NOTES – MATH 538
FALL 2013

KARL SCHWEDE

1. Monday, August 26th, 2013

1.1. **Introduction to rings, ideals and homomorphisms.** Commutative algebra is the study of commutative, associative rings with unity. Throughout this class, every *ring* will be commutative, associative and with unity. There are two main historical reasons to study commutative algebra:

- Algebraic Number Theory
- Algebraic Geometry

In algebraic number theory you might study rings like $\mathbb{Z}$ or $\mathbb{Z}[17]$ or $\mathbb{Z}_p$ (p-adics). Algebraic geometry studies geometric objects where the allowable functions are polynomials. For example, in topology you study geometric objects whose geometry is measured by continuous functions. In differential geometry you study geometric objects and you use differentiable functions to measure them. In algebraic geometry you study geometric objects using algebraic functions (polynomials). In all these types of geometry, knowing the functions is the same as understanding the geometric object.

It turns out that this is surprisingly powerful for algebraic geometry, every ring is a ring of functions on some uniquely determined geometric object (including the ring $\mathbb{Z}$, as we'll see later). This lets us interpret questions from number theory in a geometric language and thus gain access to new kinds of intuition. Furthermore, it allows you to translate number theoretic questions to the case of polynomial rings, where things are frequently easier.

> *Polynomial rings with coefficients in a field (and quotients/subrings) are generally easier to study than polynomial rings with coefficients in $\mathbb{Z}$ or some other ring of integers.*

The main way we will study rings is through their ideals. Suppose R is a ring. Note that if I, J are ideals then so is their intersection $I \cap J$, their sum $I + J = \{x + y \mid x \in I, y \in J\}$, their product $I \cdot J = \{\sum_{i=1}^{n} x_i \cdot y_i \mid x_i \in I, y_i \in J\}$. But their union $I \cup J$ is generally *not* an ideal.

Recall the following theorem:

Theorem 1.1. *Suppose that $J \subseteq R$ is an ideal. Then there is a bijection between the sets:*

$$\{\textit{ideals of } R \textit{ containing } J\} \leftrightarrow \{\textit{ideals of } R/J\}$$

Proof. The forward $\to$ direction takes an ideal I to I/J. The inverse $\leftarrow$ direction is just $\rho^{-1}(\overline{I})$ where I is an ideal of R/J. □

Definition 1.2 (Maximal ideals)**.** An ideal $I \subseteq R$ is called *maximal* if $I \neq R$ and there is no proper ideal between I and R.

Lemma 1.3. *An ideal I is maximal if and only if R/I is a field.*

Proof. The zero ring is not a field, so we can dispense with the case that $R = I$. Recall that R/I is a field if and only if the only proper ideal is $\langle 0 \rangle$. Of course, this is clearly equivalent to requiring that I is maximal by **??**. □

Definition 1.4 (Prime ideals)**.** An ideal $I \subseteq R$ is called *prime* if $I \neq R$ and if $xy \in I$, for $x, y \in R$, implies that either $x \in I$ or $y \in I$.

Lemma 1.5. *An ideal I is prime if and only if R/I is an (integral) domain.*

Proof. Suppose first that I is prime. If $\overline{x}, \overline{y} \in R/I$ (corresponding to $x, y \in R$) and $\overline{x} \cdot \overline{y} = 0$, then $x \cdot y \in I$ so either $x \in I$ and $y \in I$ by the primality of I. Thus $\overline{x} = 0$ or $\overline{y} = 0$.

Conversely, if I is not prime then there exist $x, y \in R$ with $x \cdot y \in I$ but $x, y \notin I$. Hence $\overline{x} \cdot \overline{y} = 0 \in R/I$ and R/I is not an integral domain. □

Example 1.6 (A ring of continuous functions)**.** Suppose that C is the ring of continuous functions $f : \mathbb{R} \to \mathbb{R}$. These form a ring under pointwise addition and multiplication. Consider the set $I = \{f \in C \mid f(0) = 0\}$. This is an ideal of C (the sum of two functions that vanish at the origin vanishes at the origin, the product of a function that vanishes at the origin and another function still vanishes at the origin). Is it prime or maximal?

Prime: If $f \cdot g \in I$, then $0 = (f \cdot g)(0) = (f(0)) \cdot (g(0))$. Thus either f or g vanish at the origin. In particular I is prime.

Maximal: In R/I, two functions are identified whenever they agree at the origin (note $f + I = g + I$ if and only if $f - g$ vanishes at the origin). In particular, each coset of R/I looks like $\{\text{constant}\} + I$. These have the structure of the ring $\mathbb{R}$, which is a field, and hence I is maximal.

On the other hand, the ideal $J = \{f \in C \mid f(x) = 0 \text{ for all } x \in [0, 1]\}$ is not prime and hence also not maximal. To see it isn't prime, consider f and g continuous functions where f vanishes on $[0, 0.5]$ and g vanishes on $[0.5, 1]$.

Another useful fact about prime ideals is the following.

