal $\mathfrak{M}_i$ of R. Now localize:

$$R_{\mathfrak{M}} = (I_0)_{\mathfrak{M}} \supseteq (I_1)_{\mathfrak{M}} \supseteq (I_2)_{\mathfrak{M}} \supseteq \cdots \supseteq (I_n)_{\mathfrak{M}} = 0.$$

(Keep in mind that localization is flat!) The only non-zero factors are $(R/\mathfrak{M})_{\mathfrak{M}} = R/\mathfrak{M}$. □

Proposition 3.34. [3, 2.17] *Let M be a finitely generated module over the Noetherian ring R. The following statements are equivalent*:

(a) *M has finite length, and*

(b) *$R/\operatorname{ann} M$ is an Artinian ring.*

Proof.

(b) $\Longrightarrow$ (a) The ring $R/\operatorname{ann} M$ is Artinian. Thus, $R/\operatorname{ann} M$ has finite length as a module over $R/\operatorname{ann} M$ and also as a module over R. Thus,

$$\bigoplus_{\text{finite}} R/\operatorname{ann} M$$

has finite length as a module over $R/\operatorname{ann} M$ and also as a module over R. Thus, any quotient of

$$\bigoplus_{\text{finite}} R/\operatorname{ann} M$$

(in particular, say M) has finite length as a module over $R/\operatorname{ann} M$ and also as a module over R.

(a) $\Longrightarrow$ (b) The R-module M has finite length; so

$$M = M_0 \supseteq M_1 \supseteq \cdots \supseteq M_n = (0)$$

and $M_i/M_{i+1} \cong R/\mathfrak{M}_i$ for some maximal ideal $\mathfrak{M}_i$ of R. Thus

$$\begin{aligned}
&\mathfrak{M}_0 M \subseteq M_1 \\
&\mathfrak{M}_1\mathfrak{M}_0 M \subseteq M_2 \\
&\quad\vdots \\
&\mathfrak{M}_{n-1}\cdots\mathfrak{M}_1\mathfrak{M}_0 M \subseteq M_n = (0).
\end{aligned}$$

Thus, a finite product of maximal ideals annihilates M. Let P be a prime ideal of R which contains $\operatorname{ann} M$. Then

$$\mathfrak{M}_{n-1}\cdots\mathfrak{M}_1\mathfrak{M}_0 \subseteq \operatorname{ann} M \subseteq P.$$

It follows that some $\mathfrak{M}_i$ is contained in P; indeed, some $\mathfrak{M}_i$ is equal to P. The ring $R/\operatorname{ann} M$ is Noetherian and has the property that every prime ideal is maximal. It follows from Theorem 3.31 that R is Artinian. $\square$

4. Primary Decomposition

Primary Decomposition is Emmy Noether's main contribution to Commutative Algebra. There was some form of Primary Decomposition which worked for rings of algebraic integers and which was proved using ad hoc number theory techniques; and there was some form for rings from geometry which was proved using geometric techniques. Noether realized that both forms of the theorem could be established with one proof based on the Ascending Chain Condition.

The main way I use primary decomposition is in the following result. Everybody who took the syzygies course saw that we used this result very often.

Theorem 4.1. *Let R be a Noetherian ring, I be an ideal of R, and M be a non-zero finitely generated R-module. If every element of I is a zero-divisor on M, then there exists a non-zero element $m \in M$ with $Im = 0$.*

There are two steps to the proof. One proves that the set of zero divisors on M is equal to the union of a finite set of primes ideals and each of these prime ideals is equal to the annihilator of some element of non-zero element of M. (This is the main result about Primary Decomposition.) One also proves the Prime Avoidance Lemma.

Lemma 4.2. (The Prime Avoidance Lemma) *Let $I_1, \dots, I_n, J$ be ideals in the ring R with $J \subseteq \bigcup\limits_{i=1}^{n} I_i$. If R contains an infinite field or if at most two of the I_j are not prime, then $J \subseteq I_i$, for some i.*

Proof.
Case 1. Suppose R contains an infinite field $\boldsymbol{k}$. Each of the ideals J, $J \cap I_1$, ... ,$J \cap I_n$ is a vector space over $\boldsymbol{k}$ and $J = \bigcup\limits_{i=1}^{n} (J \cap I_i)$. A vector space over an infinite field can not be the union of a finite collection of proper subspaces[2]; hence $J \cap I_{i_0} = J$ for some i_0; therefore, $J \subseteq I_{i_0}$.

Case 2. By induction on n, we may assume that J is not contained in the union of any proper subset of $\{I_1, \dots, I_n\}$. Label the ideals so that if $3 \le n$, then I_n is prime. For each i_0, select $f_{i_0} \in J \setminus \bigcup\limits_{i \neq i_0} I_i$. It follows that $f_{i_0} \in I_{i_0}$. Consider the element

$$\theta = f_1 \cdots f_{n-1} + f_n \in J.$$

[2]Let V be a vector space over the infinite field $\boldsymbol{k}$. We use contradiction to show that V is not the union of any finite collection of proper subspaces. Assume $V_1, \dots, V_n$ are proper subspaces of V and V is the union $V = \bigcup\limits_{i=1}^{n} V_1$. If such an example exists, we take the smallest such example. For i equals 1 and 2, take $v_i \in V_i$, with v_i not in any of the other V_j. (The element v_1 exists because of the minimality of our example. In particular V_1 is not the union of $V_1 \cap V_2$, $V_1 \cap V_3, \dots, V_1 \cap V_n$. The element v_2 exists because of an analogous explanation.) As α roams over $\boldsymbol{k}$ there are infinitely many choices for $v_1 + \alpha v_2 \in V = \bigcup\limits_{i=1}^{N} V_1$. Two of these choices must be in the same V_k, for some k. If $v_1 + \alpha v_2$ and $v_1 + \beta v_2$ are in V_k for some $\alpha \neq \beta \in \boldsymbol{k}$ and some index k, then v_1 and v_2 are both in V_k, which is not possible.

Observe that $\theta \notin I_j$, for $j < n$, because $f_n \notin I_j$. Observe that $\theta \notin I_n$. Indeed, if $n = 2$, then $\theta = f_1 + f_2$ and $f_1 \notin I_2$ and if $3 \le n$, then I_n is prime and $f_1 \cdots f_{n-1} \notin I_n$. $\square$

Primary Decomposition works for finitely generated modules over Noetherian rings.

Definition 4.3. Let M be a non-zero finitely generated module over the Noetherian ring R.

(a) If $\mathfrak{p}$ is a prime ideal of R and $\mathfrak{p} = \operatorname{ann} m$ for some non-zero $m \in M$, then $\mathfrak{p}$ is an *associated prime* of M.
(b) The set of associated primes of M is denoted $\operatorname{Ass} M$.
(c) The submodule N of M is called a primary submodule of M if $\operatorname{Ass} \frac{M}{N}$ has exactly one element. If $\operatorname{Ass} \frac{M}{N} = \{\mathfrak{p}\}$, then N is called $\mathfrak{p}$-primary.

Theorem 4.4. *Let M be a non-zero finitely generated module over the Noetherian ring R.*

(a) *The set $\operatorname{Ass} M$ is finite.*
(b) *The set of zero divisors on M is equal to $\bigcup\limits_{\mathfrak{p} \in \operatorname{Ass} M} \mathfrak{p}$.*
(c) *If $\mathfrak{p}$ a prime ideal of R which is minimal in the support of M (In other words $\operatorname{ann} M \subseteq \mathfrak{p}$ and there aren't any prime ideals of R which sit properly between $\operatorname{ann} M$ and $\mathfrak{p}$.), then $\mathfrak{p} \in \operatorname{Ass} M$.*
(d) *If N is a submodule of M and $\operatorname{Ass} \frac{M}{N} = \{\mathfrak{p}_1, \dots, \mathfrak{p}_\ell\}$ then $N = N_1 \cap \cdots \cap N_\ell$, where N_i is $\mathfrak{p}_i$-primary. Furthermore, if $\mathfrak{p}_i$ is minimal in $\operatorname{Supp} \frac{M}{N}$, then N_i is uniquely determined.*

Remark. However, in (d) if $\mathfrak{p}_i$ is not minimal in $\operatorname{Supp} \frac{M}{N}$, then N_i is NOT uniquely determined. In this case, N_i is an "embedded component" of N.

Example 4.5. Let I be the ideal $(x)(x,y)$ in $R = \mathbb{Q}[x,y]$. Then $\operatorname{Ass} R/I = \{(x),(x,y)\}$, $\operatorname{ann} \bar{x} = (x,y)$, $\operatorname{ann} \bar{y} = (x)$. Two primary decompositions of I in R are $(x) \cap (x^2, y) = I$ and $(x) \cap (x^2, xy, y^2) = I$.

Here is a little Macaulay2 session that I made on September 30, 2018 (and updated on October 17, 2018) which verifies all of these claims:

```
kustin@comath-Kustin03:~$ M2
Macaulay2, version 1.12
with packages: ConwayPolynomials, Elimination, IntegralClosure, InverseSystems, LLLBases
               PrimaryDecomposition, ReesAlgebra, TangentCone


i1 : R=QQ[x,y]


o1 = R


o1 : PolynomialRing


i2 : I=ideal(x^2,x*y)
```

```
             2
o2 = ideal (x , x*y)

o2 : Ideal of R

i3 : associatedPrimes(I)

o3 = {ideal x, ideal (y, x)}

o3 : List

i4 : I:x

o4 = ideal (y, x)

o4 : Ideal of R

i5 : I:y

o5 = ideal x

o5 : Ideal of R

i7 : associatedPrimes ideal(x)

o7 = {ideal x}

o7 : List

i8 : associatedPrimes ideal(x^2,y)

o8 = {ideal (y, x)}

o8 : List

i9 : associatedPrimes ideal(x^2,x*y,y^2)

o9 = {ideal (y, x)}

o9 : List
```

```
i10 : intersect(ideal(x),ideal(x^2,y))==I

o10 = true

i11 : intersect(ideal(x),ideal(x^2,x*y,y^2))==I

o11 = true
```

There are links to the Macaulay2 website given on the course homepage.

The class on Tuesday, October 23, 2018:

Today R is a Noetherian ring and M is a non-zero finitely generated R-module. Recall that $\mathfrak{p}$ is an associated prime of M means that $\mathfrak{p}$ is a prime ideal of R and $\mathfrak{p} = \operatorname{ann}_R m$ for some $m \in M$. We want to prove

(1) $\operatorname{Ass}_R(M)$ is finite,
(2) the set of zero divisors on M is equal to
$$\bigcup_{\mathfrak{p}\in\operatorname{Ass}_R(M)} \mathfrak{p},$$
(3) if $\mathfrak{p}$ is minimal in the support of M, then $\mathfrak{p} \in \operatorname{Ass}_R M$,
(4) if N is a submodule of M and $\operatorname{Ass}_R(\frac{M}{N}) = \{\mathfrak{p}_1, \cdots, \mathfrak{p}_n\}$, then $\exists$ submodules $N_1, \dots, N_n$ of M with $N = N_1 \cap \cdots \cap N_n$ and $\operatorname{Ass}_R(M/N_i) = \{\mathfrak{p}_i\}$. Furthermore, if $\mathfrak{p}_i$ is minimal in $\operatorname{Supp} M$, then N_i is uniquely determined.

Last time, we looked at an example. My argument was, Macaulay can do this instantly. As I thought about it, I realized, I would not be satisfied with that argument; so lets give a real argument. The point being that a real argument might be grubby, but it isn't hard.

Let $R = \frac{\boldsymbol{k}[x,y]}{(x^2,xy)}$, $M = R$, and $N = 0$. We want to work out all of the assertions of Noether's Primary Decomposition Theorem for this example.

Of course, 0 in R is a zero-divisor on M and $(0) = \operatorname{ann}_M 1$. There is no need to think about $0 \in R$ further.

Let $r = \alpha_0 + \alpha_1 x + yf(y)$ be a non-zero element of R and $m = \beta_0 + \beta_1 x + yg(y)$ be a non-zero element of M, where $\alpha_0, \alpha_1, \beta_0, \beta_1 \in \boldsymbol{k}$ and $f(y), g(y) \in \boldsymbol{k}[y]$, with
$$rm = 0.$$
Thus,
$$0 = \alpha_0\beta_0 + x(\alpha_0\beta_1 + \alpha_1\beta_0) + y\big(\alpha_0 g(y) + \beta_0 f(y) + f(y)g(y)\big) \text{ in } M.$$
Thus,
$$\begin{cases} 0 = \alpha_0\beta_0 \text{ and} \\ 0 = \alpha_0\beta_1 + \alpha_1\beta_0 \text{ and} \\ 0 = \alpha_0 g(y) + \beta_0 f(y) + f(y)g(y) \end{cases} \quad \text{in } \boldsymbol{k}[y].$$

Thus,

$$\begin{cases} 0=\alpha_0 \text{ and} \\ 0=\alpha_1\beta_0 \text{ and} \\ 0=f(y)\big(\beta_0+g(y)\big) \end{cases} \quad \text{or} \quad \begin{cases} 0=\beta_0 \text{ and} \\ 0=\alpha_0\beta_1 \text{ and} \\ 0=g(y)\big(\alpha_0+f(y)\big) \end{cases} \quad \text{in } \boldsymbol{k}[y].$$

Thus,

$$\begin{cases} 0=\alpha_0=\alpha_1 \text{ and} \\ 0\neq f(y) \text{ and} \\ 0=\beta_0=g(y) \text{ and} \\ \beta_1\neq 0 \end{cases} \quad \text{or} \quad \begin{cases} 0=\alpha_0=\beta_0 \text{ and} \\ 0=f(y)g(y) \end{cases} \quad \text{or} \quad \begin{cases} 0=\beta_0=\beta_1 \text{ and} \\ 0\neq g(y) \text{ and} \\ 0=\alpha_0=g(y) \text{ and} \\ \alpha_1\neq 0 \end{cases} \quad \text{or} \quad \begin{cases} 0=\beta_0=\alpha_0 \text{ and} \\ 0=g(y)f(y) \end{cases} \quad \text{in } \boldsymbol{k}[y].$$

The last situation is a duplicate. The second situation splits into two cases: Thus,

$$\begin{cases} 0=\alpha_0=\alpha_1 \text{ and} \\ 0\neq f(y) \text{ and} \\ 0=\beta_0=g(y) \text{ and} \\ \beta_1\neq 0 \end{cases} \quad \text{or} \quad \begin{cases} 0=\alpha_0=\beta_0 \text{ and} \\ 0=f(y) \text{ and} \\ \alpha_1\neq 0 \end{cases} \quad \text{or} \quad \begin{cases} 0=\alpha_0=\beta_0 \text{ and} \\ 0=g(y) \text{ and} \\ \beta_1\neq 0 \end{cases} \quad \text{or} \quad \begin{cases} 0=\beta_0=\beta_1 \text{ and} \\ 0\neq g(y) \text{ and} \\ 0=\alpha_0=g(y) \text{ and} \\ \alpha_1\neq 0 \end{cases} \quad \text{in } \boldsymbol{k}[y].$$

We conclude that if r is a non-zero element of R and m is a non-zero element of M with $rm=0$, then either

$$r=yf(y) \text{ and } m=\beta_1 x,$$

or

$$r=\alpha_1 x \text{ and } m=\beta_1 x+yg(y),$$

or

$$r=\alpha_1 x+yf(y) \text{ and } m=\beta_1 x,$$

or

$$r=\alpha_1 x \text{ and } m=yg(y).$$

Line 1 is a special case of line 3 and line 4 is a special case of line 2. If r is a non-zero element of R and m is a non-zero element of M with $rm=0$, then either

$$r=\alpha_1 x \text{ and } m=\beta_1 x+yg(y)$$

or

$$r=\alpha_1 x+yf(y) \text{ and } m=\beta_1 x.$$

Thus,

$$\{\operatorname{ann}_R(m)\mid m\in M \text{ with } m\neq 0\}=\{\operatorname{ann}_R(1)=(0),\operatorname{ann}_R(x)=(x,y),\operatorname{ann}_R(y)=(x)\}.$$

We conclude

(a) $\operatorname{Ass}_R M=\{(x),(x,y)\}$,
(b) the set of zero divisors on M is equal to

$$(x,y)=\bigcup_{\mathfrak{p}\in\operatorname{Ass}_R M}\mathfrak{p},$$

and
(c) (x), which is the only prime ideal of R which is minimal in $\operatorname{Supp} M$, is in $\operatorname{Ass}_R M$.