Lemma 1.7. *Suppose that $I \subseteq R$ is a prime ideal and $J, J' \subseteq R$ are other ideals, then the following are equivalent.*

(i) *$J \subseteq I$ or $J' \subseteq I$,*
(ii) *$J \cap J' \subseteq I$,*
(iii) *$J \cdot J' \subseteq I$.*

Proof. We will prove the equivalence of (i) and (ii) and leave the relation with (iii) as an exercise (or you can do it as we did in class). Of course, obviously (i) implies (ii). Now suppose that $J \cap J' \subseteq I$. Suppose $J' \notin I$ and choose $x' \in J' \setminus I$. We will show that $J \subseteq I$. Choose $x \in J$. Then $xx' \in J \cap J' \subseteq I$ and hence either $x \in I$ or $x' \in I$. But the latter situation is impossible, so $x \in I$ and hence $J \subseteq I$. We have just shown that (ii) implies (i). □

Example 1.8 (A polynomial ring)**.** Consider $R = \mathbb{R}[x]$ where $\mathbb{R}$ is a field. Consider the ideal I made up of all polynomials f such that $f(0) = 0$. It is easy to see that $I = \langle x \rangle$. Furthermore I is both prime (for the same reason as the ring of continuous functions) and maximal since $R/I \cong \mathbb{R}$ is a field.

Now consider $S = \mathbb{R}[x, y]$ and I is again the ideal made up of all polynomials f such that $f(0) = 0$. In this case $I = \langle x, y \rangle$ is again both prime and maximal. Note that $J = \langle x \rangle$ is prime since $S/J \cong k[y]$ (note, S/J can be viewed as polynomials under the equivalence relation where $f \sim g$ if they agree along the line $x = 0$).

Finally, I leave it as an exercise to check that $M = \langle xy \rangle$ is the set of functions that vanish on both the x and y axes.

2. Wednesday, August 28th, 2013

2.1. **Ring homomorphisms.** We now review how ideals behave under ring homomorphisms.

Definition 2.1. For us, a homomorphism of rings $f : R \longrightarrow S$ always satisfies $f(1_R) = 1_S$.

This is justified by thinking about functions. We'll see that all ring homomorphisms are basically pullbacks of functions from one topological space to another. In this case, the constant function 1 should be pulled back to the constant function 1.

Proposition 2.2. *Suppose that $f : R \longrightarrow S$ is a ring homomorphism. Then $f^{-1}(J)$ is an ideal for every ideal $J \subseteq S$. However, if I is an ideal of R, then $f(I)$ need not be an ideal of S (unless f happens to be surjective). However, the ideal $f(I)$ generates is usually denoted by IS.*

In the special case that f is injective, or better yet that $R \subseteq S$, $f^{-1}(J)$ is frequently denoted by $J \cap R$.

Furthermore:

(a) *If $J \subseteq S$ is prime, so is $f^{-1}(J)$.*
(b) *If $J \subseteq S$ is maximal, $f^{-1}(J)$ need not be.*
(c) *If $I \subseteq R$ is prime or maximal, then $J \cdot S$ need not be, unless f is surjective.*
(d) *If $I \subseteq R$, then $I \subseteq f^{-1}(IS)$.*
(e) *If $J \subseteq S$, then $J \supseteq (f^{-1}(J))S$.*

Proof. This is left as an exercise to the reader. □

2.2. **The spectrum of a ring.**

Definition 2.3 (Spec)**.** For a ring R the *(prime) spectrum* of R, denoted $\operatorname{Spec} R$, is the set of all prime ideals of R. The set of all maximal ideals is denoted by $\mathfrak{m}\text{-}\operatorname{Spec} R$.

Example 2.4 (Spec of PIDs)**.**
- If k is a field, then $\operatorname{Spec} k$ is a singleton, the ideal generated by zero.
- $\operatorname{Spec}\mathbb{Z}$ is the set $\{\langle p\rangle \mid p \in \mathbb{Z}_{>0} \text{ prime}\} \cup \{\langle 0\rangle\}$.
- For $\operatorname{Spec}\mathbb{C}[x]$, since $\mathbb{C}[x]$ is a PID, we observe that the prime ideals are just $\langle f\rangle$ where f is irreducible or zero. Since $\mathbb{C}$ is algebraically closed, the irreducible elements are linear polynomials. In particular,

$$\operatorname{Spec} R = \{\langle x-\alpha\rangle \mid \alpha \in \mathbb{C}\} \cup \{\langle 0\rangle\}.$$

  This can be identified with $\mathbb{C}$ unioned with another point $\langle 0\rangle$.
- For $\operatorname{Spec}\mathbb{R}[x]$, a similar analysis yields:

$$\operatorname{Spec} R = \{\langle x-\alpha\rangle \mid \alpha \in \mathbb{R}\} \cup \{\langle x^2+bx+c\rangle \mid b,c \in \mathbb{R}, x^2+bx+c \text{ is irreducible}\} \cup \{\langle 0\rangle\}.$$

  In this case, $\operatorname{Spec}\mathbb{R}[x]$ can be viewed as the set of conjugate pairs of $\mathbb{C}$, unioned with another point $\langle 0\rangle$.

Our next goal is to give $\operatorname{Spec} R$ the structure of a topological space. Suppose that I is an ideal of R. Then we set $V(I) \subseteq \operatorname{Spec} R$ to be the set of prime ideals containing I.

Lemma 2.5. (a) *If I, J are ideals, then $V(I \cap J) = V(I) \cup V(J)$.*
(b) *If $\{I_\lambda\}_{\lambda\in\Lambda}$ is a family of ideals then $V\big(\sum_{\lambda\in\Lambda} I_\lambda\big) = \bigcap_{\lambda\in\Lambda} V(I_\lambda)$.*

Proof. For (a), suppose that a prime ideal P contains $I \cap J$. Then P contains I or J by Lemma 1.7. The reverse direction just reverses this.

For (b), suppose that $P \supseteq \sum_{\lambda\in\Lambda} I_\lambda$, then obviously P contains every ideal in the sum. For the reverse direction, if P contains each I_λ then it contains the sum. □

Hence we declare a subset $Y \subseteq \operatorname{Spec} R$ to be *closed* if $Y = V(I)$.

Theorem 2.6. *With notation as above, the closed sets form a topology on* $\operatorname{Spec} R$*. This is called the* Zarsiki topology*.*

This *very weak* topology is very far from Hausdorff. Indeed, a point (prime ideal) $P \in \operatorname{Spec} R$ is closed if and only if P is a maximal ideal. On $\operatorname{Spec}\mathbb{Z}$, ignoring the point $\langle 0\rangle$, this is just the finite complement topology.

3. Friday, August 30th

Proposition 3.1. *Suppose that $f : R \longrightarrow S$ is a ring homomorphism. Then the map $Q \mapsto f^{-1}(Q)$, $\phi : \operatorname{Spec} S \longrightarrow \operatorname{Spec} R$ is continuous.*

Proof. Suppose that I is an ideal of R. We need to show that $\phi^{-1}(V(I))$ is closed. The obvious thing to hope is that $\phi^{-1}(V(I)) = V(IS)$. Indeed, suppose that $P \in V(I) \subseteq \operatorname{Spec} R$ so that $P \supseteq I$. Suppose that $Q \in \operatorname{Spec} S$ is such that $\phi(Q) = P$ (in other words, that $f^{-1}(Q) = P$). Certainly $P \cdot S \subseteq Q$ and so $I \cdot S \subseteq Q$ and thus $\phi^{-1}(V(I)) \subseteq V(IS)$.

Now suppose that $Q \in V(IS) \subseteq \operatorname{Spec} S$ so that $Q \supseteq IS$. Consider $P = f^{-1}(Q) = \phi(Q)$ and observe that $P \supseteq I$. Thus $V(IS) \subseteq \phi^{-1}(V(I))$. □

Example 3.2. Consider the map $f : \mathbb{C}[x] \longrightarrow \mathbb{C}[t]$ which sends x to $t^2 - 1$ and fixes $\mathbb{C}$. Let's consider the induced map on the prime spectra (note that both spectra are the same, copies of $\mathbb{C}$ with an extra zero point). Denote the map $\phi : \operatorname{Spec} \mathbb{C}[t] \longrightarrow \operatorname{Spec} \mathbb{C}[x]$. From here on out, since f is injective, we can replace x by t^2.

The zero ideal $\langle 0 \rangle$ is sent to the zero ideal (since ϕ is injective) so that isn't interesting. Now consider the prime ideal $P = \langle t - \alpha \rangle \subseteq \mathbb{C}[t]$. We ask what is $\phi(P)$. There is a unique prime ideal $Q \subseteq \mathbb{C}[t^2 - 1]$ with $Q = P \cap \mathbb{C}[t]$. Since the prime ideals of $\mathbb{C}[x] = \mathbb{C}[t^2 - 1]$ all look like $\langle (t^2 - 1) - \beta \rangle$, we need $(t^2 - 1) - \beta \in \langle t - \alpha \rangle$ (and this β is unique). Of course, $t^2 - \alpha^2 \in \langle t - \alpha \rangle$ and so we see that $1 + \beta = \alpha^2$ or in other words that $\beta = \alpha^2 - 1$.

In conclusion, the point $\langle t - \alpha \rangle$ (corresponding to α) is sent to $\langle x - (\alpha^2 - 1) \rangle$ (which corresponds to $\alpha^2 - 1$). If we identify the map ϕ with the map $\mathbb{C} \longrightarrow \mathbb{C}$ which sends α to $\alpha^2 - 1$, then f is just the pullback of this morphism (on polynomials).

Lemma 3.3. *Given any $P \in \operatorname{Spec} R$, the topological closure $\overline{\{P\}}$ is equal to $V(P)$. In particular, the closed points of $\operatorname{Spec} R$ are exactly the maximal ideals.*

Proof. The smallest $V(I)$ that contains P is simply $V(P)$. (Note if $P \in V(I)$, then $P \supseteq I$, larger ideals give smaller V's). The result follows immediately. □

3.1. **Plenty of prime ideals.** Recall Zorn's lemma, which we assume as an axiom.

Theorem 3.4 (Zorn's Lemma)**.** *Suppose that X is a non-empty partially ordered set under $\leq$ that satisfies the following condition. For every ascending chain $\ldots \leq x_\lambda \leq \ldots$ (for λ in some indexing set Λ) there exists an element $z \in X$ with $z \geq$ every element in the chain. Then, X contains at least one maximal element.*

Using this, we can show that rings have plenty of maximal ideals.