Notice that (x) is an (x)-primary submodule of M because $\frac{M}{(x)}$ is $\frac{\boldsymbol{k}[x,y]}{(x)}$ and

$$\operatorname{Ass}_R \tfrac{\boldsymbol{k}[x,y]}{(x)} = \{\operatorname{ann}_R(1) = (x)R\}.$$

Notice that (x^2, y) and (x^2, xy, y^2) are (x, y)-primary submodules of M. Indeed,

$$\frac{M}{(x^2, y)} = \frac{\boldsymbol{k}[x, y]}{(x^2, y)},$$

$$\frac{M}{(x^2, xy, y^2)} = \frac{\boldsymbol{k}[x, y]}{(x^2, xy, y^2)},$$

the only prime ideal of R in the support of $\frac{\boldsymbol{k}[x,y]}{(x^2,y)}$ is $(x, y)R$, and the only prime ideal of R in the support of $\frac{\boldsymbol{k}[x,y]}{(x^2,xy,y^2)}$ is $(x, y)R$. It follows that

$$\operatorname{Ass}_R \frac{\boldsymbol{k}[x, y]}{(x^2, y)} = \{(x, y)R\}$$

and

$$\operatorname{Ass}_R \frac{\boldsymbol{k}[x, y]}{(x^2, xy, y^2)} = \{(x, y)R\}.$$

We use the fact that $\boldsymbol{k}[x, y]$ is a UFD to see that

$$(x)R \cap (x^2, y)R = (0)R$$

and

$$(x)R \cap (x^2, xy, y^2)R = (0)R.$$

In each case $\supseteq$ is obvious. In the top situation, if

$$xf = x^2g + yh + \text{some element of } (x^2, xy)\boldsymbol{k}[x, y],$$

for f, g, h in $\boldsymbol{k}[x, y]$, then x divides h and xf is zero in R. Similarly, if

$$xf = x^2g + xyh + y^2\ell + \text{some element of } (x^2, xy)\boldsymbol{k}[x, y],$$

for f, g, h, ℓ in $\boldsymbol{k}[x, y]$, then x divides ℓ and xf is zero in R.

Example 4.6. Let R be a Noetherian domain. What is the primary decomposition of the submodule (0) of the module $M = R$?

The answer is that (0) is (0)-primary and $(0) = (0)$.

Example 4.7. Let $R = \mathbb{Z}$ and n be a positive integer. What is the primary decomposition of the submodule (n) of the module $M = R$?

Write $n = p_1^{e_1} \cdots p_n^{e_n}$ where the p_i are distinct positive prime integers. Observe that $(p_i^{e_i})$ is a (p_i)-primary submodule of $\mathbb{Z}$. (In other words, $\operatorname{Ass}_{\mathbb{Z}}(\frac{\mathbb{Z}}{(p_i^{e_i})} = \{(p_i)\}$.) Observe $(n) = \cap_i(p_i^{e_i})$ is the desired primary decomposition.

Example 4.8. Let $R = \mathbb{Q}[b,c,d,e]$ and I be the ideal generated by the 2×2 minors of the matrix

$$\begin{bmatrix} 0 & b & d \\ b & c & e \end{bmatrix}.$$

In other words,

$$I = (b^2, bd, be - dc).$$

Then $\operatorname{Ass} R/I = \{(d,b), (c,b)\}$, $(d,b) = \operatorname{ann} \bar{b}$, $(c,b) = \operatorname{ann}(\bar{d}^2)$,

$$I = (I, d^2) \cap (b,c),$$

(b,c) is (b,c)-primary, and (I,d^2) is (b,d)-primary. Here is a little Macaulay2 session that I made in 2013 which verifies all of these claims:

```
kustin@kustin-Latitude-E6520:~$ M2
Macaulay2, version 1.4
with packages: ConwayPolynomials, Elimination, IntegralClosure, LLLBases, PrimaryDecompo

i1 : R=QQ[b,c,d,e]

o1 = R

o1 : PolynomialRing

i2 : M=matrix{{0,b,d},{b,c,e}}

o2 = | 0 b d |
     | b c e |

             2       3
o2 : Matrix R  <--- R

i3 : I=minors(2,M)

              2
o3 = ideal (-b , -b*d, - c*d + b*e)

o3 : Ideal of R

i4 : associatedPrimes(I)

o4 = {ideal (c, b), ideal (d, b)}

o4 : List
```

```
i6 : I:ideal(b)

o6 = ideal (d, b)

o6 : Ideal of R

i7 : I:ideal(d^2)

o7 = ideal (c, b)

o7 : Ideal of R

i8 : intersect(ideal (I,d^2),ideal(b,c))

                                 2
o8 = ideal (c*d - b*e, b*d, b )

o8 : Ideal of R

i9 : o8==I

o9 = true

i10 : primaryDecomposition(I)

                                 2                     2
o10 = {ideal (c, b), ideal (d , c*d - b*e, b*d, b )}

o10 : List

i11 :
```

Proposition 4.9. *Let M be a non-zero finitely generated module over a Noetherian ring R. Then*

$$\textit{the set of zero divisors on } M = \bigcup_{\mathfrak{p} \in \operatorname{Ass} M} \mathfrak{p}.$$

Remark. Recall that the element r of the ring R is a zero-divisor on M if there exists an non-zero element $m \in M$ with $rm = 0$.

Proof.

$\supseteq$ This inclusion is obvious.

$\subseteq$ If r is a zero divisor on M, then $rm_0 = 0$ for some non-zero element m_0 of M. Thus, $r \in \operatorname{ann} m_0$. Consider the set of ideals

$$\mathscr{S} = \{\operatorname{ann}(m) \mid m \in M \setminus \{0\}\}$$

of R. The ideal $\operatorname{ann} m_0$ is in $\mathscr{S}$. The ring R is Noetherian, so there exists a maximal element $\operatorname{ann} m_1$ of $\mathscr{S}$ which contains $\operatorname{ann} m_0$. Recall from Observation 3.21 that $\operatorname{ann} m_1$ is a prime ideal of R and hence an associated prime of M. □

Remark. One consequence of Proposition 4.9 is that if M is a non-zero finitely generated module over a Noetherian ring R, then $\operatorname{Ass}_R M$ is not empty. Indeed, there is a non-zero element $m \in M$. Thus the set $\mathscr{S}$ is not empty. Now, just continue with the proof of Proposition 4.9

Proposition 4.10. *Let M be a non-zero finitely generated module over a Noetherian ring R. Then*

$$\mathfrak{p} \in \operatorname{Ass}_R M \iff \mathfrak{p}R_\mathfrak{p} \in \operatorname{Ass}_{R_\mathfrak{p}} M_\mathfrak{p}.$$

Proof.
($\Rightarrow$) Assume $\mathfrak{p} = \operatorname{ann}_R(m)$, for some $m \in M$. We show that $\mathfrak{p}R_\mathfrak{p} = \operatorname{ann}_{R_\mathfrak{p}}(m)$. If $\frac{r}{s}m = 0$ in $M_\mathfrak{p}$ (for some $r \in R$ and $s \in R \setminus \mathfrak{p}$), then there exists $s' \in R \setminus \mathfrak{p}$ with $s'rm = 0$ in M; hence, $s'r \in \mathfrak{p}$ and $r \in \mathfrak{p}$.
($\Leftarrow$) Assume $\mathfrak{p}R_\mathfrak{p} = \operatorname{ann}_{R_\mathfrak{p}}(\frac{m}{s})$ for some $\frac{m}{s} \in M_\mathfrak{p}$. (In particular, $m \in M$ and $s \in R \setminus \mathfrak{p}$.) We show that $\mathfrak{p} = \operatorname{ann}_R(m)$. If $r \in R$ and $rm = 0$ in R, then $r\frac{m}{s} = 0$ in $M_\mathfrak{p}$ so $r \in \mathfrak{p}R_\mathfrak{p}$. In other words, there exists $s' \in R \setminus \mathfrak{p}$ with $s'r \in \mathfrak{p}$ in R. It follows that $s'r \in \mathfrak{p}$ in R; hence $r \in \mathfrak{p}$. □

Proposition 4.11. *Let R be a Noetherian ring and*

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

be a short exact sequence of finitely generated R-modules. Then

$$\operatorname{Ass}_R M \subseteq \operatorname{Ass}_R M' \cup \operatorname{Ass}_R M''.$$

Proof. It suffices to prove the result when $M' \subseteq M$ and $M'' = M/M'$. Notice that if $\mathfrak{p} = \operatorname{ann}_R m$ for some $m \in M$ and $r \in R$, then either $r \in \mathfrak{p}$ and $rm = 0$ or $r \notin \mathfrak{p}$ and $\operatorname{ann}_R(rm) = \mathfrak{p}$.

Let $\mathfrak{p} \in \operatorname{Ass}_R M$. In particular, there is an element $m \in M$ with $\operatorname{ann}_R m = \mathfrak{p}$. There are two possibilities. Either $Rm \cap M' \neq 0$ or $Rm \cap M' = 0$. If $Rm \cap M' \neq 0$, then there is an element $r \in R$ with $rm \neq 0$ and $rm \in M'$. In this case, $\operatorname{ann}_R rm = \mathfrak{p}$ and $rm \in M'$; hence $\mathfrak{p} \in \operatorname{Ass}_R M'$. If $Rm \cap M' = 0$, then $\bar{m}$ is a non-zero element of M/M'. If $r\bar{m} = 0$ in M/M', then $rm \in RM \cap M' = 0$; hence $r \in \operatorname{ann}_R M = \mathfrak{p}$. (Of course, $\mathfrak{p}\bar{m} = 0$ in M/M'.) In this case, $\operatorname{ann}_R \bar{m} = \mathfrak{p}$ and $\mathfrak{p} \in \operatorname{Ass}_R M/M'$. □

Proposition 4.12. *If M is a non-zero finitely generated module over a Noetherian ring, then $\operatorname{Ass}_R M$ is finite.*

Proof. We exhibit an ascending chain of submodules of M
$$(0) = M_0 \subsetneq M_1 \subset M_2 \subsetneq M_3 \subsetneq \cdots$$
with $M_i/M_{i-1} \cong R/\mathfrak{p}_i$ for some prime ideal $\mathfrak{p}_i$ of R. Of course, this chain is finite because M is a Noetherian R-module and Proposition 4.11 guarantees that $\operatorname{Ass}_R M \subseteq \{\mathfrak{p}_1, \cdots\}$. To find M_1, we use the fact that $M \neq 0 \implies \operatorname{Ass}_R M \neq \emptyset$. Once we have chosen M_1, if $M_1 \neq M$, then $M/M_1 \neq 0 \implies \operatorname{Ass}_R M/M_1 \neq \emptyset$; hence there exists a submodule M_2 of M with $M_1 \subseteq M_2$ and $M_2/M_1 \cong R/\mathfrak{p}_2$. Repeat as necessary. □

Observation 4.13. *If M is a non-zero finitely generated module over a Noetherian ring R, then $\operatorname{Ass}_R M \subseteq \operatorname{Supp} M$.*

Proof. The module M is non-zero; so $\operatorname{Ass}_R M$ is non-empty and there is a non-zero element $m \in M$ with $\operatorname{ann}_R(m) = \mathfrak{p}$ for some prime ideal $\mathfrak{p}$. Observe that $(Rm)_\mathfrak{p}$ is not zero. But localization is flat, so $(m) \subseteq M \implies (m)_\mathfrak{p} \subseteq M_\mathfrak{p}$; hence $M_\mathfrak{p} \neq 0$ and $\mathfrak{p} \in \operatorname{Supp} M$. □

Proposition 4.14. *Let M be a non-zero finitely generated module over a Noetherian ring R and let $\mathfrak{p}$ be a prime ideal of R. If $\mathfrak{p}$ is minimal in $\operatorname{Supp} M$, then $\mathfrak{p} \in \operatorname{Supp} M$.*

Proof. The hypothesis that $\mathfrak{p}$ is minimal in $\operatorname{Supp} M$ guarantees that $M_\mathfrak{p} \neq 0$ and
$$\operatorname{Supp} M_\mathfrak{p} = \{\mathfrak{p}R_\mathfrak{p}\};$$
hence,
$$\emptyset \neq \operatorname{Ass}_{R_\mathfrak{p}} M_\mathfrak{p} \subseteq \operatorname{Supp} M_\mathfrak{p} = \{\mathfrak{p}R_\mathfrak{p}\}.$$
It follows that $\operatorname{Ass}_{R_\mathfrak{p}} M_\mathfrak{p} = \{\mathfrak{p}R_\mathfrak{p}\}$. Apply Proposition 4.10 to see that
$$\mathfrak{p}R_\mathfrak{p} \in \operatorname{Ass}_{R_\mathfrak{p}} \implies \mathfrak{p} \in \operatorname{Ass}_R M.$$
□

At this point we have established all of Noether's Theorem except the last assertion.