Proposition 3.5. *Suppose that $I \subsetneq R$ is a proper ideal in a ring R. Then there exists a maximal ideal of R, $\mathfrak{m} \supseteq I$.*

Proof. Let X be the set of proper ideals of R which contain I, ordered under inclusion. We claim that X satisfies the condition of Zorn's lemma. Obviously X is nonempty as it contains I. Further suppose that $I \subseteq \ldots \subseteq$

$J_\lambda \subseteq \ldots$ is an ascending chain (for λ in some indexing set Λ). Let $J = \bigcup_{\lambda\in\Lambda} J_\lambda$. We claim that J is a proper ideal.

To see it is an ideal, suppose that $x, x' \in J$, so $x \in J_\lambda$ and $x' \in J_{\lambda'}$. By symmetry we suppose that $J_\lambda \subseteq J_{\lambda'}$ so that $x, x' \in J_{\lambda'}$. Since $J_{\lambda'}$ is an ideal, $x + x' \in J_{\lambda'} \subseteq J$ which shows that J is closed under addition. If $x \in J$ and $r \in R$, then $x \in J_\lambda$ for some λ and thus so is rx. Hence $rx \in J$. This proves that J is an ideal. Finally, since each J_λ is proper, 1 is not in any J_λ and so $1 \notin J$. Hence J is also proper. It follows that Zorn's lemma is satisfied and our desired maximal ideal is guaranteed. □

Corollary 3.6. Spec R *always contains at least 1 closed point assuming it is non-empty.*

Proof. Combine Lemma 3.3 and Proposition 3.5. □

3.2. **Multiplicative sets and localization.** Suppose that R is a ring.

Definition 3.7 (Multiplicative set)**.** A multiplicative set $W \subseteq R$ is a set such that $1 \in W$ and such that W is closed under multiplication.

Example 3.8. Suppose that R is an integral domain, then $W = R \setminus \{0\}$ is a multiplicative set. Alternately, if $t \in R$, then $\{1, t, t^2, t^3, \ldots\}$ is a multiplicative set.

Lemma 3.9. *Suppose that $P \subseteq R$ is a prime ideal, then $R \setminus P$ is a multiplicative set.*

Proof. If $a, b \in W := R \setminus P$, then $ab \notin P$ and hence $ab \in W$. Of course $1 \in W$ since $1 \notin P$. □

Definition-Proposition 3.10. *Consider the set $R \times W$ under the following equivalence relation. $(r, w) \sim (r', w')$ if there exists $v \in W$ such that $rw'v = r'wv$. We denote the equivalence classes under this operation by $W^{-1}R$. For simplicity, we write $[(r, w)] \in W^{-1}R$ as r/w.*

Then $W^{-1}R$ is a ring with the following addition and multiplication.

$$\begin{aligned}(r/w) + (r'/w') &= \tfrac{rw'+r'w}{ww'}\\ (r/w) \cdot (r'/w') &= \tfrac{rr'}{ww'}\end{aligned}$$

Furthermore, there is a canonical ring homomorphism $\ell : R \longrightarrow W^{-1}R$ which sends r to $r/1$.

Proof. This is an exercise for the reader. □

Obviously if R is an integral domain and $W = R \setminus \{0\}$ then $W^{-1}R$ is a field, the smallest field containing R (up to isomorphism).

4. Wednesday, September 4th

We make a couple trivial (but useful) observations.

Lemma 4.1. (a) *An element $r/w \in W^{-1}R$ is equal to $0 = 0/1$ if and only if there exists $v \in W$ such that $vr = 0$.*

(b) *If an element $r/w \in W^{-1}R$ is equal to $1 = 1/1$, then $vr \in W$ for some $v \in W$.*

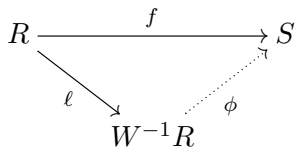
Proof. For (a), if $r/w = 0/1$, then there exists $v \in W$ such that $vr = 0w = 0$. The converse reverses this. For (b), if $r/w = 1$, then $vr = vw \in W$ for some $v \in V$. □

Example 4.2. The map $\ell : R \longrightarrow W^{-1}R$ need not be injective in general. For instance, if $0 \in W$, then $W^{-1}R$ is the zero ring.

For a slightly more interesting example, set $R = k[x, y]/\langle xy \rangle$ and fix $W = \{1, x, x^2, x^3, \ldots\}$. Then observe that $y/1 = 0 \in W^{-1}R$ since $xy = 0 \cdot 1$. It is in fact possible to show that $W^{-1}R = k[x, x^{-1}]$.

Example 4.3. If R is an integral domain and $f \in R$ is non-zero, the $W^{-1}R = R[f^{-1}] = R[x]/\langle xf - 1 \rangle$. Hopefully you proved that this is true on the homework.