The last assertion in Noether's Theorem. Let R be a Noetherian ring and M be a non-zero finitely generated R-module. If N is a submodule of M and $\operatorname{Ass}_R(\frac{M}{N}) = \{\mathfrak{p}_1, \cdots, \mathfrak{p}_n\}$, then $\exists$ submodules $N_1, \dots, N_n$ of M with $N = N_1 \cap \cdots \cap N_n$ and N_i is an $\mathfrak{p}_i$-primary submodule of M. Furthermore, if $\mathfrak{p}_i$ is minimal in $\operatorname{Supp} M$, then N_i is uniquely determined.

It does no harm to prove this result for $N = 0$. (One merely is replacing the old M with M/N.)

There are a handful of steps.

(a) If I is an ideal in a ring R, then the radical of I is
$$\sqrt{I} = \{r \in R \mid r^n \in I \text{ for some } n\}.$$
It turns out that
$$\sqrt{I} = \bigcap_{\substack{I \subseteq \mathfrak{p} \\ \mathfrak{p} \text{ a prime ideal of } R}} \mathfrak{p}.$$

(b) If M is a module with exactly one associated prime $\mathfrak{p}$, then $\mathfrak{p}^n M = 0$ for some n.
(c) Define the notion of irreducible submodule.
(d) Prove that every submodule is a finite intersection of irreducible submodules.
(e) If N_1 and N_2 are $\mathfrak{p}$-primary submodules of M, then $N_1 \cap N_2$ is a $\mathfrak{p}$-primary submodule of M.
(f) Every irreducible submodule of M is a primary submodule of M.
(g) Let M be a non-zero finitely generated module over a Noetherian ring R and N be a submodule of M. Suppose $N_1, \dots, N_r$ are submodules of M with
   - $N = N_1 \cap \cdots \cap N_r$,
   - the intersection is irredundant in the sense that $N_1 \cap \cdots \cap \widehat{N_i} \cap \cdots \cap N_r \neq N$ for any i,
   - N_i is a $\mathfrak{p}_i$-primary submodule of M for each i (in the sense that $\operatorname{Ass}_R \frac{M}{N_i} = \{\mathfrak{p}_i\}$), and
   - the primes $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ are distinct.

   Then $\operatorname{Ass} M/N = \{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}$.
(h) Let M be a non-zero finitely generated module over a Noetherian ring R and N be a submodule of M. Suppose $N_1, \dots, N_r$ are submodules of M with
   - $N = N_1 \cap \cdots \cap N_r$,
   - the intersection is irredundant in the sense that $N_1 \cap \cdots \cap \widehat{N_i} \cap \cdots \cap N_r \neq N$ for any i,
   - N_i is a $\mathfrak{p}_i$-primary submodule of M for each i (in the sense that $\operatorname{Ass}_R \frac{M}{N_i} = \{\mathfrak{p}_i\}$), and
   - the primes $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ are distinct.

   If $\mathfrak{p}_i$ is minimal in the support of M/N, for some i, then
$$N_i = \ker\big(M \to (M/N)_{\mathfrak{p}_i}\big).$$

Proof of (a). We prove that
$$\sqrt{I} = \bigcap_{I \subseteq \mathfrak{p}} \mathfrak{p}.$$
If $a^n \in I$, then $a^n \in \mathfrak{p}$ for all prime ideals $\mathfrak{p}$ which contain I; hence $a \in \mathfrak{p}$ and
$$a \in \bigcap_{I \subseteq \mathfrak{p}} \mathfrak{p}.$$
If $a^n \notin I$, for any n, then consider the set of ideals which contain I but are disjoint from $\{1, a, a^2, \cdots\}$. This set of ideals is non-empty (because it contains I) and has a maximal element J (for us because R is Noetherian, but in general one can use a Zorn's Lemma argument at this point). This maximal element is a prime ideal (by a slight modification of Observation 3.21). We have found a prime ideal which contains I but does not contain a. It follows that
$$a \notin \bigcap_{I \subseteq \mathfrak{p}} \mathfrak{p}.$$

Proof of (b). We prove that if M is a module with exactly one associated prime $\mathfrak{p}$, then $\mathfrak{p}^n M = 0$ for some n. (As always, M is a non-zero finitely generated module over a Noetherian ring.)

Key thought. Every element of $R \setminus \mathfrak{p}$ is regular on M; so it suffices to prove that $(\mathfrak{p}^n M)_{\mathfrak{p}}$ is zero.

(The element r of the ring R is <u>regular</u> on the R-module M if $rm = 0$ implies $m = 0$ for $m \in M$. Every element of R is either a zero-divisor on M or is regular on M.)

The ring $(\frac{R}{\operatorname{ann} M})_{\mathfrak{p}}$ has exactly one prime ideal, namely $\mathfrak{p}R_{\mathfrak{p}}$. (If $\operatorname{Ass}_R M = \{\mathfrak{p}\}$, then $\mathfrak{p}$ is minimal in the support of M. On the other hand, the only prime ideals that live in $\text{Ring}_{\mathfrak{p}}$ are the prime ideals of Ring that are contained in $\mathfrak{p}$.) Apply (a) (or our work with Artinian rings and modules; see especially, Proposition 3.34 and Theorem 3.31) to see that

$$\sqrt{(\operatorname{ann} M)R_{\mathfrak{p}}} = \mathfrak{p}R_{\mathfrak{p}}.$$

The ideal $\mathfrak{p}$ is finitely generated, so $\mathfrak{p}^n R_{\mathfrak{p}} \subseteq (\operatorname{ann} M)R_{\mathfrak{p}}$ for some n. Therefore, $\mathfrak{p}^n M_{\mathfrak{p}} = 0$ and hence $\mathfrak{p}^n M = 0$ (by the key thought).

(c). The submodule N of the module M is called <u>irreducible</u> if whenever N_1 and N_2 are submodules of M with $N = N_2 \cap N_2$, then either $N_1 = N$ or $N_2 = N$.

(d). Let M be a non-zero finitely generated module over the Noetherian ring R. Then every submodule of M is a finite intersection of irreducible submodules of M.

Proof. Let $\mathscr{S}$ be the set of submodules of M which are not the finite intersection of irreducible submodules of M. If $\mathscr{S}$ is non-empty, then $\mathscr{S}$ has a maximal element N because R is Noetherian. This submodule N is reducible. Hence $N = N_1 \cap N_2$, for submodules N_1 and N_2 with $N \subsetneq N_1$ and $N \subsetneq N_2$. Neither N_1 nor N_2 can be in $\mathscr{S}$. So N_1 and N_2 both are the finite intersection of irreducible submodules of M and so is $N = N_1 \cap N_2$. This is a contradiction; hence $\mathscr{S}$ must be empty and every submodule of M is a finite intersection of irreducible submodules of M. $\square$

(e). If N_1 and N_2 are $\mathfrak{p}$-primary submodules of M, then $N_1 \cap N_2$ is a $\mathfrak{p}$-primary submodule of M. (As always, M is a non-zero finitely generated module over a Noetherian ring.)

Proof. Consider the homomorphism

$$M \to \frac{M}{N_1} \oplus \frac{M}{N_2}.$$

Obtain an injection

$$\frac{M}{N_1 \cap N_2} \to \frac{M}{N_1} \oplus \frac{M}{N_2}.$$

Notice that $\operatorname{Ass}_R(\frac{M}{N_1} \oplus \frac{M}{N_2}) = \{\mathfrak{p}\}$. If this statement isn't immediately obvious, then apply Proposition 4.11 to the short exact sequence

$$0 \to \frac{M}{N_1} \to \frac{M}{N_1} \oplus \frac{M}{N_2} \to \frac{M}{N_2} \to 0.$$

□

(f). If M is a non-zero finitely generated module over a Noetherian ring R, then every irreducible submodule of M is a primary submodule of M.

Proof. It suffices to prove the result for the submodule (0) of M. (If you want to prove the result for the submodule N of M, then study the submodule (0) of M/N.) We prove that if $\mathfrak{p}_1 \neq \mathfrak{p}_2$ are in $\operatorname{Ass}_R \frac{M}{(0)}$, then (0) is a reducible submodule of M. Pick m_i in M with $\operatorname{ann}_R m_i = \mathfrak{p}_i$. Notice that

$$Rm_1 \cap Rm_2 = (0).$$

Indeed, if m is a nonzero element of the left side then

$$\mathfrak{p}_1 = \operatorname{ann}_R m = \mathfrak{p}_2,$$

and this is a contradiction. □

(g). Let M be a non-zero finitely generated module over a Noetherian ring R and N be a submodule of M. Suppose $N_1, \dots, N_r$ are submodules of M with

- $N = N_1 \cap \dots \cap N_r$,
- the intersection is irredundant in the sense that $N_1 \cap \dots \cap \widehat{N_i} \cap \dots \cap N_r \neq N$ for any i,
- N_i is a $\mathfrak{p}_i$-primary submodule of M for each i (in the sense that $\operatorname{Ass}_R \frac{M}{N_i} = \{\mathfrak{p}_i\}$), and
- the primes $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ are distinct.

Then $\operatorname{Ass} M/N = \{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}$.

Proof. It suffices to prove the result for the submodule (0) of M. (If you want to prove the result for the submodule N of M, then study the submodule (0) of M/N.)

Consider the homomorphism

(4.14.1) $$M \to \frac{M}{N_1} \oplus \dots \oplus \frac{M}{N_r}.$$

The kernel is $N_1 \cap \dots \cap N_r = (0)$; so (4.14.1) is an injection and

$$\operatorname{Ass}_R M \subseteq \operatorname{Ass}_R(\tfrac{M}{N_1} \oplus \dots \oplus \tfrac{M}{N_r}) = \{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}.$$

We prove $\mathfrak{p}_1 \in \operatorname{Ass}_R M$. Take

$$x \in N_2 \cap \dots \cap N_r,$$

with $x \neq 0$. Observe that

(4.14.2) $$\operatorname{ann}_R x = N_1 :_R x \subseteq (\text{the set of zero divisors of } \tfrac{M}{N_1}) = \mathfrak{p}_1.$$

Recall from (b) that there is a positive integer n with $\mathfrak{p}_1^n M \subseteq N_1$. Identify the number λ with

(4.14.3) $$\mathfrak{p}_1^{\lambda} x \neq 0 \quad \text{but} \quad \mathfrak{p}_1^{\lambda+1} x = 0.$$

Take a non-zero element $y \in \mathfrak{p}_1^{\lambda} x$. Observe that $\operatorname{ann}_R y = \mathfrak{p}_1$. Indeed, (4.14.2) (with x replaced by y) shows $\operatorname{ann}_R y \subseteq \mathfrak{p}_1$ and (4.14.3) shows $\mathfrak{p}_1 \subseteq \operatorname{ann}_R y$. Thus, $\mathfrak{p}_1 \in \operatorname{Ass}_R M$. The same argument works for each of the $\mathfrak{p}_i$. □

The lecture for November 1, 2018.

Opening Remark. Last time we proved that if (M/N_1 is a non-zero finitely generated module over a Noetherian ring and) $\operatorname{Ass}(M/N_1) = \{\mathfrak{p}\}$, then there exists a non-negative integer t with $\mathfrak{p}^t M \subseteq N_1$. One consequence of this is that if $\mathfrak{q} \in \operatorname{Supp}(M/N_1)$, then $\mathfrak{p} \subseteq \mathfrak{q}$ (because $\mathfrak{p}^n \subseteq \operatorname{ann} M/N_1 \subseteq \mathfrak{q}$).

Claim 4.15. *Let M be a finitely generated non-zero module over the Noetherian ring R and N be a submodule of M. Suppose that $\mathfrak{p}_1$ is a prime ideal of R which is minimal in the support of M/N. Then the $\mathfrak{p}_1$-primary component of M/N (denoted N_1) is*

$$\{m \in M \mid \exists s \in R \setminus \mathfrak{p}_1 \text{ with } sm \in N\}.$$

Proof. The inclusion $\supseteq$ holds always. (That is, this inclusion holds even without the special hypothesis that $\mathfrak{p}_1$ is minimal in the support of M/N.) Suppose $s \in R \setminus \mathfrak{p}_1$, $m \in M$, and $sm \in N$. We prove $m \in N_1$. We know that $sm \in N \subseteq N_1$; hence, $s\bar{m} = 0$ in M/N_1. We also know that $\operatorname{Ass}(M/N_1) = \{\mathfrak{p}_1\}$. So, s is regular on M/N_1. Therefore $\bar{m} = 0$ in M/N_1 and $m \in N_1$.

($\subseteq$) Let $N = N_1 \cap \cdots \cap N_r$ be a primary decompsition of N, with $\operatorname{Ass} M/N_i = \{\mathfrak{p}_i\}$. Notice that $\mathfrak{p}_i \not\subseteq \mathfrak{p}_1$ for any i with $2 \le i$. So $\mathfrak{p}_1 \notin \operatorname{Supp} M/N_i$ for $2 \le i$. So $(M/N_i)_{\mathfrak{p}_1} = 0$ and $(N_i)_{\mathfrak{p}_1} = M_{\mathfrak{p}_1}$ for $2 \le i$. Localize $N = N_1 \cap \cdots \cap N_r$ at $\mathfrak{p}_1$. Get

$$N_{\mathfrak{p}_1} = (N_1)_{\mathfrak{p}_1} \cap \cdots \cap (N_r)_{\mathfrak{p}_1} = (N_1)_{\mathfrak{p}_1} \cap M_{\mathfrak{p}_1} \cap \cdots \cap M_{\mathfrak{p}_1} = (N_1)_{\mathfrak{p}_1}.$$

Focus on $(N_1)_{\mathfrak{p}_1} \subseteq N_{\mathfrak{p}_1}$. If $n_1 \in N_1$, then there exists $s \in R \setminus \mathfrak{p}_1$ with $sn_1 \in N$. □

5. Krull dimension

We will have to prove Nakayama's Lemma and the Artin-Rees Lemma along the way, but I am eager to get started on Krull dimension; so lets start.

These lectures are mainly taken from [5, Section 13].

Definition 5.1. Let R be a ring.

(a) The Krull dimension of R is
$$\dim R = \sup\{r \mid \exists \mathfrak{p}_i \in \operatorname{Spec} R \text{ with } \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_r\}.$$

(b) If $\mathfrak{p} \in \operatorname{Spec} R$, then the height of R is
$$\operatorname{ht} \mathfrak{p} = \sup\{r \mid \exists \mathfrak{p}_i \in \operatorname{Spec} R \text{ with } \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_r = \mathfrak{p}\}.$$
(In particular,
$$\operatorname{ht} \mathfrak{p} = \dim R_{\mathfrak{p}}$$
for all prime ideals $\mathfrak{p}$ of R.)