Theorem 4.4 (Universal property of localization)**.** *Suppose that R is a ring, W is a multiplicative set and $f : R \longrightarrow S$ is a ring homomorphism such that $f(w)$ is invertible in S for each $w \in W$. Then there is a unique factorization of f making the diagram commute:*



Proof. We prove the existence of such a factorization. Obviously we want $\phi(x/w) = f(x)/f(w)$. There is the question of whether or not this is well defined, so suppose that $x/w = x'/w'$ so that $vxw' = vx'w$ for some $v \in V$. Then $f(v)f(x)f(w') = f(v)f(x')f(w)$ and so since $f(v), f(w)$ and $f(w')$ are invertible, we see that

$$f(x)/f(w) = f(x')/f(w')$$

which proves that ϕ is well defined. □

Let us now describe what localization does to extension of ideals.

Lemma 4.5. *Suppose that $I \subseteq R$ is an ideal and $W \subseteq R$ is a multiplicative set. Then we can characterize the extension*

$$I(W^{-1}R) = \{x/w \in W^{-1}R \mid x \in I\}$$

Proof. Obviously the containment $\supseteq$ holds since $(x/1) \cdot (1/w) \in I(W^{-1}R)$ for all $x \in I$ and $w \in W$. For the reverse containment, suppose that

$$\sum_i^n (x_i/1) \cdot (1/w_i) \in I(W^{-1}R)$$

is an arbitrary element. But

$$\sum_{i=1}^{n}(x_i/1)\cdot(1/w_i)=\frac{\sum_{i=1}^{n}x_i\widehat{w_i}}{\prod_{i=1}^{n}w_i}\in\{x/w\in W^{-1}R\mid x\in I\}.$$

□

Localization has a very controllable impact on the prime spectrum.

Proposition 4.6. *Suppose that R is a ring and $W\subseteq R$ is a multiplicative set. There is a canonical bijection:*

$$\left\{\begin{array}{c}\text{Primes } P\in\operatorname{Spec}R\\ \text{such that } P\cap W=\emptyset.\end{array}\right\}\leftrightarrow\Big\{\text{Primes in } W^{-1}R\Big\}.$$

The bijection is simply

$$P\mapsto P(W^{-1}R).$$

Proof. Suppose P is such that $P\cap W=\emptyset$. First we show that $P(W^{-1}R)$ is prime. Suppose that $(r/w)(r'/w')\in P(W^{-1}R)$. This means that $\frac{rr'}{ww'}\in\{x/w\in W^{-1}R\mid x\in I\}$. Hence $\frac{rr'}{ww'}=x/u$ for some $x\in P$ and $u\in W$. It follows that there exists $v\in W$ such that $uvrr'=vww'x$. In particular, $uvrr'\in P$. But $u,v\notin P$ so $rr'\in P$ so that $r\in P$ or $r'\in P$. In the first case, $r/w\in P(W^{-1}R)$ and in the second $r'/w'\in P(W^{-1}R)$. This proves that $P(W^{-1}R)$ is prime or equal to $W^{-1}R$. Finally, if $1=1/1\in P(W^{-1}R)$ then $vx\in W$ for some $v\in W$ and $x\in P$, which is impossible because $vx\in P$ since P is prime.

Now suppose that $Q\subseteq W^{-1}R$ is prime, set $P=\ell^{-1}(Q)$, a prime in R. We will show that $P(W^{-1}R)=Q$ which will show that our proposed bijection is at least surjective. Certainly $P(W^{-1}R)\subseteq Q$ so now choose $x/w\in Q\subseteq W^{-1}R$. Then $(w/1)(x/w)=x/1\in Q$ and so $x\in P$. Hence $x/w\in P(W^{-1}R)$ which proves the other containment.

Finally, we prove injectivity. Suppose $P,P'\in\operatorname{Spec}R$ both have trivial intersection with W and that $P(W^{-1}R)=P'(W^{-1}R)$. In particular, for every $x\in P$, there exists $x'\in P'$ and $w'\in W$ such that $x/1=x'/w'$. Then $vw'x=vx'$ for some $v\in W$ and so $vw'x\in P'$. Note that then $x\in P'$ since $vw'\in W$ and so not in P'. This proves that $P\subseteq P'$ which completes the proof by symmetry. □

Corollary 4.7. *The primes of R that do not contain $x\in R$ are in bijective correspondence with the primes of $R_x=\{1,x,x^2,\ldots\}^{-1}R$. In other words,* $\operatorname{Spec}R_x$ *corresponds to* $(\operatorname{Spec}R)\setminus V(x)$.

Example 4.8. Suppose that R is a ring and $\langle x_1,x_2,\ldots\rangle=I\subseteq R$ is an ideal. We know $Z=V(I)$ is a closed subset of $X=\operatorname{Spec}R$ so that $X\setminus Z$ is open. It turns out that $X\setminus Z$ is covered by *affine* charts, $X_i=\operatorname{Spec}\{1,x_i,x_i^2,\ldots\}^{-1}R=\operatorname{Spec}R_{x_i}$ for each i, here $X_i=X\setminus V(x_i)$. Indeed, suppose that $P\in X=\operatorname{Spec}R$. If P is in $Z=V(I)$, then P contains each

x_i, and so it does not correspond to any point in any of the X_i by Proposition 4.6. On the other hand, if P is not in Z, then P does not contain some x_i, and so P corresponds to a point in X_i.

Note that $X_i \cap X_j$ corresponds to $\mathrm{Spec}\{1, x_i x_j, x_i^2 x_j^2, \ldots\}^{-1} R$.

Example 4.9. Suppose that $P \subseteq R$ is a prime ideal and set $W = R \setminus P$. Then $W^{-1}R$ has a unique maximal prime ideal, $P(W^{-1}R)$. In this case, $W^{-1}R$ is denoted by R_P.

Definition 4.10. A *local ring* is a ring with a unique maximal ideal. For example each R_P is a local ring.

Geometrically, local rings some how contain only the data of functions passing through the unique maximal ideal (which is a point in the Spec).

5. Friday, September 6th

5.1. **Modules, localization of modules, and tensor products.** We begin by introducing tensor products. Suppose that R is a ring and that M and N are R-modules.

Suppose we wish to multiply elements of m and n, formally, and consider the resulting as an R-module. The tensor product lets us do exactly that. In particular, the tensor product $M \otimes_R N$ is generated by elements $m \otimes n$. Note that in order for it to be a module, it has to be closed under addition, and so we

(i) have to allow finite sums $\sum_{i=1}^{t} m_i \otimes n_i$.

We also want our multiplication to be distributive, and so we must have

(ii) $(m + m') \otimes n = m \otimes n + m' \otimes n$ and $m \otimes (n + n') = m \otimes n + m \otimes n'$.

Finally, we need to describe our action of R on this product. We have

(iii) $(rm) \otimes n = m \otimes (rn) = r.(m \otimes n)$. In other words, only elements of R can move over the tensor product.

Elements of r of course must also distribute across sums:

(iv) $r. \sum_{i=1}^{t} m_i \otimes n_i = \sum_{i=1}^{t} (rm_i) \otimes n_i$

Formally, the tensor product $M \otimes_R N$ is the free Abelian group generated by all ordered pairs $m \otimes n := (m, n) \in M \times N$ modulo the relations generated by properties (ii) and (iii) above. It is an R-module if one distributes R across sums linearly as in (iv).

Proposition 5.1 (Universal property of the tensor product)**.** *If $f : M \oplus N \longrightarrow L$ is a bilinear map of R-modules, then then there exists a unique R-linear $\phi : M \otimes N \longrightarrow L$ such that $\phi(m \otimes n) = f(m, n)$. Note that the obvious map $M \oplus N \longrightarrow M \otimes N$ is bi-linear.*

Now suppose that $N = S$ is an R-algebra (a ring with map $R \longrightarrow S$). Then we will frequently form the tensor product $M \otimes_R S$. This is both an R-module and an S-module (S acts on S and extends linearly).

Definition 5.2 (Localization of a module)**.** Suppose now that R is a ring, W is a multiplicative system and M is an R-module. Then the localization $W^{-1}M$ is the set of pairs $(m,w) \in M \times W$ modulo the equivalence relation $(m,w) \sim (m',w')$ if there exists $v \in W$ such that $vw'm = vwm'$. Equivalence classes $[(m,w)]$ are denoted by m/w. $W^{-1}M$ becomes a $W^{-1}R$-module with the following addition and $W^{-1}R$-action.

$$\begin{array}{rcl} m/w + m'/w' & = & \frac{w'm+wm'}{ww'} \\ (r/w).(m/w') & = & rm/(ww') \end{array}$$

Proposition 5.3. *Suppose R is a ring, M is an R-module and W is a multiplicative system. Then:*

$$W^{-1}R \otimes_R M \cong W^{-1}M.$$

even as $W^{-1}R$-modules.

6. Monday, September 9th

Proof of Proposition 5.3. The tensor product $W^{-1}R \otimes_R M$ is very simple as tensor products go. Indeed, notice that

$$\begin{array}{rl} & (r/w \otimes m) + (r'/w' \otimes m') \\ = & (\frac{rw'}{ww'} \otimes m) + (\frac{r'w}{ww'} \otimes m') \\ = & (\frac{1}{ww'} \otimes (rw'm)) + (\frac{1}{ww'} \otimes (r'wm')) \\ = & \frac{1}{ww'} \otimes (rw'm + r'wm'). \end{array}$$

It follows that every element of $W^{-1}R \otimes_R M$ can be expressed as $\frac{1}{w} \otimes m$. Since it is easy to see that the map $W^{-1}R \oplus M \longrightarrow W^{-1}M$, $(r/w, m) \mapsto rm/w$ is bilinear, by the universal property of the tensor product, we have a map

$$\phi : W^{-1}R \otimes M \longrightarrow W^{-1}M.$$

We need to show it is an isomorphism. Certainly it is surjective, so now choose $\frac{1}{w} \otimes m \in W^{-1}R$ and suppose that $\phi(\frac{1}{w} \otimes m) = m/w = 0$. Hence there exists $v \in W$ such that $vm = 0$. But then

$$\frac{1}{w} \otimes m = \frac{v}{wv} \otimes m = \frac{1}{wv} \otimes vm = \frac{1}{wv} \otimes 0 = 0.$$

Checking that the map is a $W^{-1}R$-module homomorphism is routine and will be left to the reader. □

There is one really useful fact about localization of modules.