(c) If I is an arbitrary ideal of R, then
$$\operatorname{ht}(I) = \min\{\operatorname{ht} \mathfrak{p} \mid I \subseteq \mathfrak{p}\}.$$

Remark. We will prove that in a Noetherian ring, all ideals have finite height.

Our first goal. Let R be a semi-local Noetherian ring and M be a finitely generated R-module. Then
$$\dim M = d(M) = \delta(M),$$
where these symbols have the following meaning.

(1) The dimension of M is $\dim M = \dim R/\operatorname{ann} M$,

(2) Let I be an ideal of R with $(\operatorname{rad} R)^{\nu} \subseteq I \subseteq (\operatorname{rad} R)$. Then there exists a polynomial (which depends on M and I) such that
$$\ell\left(\frac{M}{I^{n+1}M}\right) = \operatorname{poly}(n),$$
for $0 \ll n$. The degree of this polynomial depends only on M. We call this degree $d(M)$.

(3) The parameter $\delta(M)$ is defined to be the least integer n such that there exist $x_1, \dots, x_n \in \operatorname{rad}(R)$ such that $(M/(x_1, \dots, x_n))$ has finite length.

Example 5.2. Take $R = \boldsymbol{k}[x_1, \dots, x_s]_{(x_1,\dots,x_s)}$, $M = R$, and $\mathfrak{m} = (x_1, \dots, x_s)R$. Observe that
$$0 \subsetneq (x_1) \subsetneq (x_1, x_2) \subsetneq \cdots \subsetneq (x_1, \dots, x_s)$$
is a chain of prime ideals in R. We conclude $s \le \dim R$.

Observe that the length of $R/\mathfrak{m}^{n+1}$ is the number of monomials of degree at most n is s variables, and this is the number of monomials of degree exactly n in $s+1$ variables, which is $\binom{n+s}{n} = \frac{(n+s)\cdots(n+1)}{s!}$. This is a polynomial of degree s in n. Thus, $d(R) = s$.

Of course $\ell(R/(x_1, \dots, x_s)) = 1$, so $\delta(R) \le s$.

For quite a while, we focus on the combinatorial approach $d(M)$. We think about the associated graded ring

$$\mathrm{gr}_I(R) = \bigoplus_{i=0}^{\infty} \frac{I^i}{I^{i+1}} = \frac{R}{I} \oplus \frac{I}{I^2} \oplus \frac{I^2}{I^3} \oplus \dots$$

and the associated graded module

$$\mathrm{gr}_I(M) = \bigoplus_{i=0}^{\infty} \frac{I^iM}{I^{i+1}M} = \frac{M}{IM} \oplus \frac{IM}{I^2M} \oplus \frac{I^2M}{I^3M} \oplus \dots .$$

First we prove the relevant results about arbitrary graded rings and graded modules, then we apply the general results to $\mathrm{gr}_I(R)$ and $\mathrm{gr}_I(M)$.

5.A. **Graded rings and modules.** A ring R is graded if $R = \bigoplus_{0\le i} R_i$ as an Abelian group under addition and $R_i \cdot R_j \subseteq R_{i+j}$. For example, $R = \boldsymbol{k}[x_1, \dots, x_s]$ is graded by total degree and R_i is the set of homogeneous forms of degree i.

Remark. One could use any commutative semi-group with identity in place of the set of non-negative integers.

If R is a graded ring and M is an R-module, then M is a graded R-module if

$$M = \bigoplus_{i\in\mathbb{Z}} M_i$$

as an Abelian group and $R_iM_j \subseteq M_{i+j}$.

The lecture for November 8, 2018.

Today's goal: Let R be a standard graded algebra over the Artinian ring R_0 (So, R is generated as an algebra over R_0 by R_1, and R_1 is finitely generated as an R_0-module.) and $M = \bigoplus_{0\le i} M_i$ be a finitely generated graded R-module. Then there exists a polynomial with $\mathrm{poly}(n) = \ell_{R_0}(M_n)$, for $0 \ll n$.

Of course, if we are interested in a finitely generated module M over a semi-local ring R, then $\mathrm{gr}_R R$ and $\mathrm{gr}_R M$ satisfy the hypotheses and one can use the conclusion to learn about $\ell_{R/I}(M/I^nM)$ for large n.

Definition and Comment 5.3. An ideal I of a graded ring R is homogeneous if whenever $r = \sum_i r_i \in I$, with $r_i \in R_i$, then each r_i is an element of I. (It is easy to see that the ideal I is homogeneous if and only if I has a generating set which consists of homogeneous elements.)

Observation 5.4. *Let R be a graded ring. Then R is Noetherian if and only if R_0 is Noetherian and R is finitely generated as an R_0-algebra.*

Proof.

($\Leftarrow$) This follows from the Hilbert Basis Theorem.

($\Rightarrow$) Let I be an ideal of R_0. Then IR is a homogeneous ideal of R. By hypothesis, IR is a finitely generated ideal. Pick a finite set of homogeneous generators for IR. From this generating set select the elements of degree zero. This set generates I. Conclude that R_0 is Noetherian.

Now we show that R is finitely generated as an R_0-algebra. Consider the ideal

$$R_+ = \sum_{0<i} R_i$$

of R. This ideal is finitely generated and homogeneous. Let $\theta_1, \dots, \theta_N$ be a homogeneous generating set for the ideal R_+ of R. We claim that

$$R = R_0[\theta_1, \dots, \theta_N].$$

It suffices to show that each R_i is contained in $R_0[\theta_1, \dots, \theta_N]$. Use induction. It is clear that $R_0 \subseteq R_0[\theta_1, \dots, \theta_N]$. Suppose $R_i \subseteq R_0[\theta_1, \dots, \theta_N]$ for all $i < i_0$. Then

$$R_{i_0} = \sum_{j=1}^{N} R_{i_0 - \deg\theta_j}\theta_j \subseteq R_0[\theta_1, \dots, \theta_N].$$

□

Theorem 5.5. *Let $R = \bigoplus_{0\le n} R_n$ be a Noetherian graded ring with R_0 Artinian and let $M = \bigoplus_{0\le n} M_n$ be a finitely generated R-module. Then the Hilbert series of M is a rational function.*

Remark. The <u>Hilbert series</u> of M is the formal power series $\mathrm{HS}_M(t) = \sum_n \ell_{R_0}(M_n)t^n$. A combinatorist would refer to this Hilbert series as the generating function for the sequence $\{\ell_{R_0}(M_n)\}$.

Proof. Write $R = R_0[\theta_1, \dots, \theta_N]$, where θ_i is a homogeneous element of degree d_i.

We induct on N.

If $N = 0$, then M_i is zero all except a finite number of i; so $\mathrm{HS}_M(t)$ is a polynomial.

For $1 \le N$, consider the exact sequence

$$0 \to (0 :_M \theta_N) \to M \xrightarrow{\theta_N} M \to \frac{M}{\theta_N M} \to 0.$$

Length is additive on short exact sequences; so

$$\ell\big((\tfrac{M}{\theta_N M})_n\big) - \ell(M_n) + \ell(M_{n-d_N}) - \ell((0 :_M \theta_N)_{n-d_N}) = 0.$$

Multiply by t^n:

$$\ell\big((\tfrac{M}{\theta_N M})_n\big)t^n - \ell(M_n)t^n + \ell(M_{n-d_N})t^n - \ell((0 :_M \theta_N)_{n-d_N})t^n = 0.$$

Add

$$\sum_{n=0}^{\infty} \ell\big((\frac{M}{\theta_N M})_n\big)t^n - \sum_{n=0}^{\infty} \ell(M_n)t^n + \sum_{n=0}^{\infty} \ell(M_{n-d_N})t^n - \sum_{n=0}^{\infty} \ell((0 :_M \theta_N)_{n-d_N})t^n = 0.$$

Re-write

$$\sum_{n=0}^{\infty}\ell\big((\frac{M}{\theta_N M})_n\big)t^n-\sum_{n=0}^{\infty}\ell(M_n)t^n+t^{d_N}\sum_{n=0}^{\infty}\ell(M_{n-d_N})t^{n-d_N}-t^{d_N}\sum_{n=0}^{\infty}\ell((0:_M\theta_N)_{n-d_N})t^{n-d_n}=0.$$

Thus,

$$\operatorname{HS}_{\frac{M}{\theta_N M}}(t)-\operatorname{HS}_{\ell(M_n)}(t)+t^{d_N}\operatorname{HS}_M(t)-t^{d_N}\operatorname{HS}_{0:_M\theta_N}(t)=0$$

$$\operatorname{HS}_{\frac{M}{\theta_N M}}(t)-t^{d_N}\operatorname{HS}_{0:_M\theta_N}(t)=(1-t^{d_N})\operatorname{HS}_M(t)$$

The modules $\frac{M}{\theta_N M}$ and $0:_M\theta_N$ which are studied on the left are modules over

$$R_0[\theta_1,\dots,\theta_N]/(\theta_N);$$

consequently, the left side is a rational function by induction. Indeed the left side is

$$\frac{\text{polynomial}}{(1-t^{d_1})\cdots(1-t^{d_{N-1}})}.$$

$\square$

Doodle 5.6. $\dfrac{1}{(1-t)^d}=\displaystyle\sum_{i=0}^{\infty}\binom{i+d-1}{d-1}t^i$

Proof.

$$\frac{1}{1-t}=\sum_{i=0}^{\infty}t^i$$

$$\frac{1}{(1-t)^2}=\sum_{i=0}^{\infty}it^{i-1}=\sum_{i=0}^{\infty}(i+1)t^i$$

$$\frac{1}{(1-t)^3}=\sum_{i=0}^{\infty}\frac{(i+1)i}{2}t^{i-1}=\sum_{i=0}^{\infty}\binom{i+2}{2}t^i$$

$$\vdots$$

$$\frac{1}{(1-t)^d}=\sum_{i=0}^{\infty}\binom{i+d-1}{d-1}t^i$$

$\square$

Corollary 5.7. *Let R be a standard graded algebra over the Artinian ring R_0 (So, R is generated as an algebra over R_0 by R_1 and R_1 is a finitely generated R_0-module.) and $M=\bigoplus_{0\le i}M_i$ be a finitely generated graded R-module. (So, $\operatorname{HS}_M=\operatorname{poly}/(1-t)^{\text{power}}$.) Define d to be the least exponent so that $(1-t)^d\operatorname{HS}_M$ is a polynomial. Then there exists a polynomial of degree $d-1$ such that $\operatorname{poly}(n)=\ell_{R_0}(M_n)$, for $0\ll n$.*

The lecture for November 13, 2018.

Last time we saw that

- If $R=\bigoplus_{0\le i} R_i$ is a standard graded ring with R_0 Artinian and $M=\bigoplus_{0\le i} M_i$ is a finitely generated R-module, then
$$\sum \ell_{R_0}(M_n)t^n=\frac{f(t)}{(1-t)^d}$$
for some d and some polynomial $f(t)$ with integer coefficients.
- $$\frac{1}{(1-t)^d}=\sum_{i=0}^{\infty}\binom{i+d-1}{d-1}t^i.$$

Today's first project: Assume d is as small as possible. (That is, assume $f(1)\neq 0$.) Then there exists a polynomial $\operatorname{poly}(t)$ (with rational coefficients) of degree $d-1$ so that
$$\ell_{R_0}(M_n)=\operatorname{poly}(n)$$
for all large n.

Proof. Start with $\operatorname{HS}_M(t)=\frac{f(t)}{(1-t)^d}$, where $f(1)\neq 0$. Write $f(t)=\sum_{i=0}^{s}a_it^i$, with $a_i\in\mathbb{Z}$. Observe that
$$\begin{aligned}\sum \ell_{R_0}(M_n)t^n=\ \operatorname{HS}_M(t)&=\frac{f(t)}{(1-t)^d}=\sum_{i=0}^{s}a_it^i\sum_{i=0}^{\infty}\binom{i+d-1}{d-1}t^i\\ &=\text{lower terms}+\sum_{n=s}^{\infty}\underbrace{\left(a_0\binom{n+d-1}{d-1}+a_1\binom{n+d-2}{d-1}+\cdots+a_s\binom{n+d-1-s}{d-1}\right)}_{\text{I am a polynomial in } n \text{ which \textbf{appears} to have degree } d-1}t^n\end{aligned}$$

The polynomial is
$$a_0\frac{(n+d-1)\cdots(n+1)}{(d-1)!}+a_1\frac{(n+d-2)\cdots(n)}{(d-1)!}+\cdots+a_s\frac{(n+d-1-s)\cdots(n-s+1)}{(d-1)!}.$$
The coefficient of n^{d-1} is $\frac{\sum_i a_i}{(d-1)!}=\frac{f(1)}{(d-1)!}\neq 0$. □

Example 5.8. Lets work out the Hilbert polynomial for
$$R=\frac{k[x_0,\dots,x_r]}{(\text{a homogeneous polynomial of degree } s)}.$$
There is an exact sequence
$$0\to P(-s)\to P\to R\to 0,$$
(where $P=k[x_0,\dots,x_r]$). Thus, for large n,
$$\begin{aligned}\ell_k(R_n)=\ell(P_n)-\ell(P_{n-s})&=\binom{n+r}{r}-\binom{n-s+r}{r}\\ &=\frac{1}{r!}n^r+a_1n^{r-1}+\text{l.o.t.}-\left(\frac{1}{r!}\underbrace{(n-s)^r}_{n^r-rsn^{r-1}+a_1(n-s)^{r-1}}+\text{l.o.t.}\right)\end{aligned}$$

$$= \frac{1}{r!}\Big(n^r - (n^r - rsn^{r-1})\Big) + a_1(\text{some polynomial in } n \text{ of degree } r-2) + \text{l.o.t.}$$

$$= \frac{\boxed{s}}{(r-1)!} n^{r-1} + \text{l.o.t.}.$$

The normalized leading coefficient of the Hilbert polynomial is the constant s. Commutative Algebraists call s the multiplicity of the ring R. Algebraic Geometers call s the degree of the hypersurface defined by the homogeneous polynomial of degree s.

Go back to the original setting: R is semi-local and Noetherian, I is an ideal of definition of R,

$$\operatorname{gr}_I(R) = \bigoplus_{i=0}^{\infty} \frac{I^i}{I^{i+1}} = \frac{R}{I} \oplus \frac{I}{I^2} \oplus \frac{I^2}{I^3} \oplus \dots$$

and

$$\operatorname{gr}_I(M) = \bigoplus_{i=0}^{\infty} \frac{I^iM}{I^{i+1}M} = \frac{M}{IM} \oplus \frac{IM}{I^2M} \oplus \frac{I^2M}{I^3M} \oplus \dots .$$

(Recall that $R$is semi-local means that R only has a finite number of maximal ideals. Also, the ideal I is an ideal of definition means that $\operatorname{rad}(R)^v \subseteq I \subseteq \operatorname{rad}(R)$ for some integer v, where $\operatorname{rad}(R)$ is the intersection of the maximal ideals of R.) We have shown that there exists a polynomial $\operatorname{HP}(t)$ with rational coefficients such that $\operatorname{HP}(n) = \ell_{R/I}(\frac{I^nM}{I^{n+1}M})$ for all large n. It is not a big deal, but we can re-configure this information to produce a polynomial $\operatorname{HSP}(t)$ (of one degree higher) such that

$$\operatorname{HSP}(n) = \ell_R(M/I^{n+1}M).$$

This polynomial is called the <u>Hilbert-Samuel polynomial</u>. If the Hilbert polynomial is

$$\frac{\text{integer}}{(d-1)!} n^{d-1} + \text{l.o.t.},$$

then the corresponding Hilbert-Samuel polynomial is

$$\frac{\text{same integer}}{d!} n^d + \text{l.o.t.}.$$

Reconfiguration 5.9. Suppose $\ell_{R/I}(I^nM/I^{n+1}M) = \operatorname{HP}(n)$ for $c \le n$. Let $\operatorname{HP}(t) = \sum_{j=0}^{d-1} q_j t^j$. Then

$$\begin{aligned} \ell(M/I^{n+1}M) &= \ell(M/I^cM) + \sum_{i=c}^{n} \operatorname{HP}(i) \\ &= \ell(M/I^cM) - \sum_{i=0}^{c-1} \operatorname{HP}(i) + \sum_{i=0}^{n} \operatorname{HP}(i) \end{aligned}$$

(Let C be the constant $C = \ell(M/I^cM) - \sum_{i=0}^{c-1} \operatorname{HP}(i)$.)

$$\begin{aligned}
&= \sum_{i=0}^{n} \mathrm{HP}(i) + C \\
&= \sum_{i=0}^{n} \sum_{j=0}^{d-1} q_j i^j + C \\
&= \sum_{j=0}^{d-1} q_j \sum_{i=0}^{n} i^j + C \\
&= \sum_{j=0}^{d-1} q_j \frac{n^{j+1}}{j+1} + \text{l.o.t.} + C && \text{I'll do this step on the side.} \\
&= q_{d-1} \frac{n^d}{d} + \text{l.o.t.}
\end{aligned}$$

Claim 5.10. $\sum_{i=1}^{n} i^j = \frac{n^{j+1}}{j+1} + \text{l.o.t.}$

Examples 5.11.

$$\sum_{i=1}^{n} i^0 = n$$
$$\sum_{i=1}^{n} i^1 = n(n+1)/2$$
$$\sum_{i=1}^{n} i^2 = n(n+1)(2n+1)/6$$
$$\sum_{i=1}^{n} i^3 = n^2(n+1)^2/4$$

Proof. Use induction on j. Assume the result for $j-1$.

$$\begin{aligned}
n^{j+1} - 0 &= \sum_{i=1}^{n} (i^{j+1} - (i-1)^{j+1}) \\
&= \sum_{i=1}^{n} \left((j+1)i^j - \binom{j+1}{2} i^{j-1} + \binom{j+1}{3} i^{j-2} + \dots \right) \\
&= (j+1) \sum_{i=1}^{n} i^j + \text{a polynomial in } n \text{ of degree } j.
\end{aligned}$$

We conclude that

$$\sum_{i=1}^{n} i^j = \frac{n^{j+1}}{j+1} + \text{l.o.t.}\ .$$

□

Observation 5.12. *Let R be a Noetherian semi-local ring, M be a finitely generated R-module, and I and J be ideals of definition of R. Then the polynomials which give $\ell(M/I^{n+1}M)$ and $\ell(M/J^{n+1}M)$, for large n, have the same degree.*

Proof. We begin with $\operatorname{rad}(R)^v \subseteq I \subseteq \operatorname{rad}(R)$ and $\operatorname{rad}(R)^w \subseteq J \subseteq \operatorname{rad}(R)$ for some integers v and w. Thus, there are positive integers a and b with $I^a \subseteq J$ and $J^b \subseteq I$. Anyhow, there is a surjective map

$$R/(I^a)^{n+1} \to R/J^{n+1};$$

(with kernel $J^{n+1}/(I^a)^{n+1}$) hence

$$\ell(R/J^{n+1}) \leq \ell(R/(I^a)^{n+1})$$

and $\mathrm{HSP}^J(n) \leq \mathrm{HSP}^I(an+a-1)$ for all large n. (I am writing $\mathrm{HSP}^I(n)$ and $\mathrm{HSP}^J(n)$ for the polynomials which give $\ell(M/I^{n+1}M)$ and $\ell(M/J^{n+1}M)$, respectively, for all large n.) This forces $\deg \mathrm{HSP}^J \leq \deg \mathrm{HSP}^I$. (This is a calculus statement.) Use $J^b \subseteq I$ to get the other inequality. □

Theorem 5.13. *Let R be a Noetherian semi-local ring and let*

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

be a short exact sequence of finitely generated R-modules. Then

(a) $d(M) = \max\{d(M'), d(M'')\}$*, and*

(b) *If I is an ideal of definition of R, then $\mathrm{HSP}^I_M - \mathrm{HSP}^I_{M''}$ and $\mathrm{HSP}^I_{M'}$ have the same degree and leading term.*

(Recall that $d(M)$ is the degree of the Hilbert-Samuel polynomial $\mathrm{HSP}^I_M(t)$ which gives $\ell_R(M/I^{n+1}M)$ for all large n, where I is an ideal of definition of R. The degree of $\mathrm{HSP}^I_M(t)$ does not depend on the choice of I.)

Proof. Let I be an ideal of definition. No harm is done if we take M' to be a submodule of M and M'' to be M/M'. In this case,

$$\frac{M''}{I^nM''} = \frac{\frac{M}{M'}}{I^n\frac{M}{M'}} = \frac{M}{M'+I^nM}.$$

Consider the filtration

$$0 \subseteq I^nM \subseteq M'+I^nM \subseteq M.$$

We see that

$$\ell\left(\frac{M}{I^nM}\right) = \underbrace{\ell\left(\frac{M}{M'+I^nM}\right)}_{\ell\left(\frac{M''}{I^nM''}\right)} + \underbrace{\ell\left(\frac{M'+I^nM}{I^nM}\right)}_{\ell\left(\frac{M'}{I^nM\cap M'}\right)}.$$

The Artin-Rees Lemma says that if R is a Noetherian ring, M is a finitely generated R-module, N is a submodule of M, and I is an ideal of R, then there is an integer c such that $I^nM \cap N = I^{n-c}(I^cM \cap N)$, for all n with $c \leq n$. We did not yet prove the Artin-Rees Lemma; but we will use it anyhow.

Fix c with $I^nM \cap M' = I^{n-c}(I^cM \cap M')$. We have shown that

$$\ell\left(\frac{M}{I^nM}\right) = \ell\left(\frac{M''}{I^nM''}\right) + \ell\left(\frac{M'}{I^{n-c}(I^cM \cap M')}\right). \tag{5.13.1}$$

The length on the left is used to find $d(M)$; the middle length is used to find $d(M'')$; the modules on the right are similar enough to the modules that are used to compute $d(M')$. We will show that for large n, the length of these modules is given by a polynomial and that this polynomial has the same degree and the same leading coefficient as the Hilbert-Samuel polynomial $\mathrm{HSP}^I_{M'}$.

Consider the short exact sequence

$$0 \to \frac{(I^cM \cap M')}{I^{n-c}(I^cM \cap M')} \to \frac{M'}{I^{n-c}(I^cM \cap M')} \to \frac{M'}{(I^cM \cap M')} \to 0$$

The module on the right has fixed finite length.

There is a polynomial so that the length of the module on the left is equal to $\mathrm{poly}(n)$ for all large n.

Thus, there is a polynomial $p(t)$ such that the length of the module in the middle, namely

$$\frac{M'}{I^{n-c}(I^cM \cap M')} = \frac{M'}{(I^nM \cap M')},$$

is given by $p(n)$ for all large n. At any rate, (5.13.1) gives

$$\mathrm{HSP}_M(n) = \mathrm{HSP}_{M''}(n) + p(n)$$

for all large n. It follows that

$$\deg \mathrm{HSP}_M(t) = \deg\big(\mathrm{HSP}_{M''}(n) + p(n)\big) = \max\{\deg \mathrm{HSP}_{M''}(t), \deg p(t)\}$$

(The last equality holds because $\deg \mathrm{HSP}_{M''}(t)$ and $\deg p(t)$ both have POSITIVE leading coefficients!) and the leading coefficient of $\mathrm{HSP}_M(t) - \mathrm{HSP}_{M''}(t)$ is equal to the leading coefficient of $p(t)$.

We finish the proof by showing that $p(t)$ and $\mathrm{HSP}_{M'}(t)$ have the same degree and the same leading coefficient. Observe that

$$I^nM' \subseteq I^nM \cap M' = I^{n-c}(I^cM \cap M') \subseteq I^{n-c}M'$$

(The equality in the middle is the Artin-Rees Lemma.) Thus,

$$\tfrac{M'}{I^nM'} \twoheadrightarrow \tfrac{M'}{I^nM \cap M'} \twoheadrightarrow \tfrac{M'}{I^{n-c}M'}$$

and

$$\mathrm{HSP}_{M'}(n-c) \le p(n) \le \mathrm{HSP}_{M'}(n)$$

for all large n. Use calculus to see that the polynomials $\mathrm{HSP}_{M'}(t)$ and $p(t)$ have the same degree and the same leading coefficient. □

Lemma 5.14. [Nakayama's Lemma] *Let M be a finitely generated module over the Noetherian semi-local ring R. If $\mathrm{rad}(R) \cdot M = M$, then $M = 0$.*

Proof. Let $m_1, \dots, m_N$ be a generating set for M. Identify elements $r_{i,j}$ in $\operatorname{rad}(R)$ with

$$\begin{bmatrix} m_1 \\ \vdots \\ m_N \end{bmatrix} = \begin{bmatrix} r_{1,1} & \dots & r_{1,N} \\ \vdots & & \vdots \\ r_{N,1} & \dots & r_{N,N} \end{bmatrix} \begin{bmatrix} m_1 \\ \vdots \\ m_N \end{bmatrix}$$

Rewrite this equation as $0 = (I - \phi) \begin{bmatrix} m_1 \\ \vdots \\ m_N \end{bmatrix}$, where each entry of ϕ is in $\operatorname{rad}(R)$. Multiply both sides of the equation on the left by the classical adjoint of $I - \phi$. Get

$$0 = \det(I - \phi) \begin{bmatrix} m_1 \\ \vdots \\ m_N \end{bmatrix}.$$

Thus, $\det(I - \phi) \cdot M = 0$. On the other hand, $\det(I - \phi)$ is equal to one plus an element of $\operatorname{rad}(R)$; hence, $\det(I - \phi)$ is not in any maximal ideal of R. Thus, $\det(I - \phi)$ is a unit of R (I think I used that R is Noetherian at this point.) and M is the zero module. ☐

5.B. **Proof of the main Theorem.**

Theorem 5.15. *Let R be a semi-local Noetherian ring and M be a finitely generated R-module, then* $\dim M = d(M) = \delta(M)$.

(Recall that $\dim(M)$ is the Krull dimension of M, $d(M)$ is the degree of the Hilbert-Samuel polynomial of M, and $\delta(M)$ is the least number of elements $r_1, \dots, r_n$ in $\operatorname{rad}(R)$ such that $M/(r_1, \dots, r_n)M$ has finite length.)

Proof.

Claim 5.16. $\dim R \leq d(R)$

Proof. Induct on $d(R)$.

If $d(R) = 0$, then $\ell(R/(\operatorname{rad} R)^n)$ is constant for large n. It follows that there exists n with $(\operatorname{rad} R)^n = (\operatorname{rad} R)^{n+1}$. Apply Nakayama's Lemma to conclude that $(\operatorname{rad} R)^n = 0$. It follows that $\operatorname{rad}(R)$ is contained in every prime ideal of R. Thus, every prime ideal of R is a maximal ideal and R has Krull dimension zero.

If $0 < d(R)$. (We know that $d(R)$ is finite. We do not yet know that $\dim(R)$ is finite; but we will learn that very soon.)

Consider a chain of prime ideals

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_e$$

in R. Pick $x \in \mathfrak{p}_1 \setminus \mathfrak{p}_0$. Consider the short exact sequence

$$0 \to R/\mathfrak{p}_0 \xrightarrow{x} R/\mathfrak{p}_0 \to R/(\mathfrak{p}_0 + x) \to 0.$$

Recall from Theorem 5.13 that

$$\underbrace{\mathrm{HSP}_{R/\mathfrak{p}_0}}_{\text{middle}} - \mathrm{HSP}_{R/(\mathfrak{p}_0,x)} \quad \text{and} \quad \underbrace{\mathrm{HSP}_{R/\mathfrak{p}_0}}_{\text{left}}$$

have the same degree and the same leading coefficient. Thus,

$$d(R/(\mathfrak{p}_0, x)) < d(R/\mathfrak{p}_0) \le d(R).$$

Thus, induction gives

$$\dim(R/(\mathfrak{p}_0, x)) \le d(R/(\mathfrak{p}_0, x)).$$

In particular,

$$e - 1 \le \dim(R/(\mathfrak{p}_0, x)) \le d(R/(\mathfrak{p}_0, x)) < d(R).$$

Thus, $\dim R < \infty$ and $\dim R - 1 < d(R)$; hence $\dim R \le d(R)$. This completes the proof of Claim 5.16. □

Claim 5.17. $\dim M \le d(M)$

Proof. The proof has two steps.

Step 1. We observe that if

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

is a short exact sequence of finitely generated R-modules then

$$d(M) = \max\{d(M'), d(M'')\} \quad \text{and} \quad \dim(M) = \max\{\dim(M'), \dim(M'')\}$$

Step 2. We identify a filtration

$$0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n = M$$

of M with $M_i/M_{i-1} = R/\mathfrak{p}_i$.

Actually, the left assertion in Step 1 is established in Theorem 5.13 and we did Step 2 in the proof of Proposition 4.12, when we proved that $\operatorname{Ass} M$ is finite. We still must do the right assertion in Step 1. This is easy. Now that we know that the set of prime ideals in a Noetherian ring satisfy Descending Chain Condition, we know

$$\dim M = \max\{\dim R/\mathfrak{p} \mid \mathfrak{p} \in \operatorname{Supp} M\}.$$

Furthermore,

$$\operatorname{Supp} M = \operatorname{Supp} M' \cup \operatorname{Supp} M''. \tag{5.17.1}$$

We prove (5.17.1).