Lemma 6.1. *Suppose that $\phi : M \longrightarrow N$ is an injective map of R-modules and $W \subseteq R$ is a multiplicative system, then the induced map*

$$\phi' : W^{-1}M \longrightarrow W^{-1}N$$

is also injective. Equivalently the induced map, $W^{-1}R \otimes_R M \longrightarrow W^{-1}R \otimes_R N$ is injective.

Proof. Ok, what do I mean by ϕ'? $\phi'(m/w) = \phi(m)/w$ (what else could it be?) Suppose that $\phi'(m/w) = \phi(m)/w = 0$. Hence there exists $v \in W$ such that $v\phi(m) = 0$. But $v\phi(m) = \phi(vm)$ so that $vm = 0$ since ϕ is injective. But then $0 = m/v \in W^{-1}M$. □

It is actually really uncommon that tensoring preserves injectivity (as we'll see in the next section). Modules L such that if $M \longrightarrow N$ is injective, then so is $L \otimes M \longrightarrow L \otimes N$ are called *flat*. Thus $W^{-1}R$ is a flat R-module.

What we have just done is a great example of a special type of tensor product called *extension of scalars*. Suppose M is an R-module, $R \longrightarrow S$ is a ring homomorphism, and we really want to make M into an S-module. The most obvious thing to do is $M \otimes_R S$. Then S can act on this tensor product on the right. For example, $\mathbb{R}[x] \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{C}[x]$. Likewise $\mathbb{Z}[x] \otimes_{\mathbb{Z}} (\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})[x]$.

7. On the geometry of tensor products

Theorem 7.1. *Suppose that k is an algebraically closed field, and that R and S are two finite generated k algebras (in other words, $R = k[x_1, \ldots, x_m]/I$ and $S = k[y_1, \ldots, y_n]/J$. Then there is a natural bijection between m-Spec $R \otimes_k S$, the maximal ideals of the ring $R \otimes_k S$, with $(m\text{-Spec } R) \times (m\text{-Spec } S)$.*

Proof. Consider maps $f : R \longrightarrow R \otimes_k S$ and $g : S \longrightarrow R \otimes_k S$ which sends $r \mapsto r \otimes 1$ and $s \mapsto 1 \otimes s$ respectively. This gives us a map $(f^\# \times g^\#) : \text{m-Spec}(R \otimes_k S) \longrightarrow (\text{m-Spec } R) \times (\text{m-Spec } S)$. We will call this map φ. We need to show it is bijective. We will use the letter A to denote the ring $R \otimes_k S$.

First we prove a lemma.

Lemma 7.2. *If $\mathfrak{m}$ is a maximal ideal of R and $\mathfrak{n}$ is a maximal ideal of S, then $\mathfrak{c} := \langle f(\mathfrak{m})\rangle + \langle g(\mathfrak{n})\rangle = \mathfrak{m}A + \mathfrak{n}A$ is a maximal ideal of A.*

Proof. Consider the map $f : R \longrightarrow A$ and apply the functor $R/\mathfrak{m} \otimes_R \bullet$, we obtain

$$f' : R/\mathfrak{m} \longrightarrow R/\mathfrak{m} \otimes_R (R \otimes_k S) \cong (R/\mathfrak{m} \otimes_R R) \otimes_k S \cong R/\mathfrak{m} \otimes_k S \cong S \cong A/(\mathfrak{m}A)$$

This map is injective because S is a free k-module (in fact every module over a vector space is free). Now consider the map $\rho \circ g : S \longrightarrow A \longrightarrow A/(\mathfrak{m}A)$ which is an isomorphism by above and tensor with $\bullet \otimes_S S/\mathfrak{n}$ and obtain the isomorphism

$$g'' : S/\mathfrak{n} \xrightarrow{\overline{\rho \circ g}} A/(\mathfrak{m}A) \otimes_S S/\mathfrak{n} \cong (R/\mathfrak{m} \otimes_k S/\mathfrak{n}) \cong k \cong A/(\mathfrak{m}A + \mathfrak{n}A)$$

Thus $A/(\mathfrak{m}A + \mathfrak{n}A)$ is a field and so $\mathfrak{m}A + \mathfrak{n}A$ is maximal. Now we return to our main proof. □

We continue our proof of Theorem 7.1. We first prove the injectivity so suppose that $\mathfrak{a}$ and $\mathfrak{b}$ are maximal ideals of $R \otimes_k S$ and that $\varphi(\mathfrak{a}) = \varphi(\mathfrak{b})$ (so $f^{-1}(\mathfrak{a}) = f^{-1}(\mathfrak{b})$ and likewise $g^{-1}(\mathfrak{a}) = g^{-1}(\mathfrak{b})$). Consider the ideal $\langle f(f^{-1}(\mathfrak{a}))\rangle + \langle g(g^{-1}(\mathfrak{a}))\rangle = \langle f(f^{-1}(\mathfrak{b}))\rangle + \langle g(g^{-1}(\mathfrak{b}))\rangle$. This is a maximal

ideal, by the Lemma, contained inside both $\mathfrak{a}$ and $\mathfrak{b}$ and so the injectivity of φ is done.