($\subseteq$) If $M_{\mathfrak{p}} \neq 0$, then at least one of $M'_{\mathfrak{p}}$ or $M''_{\mathfrak{p}}$ is non-zero.

($\supseteq$) If either $M'_{\mathfrak{p}} \neq 0$ or $M''_{\mathfrak{p}} \neq 0$, then $M_{\mathfrak{p}}$ is also non-zero.

Equation (5.17.1) is established.

We prove the assertion on the right of Step 1. Observe that

$$\begin{aligned}\dim M &= \max\{\dim R/\mathfrak{p} \mid \mathfrak{p} \in \operatorname{Supp} M\} = \max\{\dim R/\mathfrak{p} \mid \mathfrak{p} \in \operatorname{Supp} M' \cup \operatorname{Supp} M''\} \\ &= \max\{\max\{\dim R/\mathfrak{p} \mid \mathfrak{p} \in \operatorname{Supp} M'\}, \max\{\dim R/\mathfrak{p} \mid \mathfrak{p} \in \operatorname{Supp} M''\}\} \\ &= \max\{\dim M', \dim M''\}.\end{aligned}$$

Now we can finish the proof of Claim 5.17. Iterate the statements about how $\dim$ and d behave on short exact sequences and apply Claim 5.16 to see that

$$\begin{aligned} \dim(M) &= \max\{\dim(R/\mathfrak{p}_i)\} \\ &\leq \max\{d(R/\mathfrak{p}_i)\} && \text{Claim 5.16} \\ &= d(R/\mathfrak{p}_i) \end{aligned}$$

This completes the proof of Claim 5.17. □

Claim 5.18. $d(M) \leq \delta(M)$.

Proof.

Observe first that

$$\delta(M) = 0 \implies \ell(M) = 0 \implies \mathrm{HSP}_M(t) \text{ is a constant } \implies d(M) = 0.$$

The Key Calculation If $x \in \mathrm{rad}(R)$ and $M_1 = M/(x)M$, then

$$\ell(M/(\mathrm{rad}\, R)^n \cdot M) - \ell(M/(\mathrm{rad}\, R)^{n-1} \cdot M) \leq \ell(M_1/(\mathrm{rad}\, R)^n \cdot M_1).$$

Assume The Key Calculation (for the time being) and finish the argument.

The Key Calculation yields that if $x \in \mathrm{rad}(R)$, then $d(M) - 1 \leq d(M/xM)$. Assume $\delta(M) = s$ and $M/(x_1, \ldots, x_s)M$ has finite length.

Then

$$d(M) - s \leq \cdots \leq d(M/(x_1, \cdots, x_{s-1}) - 1 \leq d(M/(x_1, \cdots, x_s)) = 0.$$

Thus, $d(M) \leq s = \delta(M)$.

Prove the Key Calculation. Consider the short exact sequence

$$0 \to \frac{xM + (\mathrm{rad}\, R)^n \cdot M}{(\mathrm{rad}\, R)^n \cdot M} \to \frac{M}{(\mathrm{rad}\, R)^n \cdot M} \to \underbrace{\frac{M}{xM + (\mathrm{rad}\, R)^n \cdot M}}_{\frac{M_1}{(\mathrm{rad}\, R)^n \cdot M_1}} \to 0. \tag{5.18.1}$$

Observe that multiplication by x induces a surjection

$$M \to \frac{xM + (\mathrm{rad}\, R)^n \cdot M}{(\mathrm{rad}\, R)^n \cdot M}$$

with kernel

$$(\mathrm{rad}\, R)^n M :_M x.$$

Thus

$$\frac{M}{(\mathrm{rad}\, R)^n M :_M x} \xrightarrow{\cong} \frac{xM + (\mathrm{rad}\, R)^n \cdot M}{(\mathrm{rad}\, R)^n \cdot M}.$$

Of course, $(\mathrm{rad}\, R)^{n-1} M \subseteq (\mathrm{rad}\, R)^n M :_M x$; so there is a surjection

$$\frac{M}{(\mathrm{rad}\, R)^{n-1} M} \longrightarrow \frac{M}{(\mathrm{rad}\, R)^n M :_M x} \xrightarrow{\cong} \frac{xM + (\mathrm{rad}\, R)^n \cdot M}{(\mathrm{rad}\, R)^n \cdot M}.$$

It follows that

$$\ell\left(\frac{xM+(\operatorname{rad}R)^n\cdot M}{(\operatorname{rad}R)^n\cdot M}\right)\le \ell\left(\frac{M}{(\operatorname{rad}R)^{n-1}M}\right). \tag{5.18.2}$$

Combine (5.18.1) and (5.18.2) to see that

$$\begin{aligned}\ell\left(\frac{M}{(\operatorname{rad}R)^n\cdot M}\right)&=\ell\left(\frac{M_1}{(\operatorname{rad}R)^n\cdot M_1}\right)+\ell\left(\frac{xM+(\operatorname{rad}R)^n\cdot M}{(\operatorname{rad}R)^n\cdot M}\right)\\ &\le \ell\left(\frac{M_1}{(\operatorname{rad}R)^n\cdot M_1}\right)+\ell\left(\frac{M}{(\operatorname{rad}R)^{n-1}M}\right)\end{aligned}$$

This completes the proof of Claim 5.18. □

Class on Nov. 27, 2018

We are proving the following Theorem. If R is a Noetherian semi-local ring and M is a finitely generated R-module, then $\dim M = d(M) = \delta(M)$, where $\dim M$ is the length of the longest chain of prime ideals in $R/\operatorname{ann} M$, $d(M)$ is the degree of HSP^I_M, where HSP^I_M is the polynomial with $\mathrm{HSP}^I_M(n) = \ell(M/I^{n+1}M)$ for all large n (and I is an ideal of definition of R), and $\delta(M)$ is the least integer s with the property that there exist $x_1,\dots,x_s$ in $\operatorname{rad}(R)$ with $\ell(M/(x_1,\dots,x_s)M)$ finite.

Last time we proved $\dim M \le d(M) \le \delta(M)$.

The mathematical key to $\dim M \le d(M)$ is: If $\mathfrak{p}$ is a prime ideal of R and $x \in R\setminus\mathfrak{p}$, then every chain of primes in $R/(x,\mathfrak{p})$ is shorter then the corresponding chain of primes in $R/\mathfrak{p}$ and we can employ the exact sequence

$$0\to R/\mathfrak{p}\xrightarrow{x} R/\mathfrak{p}\to R/(x,\mathfrak{p})\to 0$$

to see that $d(R/(x,\mathfrak{p})) < d(R/\mathfrak{p})$. (The in-between step is the Theorem that says that if

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

is a short exact sequence of finitely generated R-modules, then $\mathrm{HSP}_M-\mathrm{HSP}_{M''}$ and $\mathrm{HSP}_{M'}$ have the same degree and the same leading coefficient.)

The mathematical key to $d(M)\le\delta(M)$ is an estimate for how small $d(M/xM)$ can be when $x\in\operatorname{rad}(R)$. Indeed,

$$d(M)-1\le d(M/xM)\le d(M).$$

The reason is

$$\ell(M/(\operatorname{rad}R)^nM)-\ell(M/(\operatorname{rad}R)^{n-1}M)\le \ell((M/xM)/(\operatorname{rad}R)^n(M/xM)).$$

Once one gets this, one learns

$$\mathrm{HSP}_M(n)-\mathrm{HSP}_M(n-1)\le \mathrm{HSP}_{M/xM}(n).$$

The combinatorial key is: if $f(t)$ is a polynomial in $\mathbb{Z}[t]$, then $f(t)-f(t-1)$ is a polynomial with degree equal to degree f minus 1. Indeed, if $f=a_rt^r+a_{r-1}t^{r-1}+$l.o.t., with $a_r\neq 0$, then

$$f(t)-f(t-1)=a_r(t^r-(t-1)^r)+a_{r-1}(t^{r-1}-(t-1)^{r-1})+\text{l.o.t.}$$

$$= a_r(rt^{r-1} + \text{l.o.t.}) + a_{r-1}((r-1)t^{r-2} + \text{l.o.t.}) + \text{l.o.t.} = a_r r t^{r-1} + \text{l.o.t.}$$

and this has degree $r-1$.

Finally, we prove $\delta(M) \le \dim M$.

Observe that

$$\begin{aligned} \dim M = 0 &\implies \text{all prime ideals of } R/\operatorname{ann} M \text{ are maximal ideals} \\ &\implies R/\operatorname{ann} M \text{ is an Artinian ring} && \text{by Theorem 3.31} \\ &\implies M \text{ has finite length} && \text{by Proposition 3.34} \\ &\implies \delta M = 0. \end{aligned}$$

Henceforth, we assume $\dim M$ is positive. Let $\mathfrak{p}_1, \dots, \mathfrak{p}_t$ be the prime ideals in R which are minimal over $\operatorname{ann} M$ and which have $\dim M = \dim R/\mathfrak{p}_i$. Observe that every chain of prime ideals in $R/\operatorname{ann} M$ which exhibits $\dim M$ contains one of these $\mathfrak{p}_i$. None of these prime ideals is a maximal ideal; so $\operatorname{rad}(R) \not\subseteq \mathfrak{p}_i$ for any i and therefore, by the Prime Avoidance Lemma,

$$\operatorname{rad} R \not\subseteq \bigcup_{i=1}^{t} \mathfrak{p}_i.$$

So, there exists an element x, with $x \in \operatorname{rad}(R)$ but $x \notin \mathfrak{p}_i$ for any i. Thus, the chains of primes which live in $\operatorname{Supp} R/\operatorname{ann}(M/xM)$ all are SHORTER than the maximal chains of primes in $\operatorname{Supp} R/\operatorname{ann} M$. Thus, $\dim M/xM < \dim M$. Induction on $\dim$ gives $\delta(M/xM) \le \dim(M/xM)$. Of course, $\delta(M) \le \delta(M/xM) + 1$. Thus,

$$\delta(M) - 1 \le \delta(M/xM) \le \dim(M/xM) \le \dim M - 1,$$

and $\delta(M) \le \dim(M)$, as desired. This completes the proof of Theorem 5.15 □

5.C. **Quick consequences of the main Theorem.**

Corollary 5.19. [Krull Principal Ideal Theorem] *Let R be a Noetherian ring and I be an ideal of R which can be generated by r elements. If $\mathfrak{p}$ is a prime ideal of R which is minimal over I, then $\operatorname{ht} \mathfrak{p} \le r$.*

Proof. Observe that

$$\operatorname{ht} \mathfrak{p} = \dim R_{\mathfrak{p}} = \delta(\dim R_{\mathfrak{p}}) \le r$$

because $R_{\mathfrak{p}}$ mod the r generators of I has finite length! □

Theorem 5.20. *Let $\mathfrak{p}$ be a prime ideal of height r in a Noetherian ring R. The following statements hold.*

(a) *There exist r elements $a_1, \dots, a_r$ in $\mathfrak{p}$, with $\mathfrak{p}$ minimal over $(a_1, \dots, a_r)$.*
(b) *If $b_1, \dots, b_s$ are elements of $\mathfrak{p}$, then*

$$\operatorname{ht} \mathfrak{p} - s \le \operatorname{ht} \mathfrak{p}/(b_1, \dots, b_s) \le \operatorname{ht} \mathfrak{p}.$$

(c) *If $a_1, \dots, a_r$ are in $\mathfrak{p}$, with $\mathfrak{p}$ minimal over $(a_1, \dots, a_r)$, then $\operatorname{ht} \mathfrak{p} - s = \operatorname{ht} \mathfrak{p}/(a_1, \dots, a_s)$.*

Proof.
(a) We calculate in $R_\mathfrak{p}$. We know $\operatorname{ht}\mathfrak{p} = \dim R_\mathfrak{p} = \delta(R_\mathfrak{p})$. Thus, there exist $\alpha_1, \cdots, \alpha_r$ in $\mathfrak{p}R_\mathfrak{p}$ with the property that $R_\mathfrak{p}/(\alpha_1, \cdots, \alpha_r)R_\mathfrak{p}$ has finite length. Write α_i as a_i/s_i with $\alpha_i \in \mathfrak{p}$ and $s_i \in R \setminus \mathfrak{p}$. It follows that $R_\mathfrak{p}/(a_1, \cdots, a_r)R_\mathfrak{p}$ has finite length. In particular, $\mathfrak{p}R_\mathfrak{p}$ is minimal over $(a_1, \cdots, a_r)R_\mathfrak{p}$; and therefore, $\mathfrak{p}$ is minimal over $(a_1, \cdots, a_r)R$.

(b) It suffices to show that

$$\operatorname{ht}\mathfrak{p} - s \leq \operatorname{ht}\mathfrak{p}/(b_1, \dots, b_s).$$

Let $t = \operatorname{ht}\mathfrak{p}/(b_1, \dots, b_s)$. By (a), there exist elements $c_1, \dots, c_t$ in R with $\mathfrak{p}$ minimal over $(c_1, \dots, c_t, b_1, \dots, b_s)$. At this point, the Krull Principal Ideal Theorem guarantees that

$$r = \operatorname{ht}\mathfrak{p} \leq t + s;$$

thus,

$$\operatorname{ht}\mathfrak{p} - s = r - s \leq t = \operatorname{ht}\mathfrak{p}/(b_1, \dots, b_s).$$

(c) The ideal $\mathfrak{p}$ has height r and $\mathfrak{p}$ is minimal over $(a_1, \dots, a_r)$. We are supposed to prove that

$$\operatorname{ht}\mathfrak{p}/(a_1, \dots a_s) = \operatorname{ht}\mathfrak{p} - s.$$

We know from (b) that

$$\operatorname{ht}\mathfrak{p} - s \leq \operatorname{ht}\mathfrak{p}/(a_1, \dots a_s).$$

On the other hand, $\mathfrak{p}/(a_1, \dots a_s)$ is minimal over $(a_{s+1}, \dots, a_r)R/(a_1, \dots a_s)$; hence the Krull Principal Ideal Theorem yields that

$$\operatorname{ht}\mathfrak{p}/(a_1, \dots a_s) \leq r - s.$$

□

5.D. **Proof of the Artin-Rees Lemma.** This is the proof from Chapter 5 in [3]; it is beautiful!

Lemma 5.21. [The Artin-Rees Lemma] *If R is a Noetherian ring, M is a finitely generated R-module, N is a submodule of M, and I is an ideal of R, then there is an integer c such that $I^n M \cap N = I^{n-c}(I^c M \cap N)$, for all n with $c \leq n$.*

Proof. Let $\mathscr{R}(I)$ be the graded R-algebra

$$\mathscr{R}(I) = R \oplus I \oplus I^2 \oplus \dots.$$

(This R-algebra is called the Rees algebra of I.) Notice that the component in degree zero is R (which is Noetherian), the component in degree 1 is I (which is finitely generated as an R-module), and $\mathscr{R}(I)$ is generated over the zero component by the first component. Thus, $\mathscr{R}(I)$ is a Noetherian ring. Consider the graded $\mathscr{R}(I)$-module

$$\mathscr{M} = M \oplus IM \oplus I^2 M \oplus \dots .$$

Notice that the generators of M as an R-module generate $\mathscr{M}$ as an $\mathscr{R}(I)$-module; hence $\mathscr{M}$ is a finitely generated $\mathscr{R}(I)$-module. Consider also the graded $\mathscr{R}(I)$-submodule

$$\mathscr{N} = N \oplus (IM \cap N) \oplus (I^2M \cap N) \oplus \dots$$

of $\mathscr{M}$. Notice that $\mathscr{N}$ is a graded submodule of a graded Noetherian module. It follows that $\mathscr{N}$ is generated by a finite set of homogeneous elements! Let c be the largest degree among this finite set of homogeneous generators of $\mathscr{N}$. It follows that

$$I^nM \cap N = I^{n-c}(I^cM \cap N).$$

□

5.E. **The amazing Corollary of Nakayama's Lemma.** We proved (see 5.14) that if M is a finitely generated module over the Noetherian local ring $(R, \mathfrak{m})$ with $\mathfrak{m}M = M$, then $M = 0$.

Corollary 5.22. *Let M be a finitely generated module over the Noetherian local ring $(R, \mathfrak{m}, \boldsymbol{k})$ and let $m_1, \dots, m_n$ be elements of M. Then $m_1, \dots, m_n$ generate M if and only if $\bar{m}_1, \dots \bar{m}_n$ generate $M/\mathfrak{m}M$.*

Proof. The assertion $(\Rightarrow)$ is obvious. We prove $(\Leftarrow)$. We assume $M = R(m_1, \dots, m_n) + \mathfrak{m}M$. We prove $M = R(m_1, \dots, m_n)$. Let $N = M/R(m_1, \dots, m_n)$. Observe that

$$\mathfrak{m}N = \frac{\mathfrak{m}M + R(m_1, \dots, m_n)}{R(m_1, \cdots, m_n)} = \frac{M}{R(m_1, \cdots, m_n)} = N;$$

thus $N = 0$ by Nakayama's Lemma and $M = R(m_1, \dots, m_n)$. □

The point is that $M/\mathfrak{m}M$ is a finite dimensional vector space over $\boldsymbol{k}$. Every linearly independent subset is part of a basis. Every generating set contains a basis. If one has the right number ($\dim_{\boldsymbol{k}} M/\mathfrak{m}M$) of linearly independent elements, then these elements automatically generate. If one has the the right number ($\dim_{\boldsymbol{k}} M/\mathfrak{m}M$) of elements and they generate, then they automatically are linearly independent.

If m is an arbitrary non-zero element in a finitely generated module M over a Noetherian local ring, then m is part of a minimal generating set for M. (Nothing like this is true for modules over non-local rings. Think of the $\mathbb{Z}$-module of even integers: 4 is a non-zero even integer, but 4 is not part of a minimal generating set for $(2)\mathbb{Z}$.) If m_2 is in M but not in (m), then m, m_2 is part of a minimal generating for M.

5.F. **Chains of homogeneous prime ideals.** I want to prove a little result.

Proposition 5.23. *Let R be a non-negatively graded Noetherian ring and $\mathfrak{p}$ be a homogeneous ideal R with $\operatorname{ht} \mathfrak{p} = r$. Then there exists a chain of homogeneous prime ideals in R*

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_r = \mathfrak{p}.$$

Obviously, there can be chains of prime ideals in R which exhibit $\operatorname{ht}\mathfrak{p}$ and which involve non-homogeneous prime ideals:

$$(0) \subsetneq (x+y^2) \subsetneq (x,y)$$

in $\boldsymbol{k}[x,y]$. (One can apply Eisenstein's criteria to the ring $(\boldsymbol{k}[x])[y]$ to see that $x+y^2$ is an irreducible polynomial in a Unique Factorization Domain and therefore generates a prime ideal.) The Proposition makes no assertion about every chain, it merely makes an assertion about some chain.

Homogeneous ideals are interesting because folks that do geometry in projective space are interested only in homogeneous ideals!

The proof is a little bit delicate; but it uses the results we proved after we proved $\dim = d = \delta$.

There is one preliminary Lemma that we need.

Lemma 5.24. *Let R be a non-negatively graded Noetherian ring and M be a finitely generated homogeneous R-module. If $\mathfrak{p} \in \operatorname{Ass} M$, then $\mathfrak{p}$ is homogeneous.*

Proof. Let $\mathfrak{p}$ be in $\operatorname{Ass} M$. Then there exists a non-zero element $m \in M$ with $\operatorname{ann} m = \mathfrak{p}$. Write $m = m_a + m_{a+1} + \dots m_{a+s}$, with $m_i \in M_i$. Let $f = f_b + f_{b+1} + \dots + f_{b+t}$ be in $\mathfrak{p}$ with $f_i \in R_i$. We prove $f_b \in \mathfrak{p}$. To do this, we prove $f_b^N m = 0$ for some large N. Observe that

$$\begin{aligned} 0 = fm &= (f_b + f_{b+1} + \dots + f_{b+t})(m_a + m_{a+1} + \dots m_{a+s}) \\ &= f_b m_a + (f_b m_{a+1} + f_{b+1} m_a) + \dots \ . \end{aligned}$$

Thus, $f_b m_a = 0$, $f_b^2 m_{a+1} = 0$, $f_b^3 m_{a+2} = 0$, $\dots$, and $f_b^{\text{a large power}} m = 0$ as desired. $\square$

The class on Dec. 4, 2018.

Last time we proved:

Lemma. Let R be a non-negatively graded Noetherian ring and M be a finitely generated graded R-module. If $\mathfrak{p} \in \operatorname{Ass} M$, then $\mathfrak{p}$ is homogeneous.

Today's first project is

Proposition. Let R be a non-negatively graded Noetherian ring and $\mathfrak{p}$ be a homogeneous ideal R with $\operatorname{ht}\mathfrak{p} = r$. Then there exists a chain of homogeneous prime ideals in R

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \dots \subsetneq \mathfrak{p}_r = \mathfrak{p}.$$

Proof of Proposition 5.23. Let

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \dots \subsetneq \mathfrak{p}_r = \mathfrak{p}$$

be a chain of primes R. The prime $\mathfrak{p}_0$ is a minimal prime of R, so $\mathfrak{p}_0 \in \operatorname{Ass} R$ and therefore, $\mathfrak{p}_0$ is homogeneous by Lemma 5.24. If $r = 0$, we are finished. Otherwise, we use induction. We prove the conclusion for $\frac{\mathfrak{p}}{\mathfrak{p}_0}$ in $\frac{R}{\mathfrak{p}_0}$. That, is we assume R is a graded domain and we use the old notation: $\mathfrak{p}$ is a homogeneous ideal of height r in the domain R. We prove that there exists a chain of homogeneous prime ideals of length r descending from $\mathfrak{p}$.

Let b be a non-zero homogeneous element in $\mathfrak{p}$. Observe that

$$r-1 \le \operatorname{ht} \frac{\mathfrak{p}}{(b)} \le r-1.$$

The inequality on the left is Theorem 5.20.(b) which says that

$$b \in \mathfrak{p} \implies \operatorname{ht}\mathfrak{p} - 1 \le \operatorname{ht} \frac{\mathfrak{p}}{(b)}$$

always! The inequality on the right is due to the fact that every maximal chain of prime ideals in R starts at (0). This (0) is not an ideal in $R/(b)$; thus every maximal chain of primes in $R/(b)$ is shorter than the corresponding chain of primes in R. Consider a maximal chain of prime ideals in R of the form

$$\mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_r$$

with $b \in \mathfrak{q}_1$. The ideal $\mathfrak{q}_1$ is minimal over (b); hence $\mathfrak{q}_1 \in \operatorname{Ass} R/(b)$ and $\mathfrak{q}_1$ is homogeneous. Now look at $\frac{\mathfrak{p}}{\mathfrak{q}_1}$, which is a homogeneous prime of height $r-1$ in the graded ring $R/\mathfrak{q}_1$. Apply induction. □

5.G. **Examples.**

Example 5.25. Consider the ring $R = P/I_2(X)$, where P is the polynomial ring

$$P = \boldsymbol{k}[x_{1,1}, x_{1,2}, x_{1,3}, x_{2,1}, x_{2,2}, x_{2,3}]$$

and X is the matrix

$$X = \begin{bmatrix} x_{1,1} & x_{1,2} & x_{1,3} \\ x_{2,1} & x_{2,2} & x_{2,3} \end{bmatrix}.$$

(There is a spot or two where it might be necessary to assume that the field $\boldsymbol{k}$ is infinite.) Here is my list of objectives.

(i) I want to prove that $I_2(X)$ is a prime ideal.

(ii) I want to explore the sense in which R is the homogeneous coordinate ring for the Segre embedding of $\mathbb{P}^1 \times \mathbb{P}^2$ into $\mathbb{P}^5$.

(iii) I want to explore the dimension of R in terms of chains of prime ideals.

(iv) I want to explore the dimension of R in terms of the Hilbert-Samuel polynomial. In particular, I want to identify the multiplicity of R (which is the normalized leading coefficient of the Hilbert-Samuel polynomial). Our main tool in this sub-project is the free resolution of R by free P-modules.

(v) I want to explore the dimension of R in terms of how many homogeneous forms are needed to make $R/(\lambda_1, \dots, \lambda_s)$ have finite length. If possible, I want to choose these forms to be linear and I want to choose the forms in such a way that R and $R/(\lambda_1, \dots, \lambda_s)$ have the same multiplicity. In this case, what is the geometric significance of this "multiplicity"?

Remark. If you are bothered that R is a graded but not local ring; and our Theorem is about local rings (or semi-local rings), then think about the localization $R_{\mathfrak{m}}$ where $\mathfrak{m}$ is the maximal homogeneous ideal of R. Of course, to figure out $\operatorname{HSP}_{R_{\mathfrak{m}}}$ we immediately pass to

$\mathrm{gr}(R_{\mathfrak{m}})$, which is equal to R. (The ring $R_{\mathfrak{m}}$ is the the ring of rational functions which are defined at the origin on the cone in affine 6-space of the the image of the Segre embedding. Draw the standard cone picture.)

Lets get to work.

(i) First we prove that $I_2(X)$ is a prime ideal.

Claim 5.26. *If*

$$\phi : P = \boldsymbol{k}[x_{1,1}, x_{1,2}, x_{1,3}, x_{2,1}, x_{2,2}, x_{2,3}] \to \boldsymbol{k}[X_1Y_1, X_1Y_2, X_1Y_3, X_2Y_1, X_2Y_2, X_2Y_3]$$

is the homomorphism defined by $\phi(x_{i,j}) = X_iY_j$, *then*

$$\ker(\phi) = I_2 \underbrace{\begin{bmatrix} x_{1,1} & x_{1,2} & x_{1,3} \\ x_{2,1} & x_{2,2} & x_{2,3} \end{bmatrix}}_{X}.$$

Proof. It is clear that the containment $\supseteq$ holds. We prove $\subseteq$. We replace all appearances of

$$x_{1,1}x_{2,2}, \quad x_{1,1}x_{2,3}, \quad \text{and} \quad x_{1,2}x_{2,3}$$

(with $x_{1,2}x_{2,1}$, $x_{1,3}x_{2,1}$, and $x_{1,3}x_{2,2}$, respectively). If f is an arbitrary element of P, then

$$f = x_{1,1}F(x_{1,1}, x_{2,1}, x_{1,2}, x_{1,3}) + x_{1,2}G(x_{1,2}, x_{1,3}, x_{2,1}, x_{2,2}) + H(x_{1,3}, x_{2,1}, x_{2,2}, x_{2,3}) + \text{an element of } I_2(X).$$

Suppose f is in $\ker(\phi)$ and is homogeneous. We want to prove that F, G, and H are identically zero. Observe that

$$0 = \phi(f) = \begin{cases} +X_1Y_1F(X_1Y_1, X_2Y_1, X_1Y_2, X_1Y_3) & \text{every term has } Y_3 \deg < X_1 \deg \\ +X_1Y_2G(X_1Y_2, X_1Y_3, X_2Y_1, X_2Y_2) & \text{every term has } Y_3 \deg < X_1 \deg \\ +H(X_1Y_3, X_2Y_1, X_2Y_2, X_2Y_3) & \text{every term has } X_1 \deg \le Y_3 \deg \end{cases}$$

So $H(X_1Y_3, X_2Y_1, X_2Y_2, X_2Y_3)$ is the zero polynomial. Write

$$H(x_{1,3}, x_{2,1}, x_{2,2}, x_{2,3}) = \sum_i x_{1,3}^i H_i(x_{2,1}, x_{2,2}, x_{2,3})$$

We know that

$$0 = \phi(H) = \sum_i (X_1Y_3)^i H_i(X_2Y_1, X_2Y_2, X_2Y_3)$$

Use the $x_1 \deg$ to see that $H_i(X_2Y_1, X_2Y_2, X_2Y_3) = 0$ for each i. But H_i is homogeneous. We may factor out $X_2^{\deg H_i}$ to see that $H_i(Y_1, Y_2, Y_3)$ is identically zero; hence H_i is identically zero for each i and H is identically zero.

At this point,

$$0 = \phi(f) = \begin{cases} +X_1Y_1F(X_1Y_1, X_2Y_1, X_1Y_2, X_1Y_3) & \text{every term has } X_2 \deg < Y_1 \deg \\ +X_1Y_2G(X_1Y_2, X_1Y_3, X_2Y_1, X_2Y_2) & \text{every term has } X_2 \deg = Y_1 \deg \end{cases}$$

So, $G(X_1Y_2, X_1Y_3, X_2Y_1, X_2Y_2)$ is identically zero. Write

$$G(x_{1,2}, x_{1,3}, x_{2,1}, x_{2,2}) = \sum_i x_{1,3}^i G_i(x_{1,2}, x_{2,1}, x_{2,2}).$$

We know
$$0=\phi(G)=\sum_i (X_1Y_3)^iG_i(X_1Y_2,X_2Y_1,X_2Y_2).$$
Use Y_3 degree to see that each $G_i(X_1Y_2,X_2Y_1,X_2Y_2)=0$. Write
$$G_i(x_{1,2},x_{2,1},x_{2,2})=\sum_j (x_{1,2})^j\sum_j G_{i,j}(x_{2,1},x_{2,2}).$$
We know
$$0=\phi(G_i(x_{1,2},x_{2,1},x_{2,2}))=\sum_j (X_1Y_2)^j\sum_j G_{i,j}(X_2Y_1,X_2Y_2).$$
Use X_1 degree to see that each homogeneous form $G_{i,j}(X_2Y_1,X_2Y_2)$ is zero. Now factor out $X_2^{\deg G_{i,j}}$ to see that each $G_{i,j}(Y_1,Y_2)$ is zero. Conclude that each $G_{i,j}(x_{2,1},x_{2,2})$ is identically zero. It follows that each $G_i(x_{1,2},x_{2,1},x_{2,2})$ is identically zero and $G(x_{1,2},x_{1,3},x_{2,1},x_{2,2})$ is zero. One treats F the same way. First $F=\sum_i x_{2,1}^iF_i(x_{1,1},x_{1,2},x_{1,3})$. Apply ϕ. Use X_2 degree to see that each $\phi(F_i)=0$. Factor a power of X_1 from $\phi(F_i)=0$ to see that each F_i is identically zero. □

(ii) Affine space is nice; but it isn't compact and curves that "should" intersect (like parallel lines) don't intersect "until infinity". One introduces projective space to "correct" these quirks. Ah, but projective space has its own issues. The product of two projective spaces isn't a projective space. But the Segre embedding embeds a product of projective spaces into a projective space. In particular, the Segre embedding
$$\mathbb{P}^1\times\mathbb{P}^2\to\mathbb{P}^5$$
is given by
$$([a_1:a_2],[b_1:b_2:b_3])\mapsto[a_1b_1:a_1b_2:a_1b_3:a_2b_1:a_2b_2:a_2b_3].$$
If the coordinates of $\mathbb{P}^5$ are
$$[x_{1,1}:x_{1,2}:x_{1,3}:x_{2,1}:x_{2,2}:x_{2,3}],$$
then it is clear that the image of the Segre embedding vanishes when plugged into $I_2(X)$:
$$x_{1,i}x_{2,j}-x_{1,j}x_{2,i}|_{[a_1b_1:a_1b_2:a_1b_3:a_2b_1:a_2b_2:a_2b_3]}=(a_1b_i)(a_2b_j)-(a_1bb_j)(a_2b_i)=0.$$
It turns out that the ideal $I_2(X)$ is equal to the set of polynomials which vanish on the image of the above Segre embedding. We proved this in our claim! If $f\in P$ vanishes on the image of the Segre embedding, then $\phi(f)$ is identically zero (hence, maybe $\boldsymbol{k}$ must be infinite here) $\phi(f)$ is the zero polynomial and $f\in I_2(X)$.

(iii) One chain of prime ideals in P that contains $I_2(X)$ is
$$I_2(X)\subsetneq(x_{1,1},x_{2,1},x_{1,2}x_{2,3}-x_{1,3}x_{2,2})\subsetneq(x_{1,1},x_{2,1},x_{1,2},x_{2,2})\subsetneq(x_{1,1},x_{2,1},x_{1,2},x_{2,2},x_{1,3})\subsetneq\mathfrak{m}.$$
To show that $x_{1,2}x_{2,3}-x_{1,3}x_{2,2}$ generates a prime ideal in the Unique Factorization Domain $\boldsymbol{k}[x_{1,2},x_{2,3},x_{1,3},x_{2,2}]$ one can probably use tricks that were learned in the first year graduate sequence.

(iv) Let Δ_i be the determinant of X with column i deleted. Observe that

$$F: \quad 0 \to P(-3)^2 \xrightarrow{X^{\text{transpose}}} P(-2)^3 \xrightarrow{\begin{bmatrix}\Delta_1 & -\Delta_2 & \Delta_3\end{bmatrix}} P \tag{5.26.1}$$

is a complex with zero-th homology equal to R. This complex is actually a resolution. We first compute $(\Delta_1, \Delta_2) : \Delta_3$.

The argument I propose for this is pretty cute.

$$(\Delta_1, \Delta_2) \subseteq (x_{1,3}, x_{2,3}).$$

So,

$$(\Delta_1, \Delta_2) : \Delta_3 \subseteq (x_{1,3}, x_{2,3}) : \Delta_3.$$

But, $(x_{1,3}, x_{2,3})$ is a prime ideal and $\Delta_3 \notin (x_{1,3}, x_{2,3})$. Thus, $(x_{1,3}, x_{2,3}) : \Delta_3 = (x_{1,3}, x_{2,3})$. When you agreed that (5.26.1) is a complex, you agreed that $(x_{1,3}, x_{2,3}) \subseteq (\Delta_1, \Delta_2) : \Delta_3$. Thus,

$$(x_{1,3}, x_{2,3}) \subseteq (\Delta_1, \Delta_2) : \Delta_3 \subseteq (x_{1,3}, x_{2,3}) : \Delta_3 = (x_{1,3}, x_{2,3}).$$

At this point we know that the kernel of

$$\begin{bmatrix}\Delta_1 & -\Delta_2 & \Delta_3\end{bmatrix}$$

looks like

$$\begin{bmatrix} x_{1,1} & x_{2,1} & * \\ x_{1,2} & x_{2,2} & * \\ x_{1,3} & x_{2,3} & 0 \end{bmatrix},$$

where

$$\begin{bmatrix} * \\ * \end{bmatrix}$$

consists of all relations on

$$\begin{bmatrix}\Delta_1 & -\Delta_2\end{bmatrix}$$

for which

$$\begin{bmatrix} * \\ * \\ 0 \end{bmatrix}$$

is not already in the column space of

$$\begin{bmatrix} x_{1,1} & x_{2,1} \\ x_{1,2} & x_{2,2} \\ x_{1,3} & x_{2,3} \end{bmatrix}.$$

It turns out that Δ_1 and Δ_2 are each irreducible (we discussed this) and neither one is a unit times the other. Thus, the relations on

$$\begin{bmatrix}\Delta_1 & -\Delta_2\end{bmatrix}$$

are generated by

$$\begin{bmatrix} \Delta_2 \\ \Delta_1 \\ 0 \end{bmatrix}$$

and this relation is in the column space of

$$\begin{bmatrix} x_{1,1} & x_{2,1} \\ x_{1,2} & x_{2,2} \\ x_{1,3} & x_{2,3} \end{bmatrix}.$$

That finishes the proof.

We immediately read that

$$\ell(R_n) = \ell(P_n) - 3\ell(P_{n-2}) + 2\ell(P_{n-3})$$
$$\sum_n \ell(R_n)t^n = \sum_n \ell(P_n)t^n - 3\sum_n \ell(P_{n-2})t^n + 2\sum_n \ell(P_{n-3})t^n$$

Thus,

$$\begin{aligned}\sum_n \ell\left(\frac{\mathfrak{m}^n}{\mathfrak{m}^{n+1}}\right) t^n &= \sum_n \ell(R_n)t^n = \Big(\sum_n \ell(P_n)t^n\Big)(1-3t^2+2t^3) = \frac{(1-t)^2(1+2t)}{(1-t)^6} \\ &= \frac{1+2t}{(1-t)^4} = (1+2t)\sum_n \binom{n+3}{3} t^n =^* \sum_n \left[1\binom{n+3}{3} + 2\binom{n+2}{3}\right] t^n \\ &= \sum_n \left[\frac{3n^3}{3!} + \text{l.o.t.}\right] t^n\end{aligned}$$

The step labeled $*$ might only work for large n. Thus, for large n,

$$\ell(R/m^{n+1}) = \sum_{i=n_0}^{n} \left(\frac{3i^3}{3!} + \text{l.o.t.}\right) + \text{constant} = \frac{3n^4}{4!} + \text{l.o.t.}.$$

We conclude that $\dim R$ (or if you prefer, $\dim R_{\mathfrak{m}}$) is 4 and the multiplicity of R is 3. This might be a good time to notice that if P is replace by a polynomial ring P' in d variables (for some d with $2 \leq d$); but otherwise the resolution

$$0 \to P'(-3)^2 \to P'(-2)^3 \to P'$$

remains "the same" (i.e., fix a homomorphism $P \to P'$ and apply $P' \otimes_P -$ to the original resolution and still get a resolution!), then the Hilbert Series

$$\sum_n \ell\left(\frac{(\mathfrak{m}P')^n}{(\mathfrak{m}P')^{n+1}}\right) t^n$$

will still be

$$\frac{1+2t}{(1-t)^{d-2}}$$

and the length

$$\ell\left(\frac{P'}{(\mathfrak{m}P')^{n+1}}\right)$$

will still be

$$\frac{3n^{d-2}}{(d-2)!} + \text{l.o.t.}.$$

(v) One collection of linear forms with the property that $R/(\lambda_1,\dots,\lambda_4)R$ has finite length is

$$\lambda_1 = x_{2,1}, \lambda_2 = x_{1,3}, \lambda_3 = x_{2,2} - x_{1,1}, \lambda_4 = x_{1,2} - x_{2,3}$$

because

$$\frac{R}{(\lambda_1,\dots,\lambda_4)R} = \frac{\boldsymbol{k}[x_{1,1},x_{1,2}]}{I_2\left(\begin{bmatrix} x_{1,1} & x_{1,2} & 0 \\ 0 & x_{1,1} & x_{1,2}\end{bmatrix}\right)} = \frac{\boldsymbol{k}[x_{1,1},x_{1,2}]}{(x_{1,1},x_{1,2})^2},$$

which has length $\boxed{3}$.

An Algebraic Geometer thinks "If I have a (Cohen-Macaulay) variety of dimension dim and degree deg and I slice this variety with dim hyperplanes in general position, then I end up with deg points, if I count the multiplicity correctly." (Our specialization produced the origin counted with multiplicity 3.)

A commutative algebraist thinks, "If I have a Cohen-Macaulay local ring of dimension dim and multiplicity mult, and I mod out by a regular sequence of dim elements from $\mathfrak{m}\setminus\mathfrak{m}^2$, then I end up with a local ring of length equal to mult."

Be sure to notice that if $P' = P/(\lambda_1,\lambda_2,\lambda_3,\lambda_4)$, then $P'\otimes_P F$, for F given in (5.26.1) becomes

$$0 \to P'(-3)^2 \xrightarrow{\begin{bmatrix} x_{1,1} & 0 \\ x_{1,2} & x_{1,1} \\ 0 & x_{1,2}\end{bmatrix}} P'(-2)^3 \xrightarrow{\begin{bmatrix} x_{1,2}^2 & -x_{1,1}x_{1,2} & x_{1,1}^2\end{bmatrix}} P'.$$

One can easily check by hand that $P'\otimes_P F$ is a resolution of $P'/(x_{1,1},x_{1,2})^2$.

Examples 5.27. (a) Let R_0 be a Noetherian domain and R be the polynomial ring $R = R_0[x_1,\dots,x_n]$. Then the prime ideal $(x_1,\dots,x_i)$ of R has height i for all i. Of course,

$$(0) \subsetneq (x_1) \subsetneq (x_1,x_2) \subsetneq \cdots \subsetneq (x_1,\dots,x_i)$$

is a chain of prime ideals in R which demonstrates $i \le \operatorname{ht}(x_1,\dots,x_i)$. On the other hand, $(x_1,\dots,x_i)$ is a prime ideal minimal over an ideal (namely $(x_1,\dots,x_i)$) which can be generated by i elements; so the Krull Principal Ideal Theorem guarantees that $\operatorname{ht}(x_1,\dots,x_i) \le i$.

(b) Let R_0 be a Noetherian ring and R be the polynomial ring $R = R_0[x_1,\dots,x_n]$. Let $\mathfrak{p}_0$ be a minimal prime ideal of R_0. Then the prime ideal $(\mathfrak{p}_0,x_1,\dots,x_i)$ of R has height i for all i. (For example, if $R_0 = \mathbb{Z}/(6)$, then $\mathfrak{p}_0$ could be $(2)R_0$ or $(3)R_0$.) Of course,

$$(\mathfrak{p}_0)R \subsetneq (\mathfrak{p}_0,x_1)R \subsetneq (\mathfrak{p}_0,x_1,x_2)R \subsetneq \cdots \subsetneq (\mathfrak{p}_0,x_1,\dots,x_i)R$$

is a chain of prime ideals in R which demonstrates $i \le \operatorname{ht}(\mathfrak{p}_0,x_1,\dots,x_i)R$. On the other hand, $(\mathfrak{p}_0,x_1,\dots,x_i)$ is a prime ideal of R which is minimal over an ideal (namely $(x_1,\dots,x_i)$) which can be generated by i elements; so the Krull Principal Ideal Theorem guarantees that $\operatorname{ht}(\mathfrak{p}_0,x_1,\dots,x_i)R \le i$.

I want to prove that $(\mathfrak{p}_0, x_1, \ldots, x_i)$ is a prime ideal of R which is minimal over $(x_1, \ldots, x_i)$. Suppose $\mathfrak{q}$ is a prime ideal of R with

$$(x_1, \ldots, x_i)R \subseteq \mathfrak{q} \subseteq (\mathfrak{p}_0, x_1, \ldots, x_i)R$$

Intersect with R_0 to get

$$\underbrace{(x_1, \ldots, x_i)R \cap R_0}_{(0)} \subseteq \mathfrak{q} \cap R_0 \subseteq \underbrace{(\mathfrak{p}_0, x_1, \ldots, x_i)R \cap R_0}_{\mathfrak{p}_0 R}.$$

Thus, $\mathfrak{q} \cap R_0$ is a prime ideal of R_0 which is contained in the minimal prime ideal $\mathfrak{p}_0$; hence $\mathfrak{q} \cap R_0 = \mathfrak{p}_0$ and $(\mathfrak{p}_0, x_1, \ldots, x_i)$ is a prime ideal of R which is minimal over $(x_1, \ldots, x_i)$ as claimed.

Contents

References

[1] W. Bruns and J. Herzog Cohen-Macaulay rings, Cambridge Studies in Advanced Mathematics, **39**. Cambridge University Press, Cambridge, 1993.
[2] W. Bruns and U. Vetter, *Determinantal rings* Lecture Notes in Mathematics, **1327** Springer-Verlag, Berlin, 1988.
[3] D. Eisenbud, *Commutative algebra. With a view toward algebraic geometry*, Graduate Texts in Mathematics, **150** Springer-Verlag, New York, 1995.
[4] H. Matsumura, *Commutative algebra*, Second edition, Mathematics Lecture Note Series, **56** Benjamin/Cummings Publishing Co., Inc., Reading, Mass., 1980.
[5] H. Matsumura, *Commutative ring theory* Cambridge Studies in Advanced Mathematics, **8**. Cambridge University Press, Cambridge, 1986.