Now we prove the surjectivity of φ. But this is easy since given $\mathfrak{m}$ and $\mathfrak{n}$ and constructing $\mathfrak{c}$ as in the lemma, it is clear that $f^{-1}(\mathfrak{c}) \supseteq \mathfrak{m}$ (and so we must have equality) and likewise for $\mathfrak{n}$. □

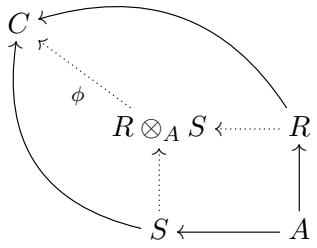
Example 7.3. When not working of finite type over an algebraically closed field, the above theorem fails. For example, $\mathbb{C}$ is a finitely generated $\mathbb{R}$-module, and $\operatorname{Spec}\mathbb{C}$ is a singleton. However, $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ has two points in its prime spectrum (this kind of behavior can also happen in number theoretic settings).

Example 7.4. $k[x] \otimes_k k[y] \cong k[x,y]$ (this is easy to see explicitly as well). Note that the Cartesian product only works for the maximal ideals.

8. Monday, September 16th

We have a universal property for a tensor product of rings as well.

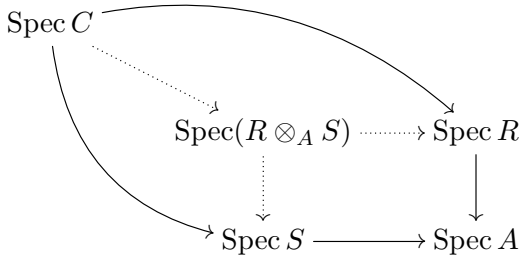
Proposition 8.1. *Suppose that A is a ring and that R and S are A-algebras (rings with maps $A \longrightarrow R$, $A \longrightarrow S$). Then for every other ring C with maps $f : R \longrightarrow C$ and $g : S \longrightarrow C$ making the diagram commute*



there exists a unique map of rings ϕ as above making the diagram commute.

Proof. This follows easily from the other universal (bilinear) property for modules we already mentioned. □

If we dualize the diagram, we have the following picture.



The dual of the universal property is exactly the universal property of the fiber product for topological spaces (this works well for the $\mathfrak{m}$-Spec when we are finite type over an algebraically closed field A, in which case the fiber product is all pairs whose image is the same in $\operatorname{Spec} A$).

8.1. **Exactness of tensor products and the** Hom **functor.** We have just seen that localization of modules (ie tensoring with the localized ring) preserve injectivities of modules. This is *NOT* true for arbitrary tensor products.

Example 8.2. Indeed, consider the injection $\mathbb{Z} \xrightarrow{\times 2} \mathbb{Z}$ and let us tensor it with $\otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$. Then we have the map

$$\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} \xrightarrow{(\times 2)\otimes(\mathrm{id})} \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}. \tag{8.2.1}$$

Note that first $\mathbb{Z}\otimes_{\mathbb{Z}}\mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z}$. Let's convince ourselves of this explicitly, indeed each $a\otimes b = 1\otimes ab$ and so we can represent each element of the tensor as an element of $\mathbb{Z}/2\mathbb{Z}$. Of course, there is a surjective map $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z}$ (coming from the universal property of the tensor product) and the isomorphism follows.

We return to the map and observe that $1 \otimes 1$ is sent to $2 \otimes 1 = 1 \otimes 2 = 1 \otimes 0 = 0$. In particular, the map from (8.2.1) is the zero map and hence not injective.

Tensor products do preserve a lot of other properties though.

Definition 8.3 (Short exact sequences)**.** Suppose that L, M, N are R-modules. A *short exact sequence*, denoted

$$0 \longrightarrow L \xrightarrow{\phi} M \xrightarrow{\psi} N \longrightarrow 0$$

is a pair of maps $\phi : L \longrightarrow M$ and $\psi : M \longrightarrow N$ such that ϕ is injective, ψ is surjective and $\ker \psi = \operatorname{im} \phi$.

For example, $0 \longrightarrow \mathbb{Z} \xrightarrow{\times 2} \mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$ is a short exact sequence.

Example 8.4. The canonical example of a short exact sequence comes from picking $I \subseteq R$ an ideal and forming:

$$0 \longrightarrow I \longrightarrow R \longrightarrow R/I \longrightarrow 0.$$

Short exact sequences are special cases of exact sequences.

Definition 8.5 (Complexes Exact sequence)**.** Suppose that $\{C_i\}$ is a collection of R-modules with maps $C_i \xrightarrow{\phi_i} C_{i+1}$, written diagrammatically as:

$$\ldots \xrightarrow{\phi_{i-2}} C_{i-1} \xrightarrow{\phi_{i-1}} C_i \xrightarrow{\phi_i} C_{i+1} \xrightarrow{\phi_{i+1}} C_{i+2} \xrightarrow{\phi_{i+2}} \ldots$$

This is called a (cochain) complex if $\ker \phi_i \supseteq \operatorname{im} \phi_{i-1}$ for all i. It is called an *exact sequence* if $\ker \phi_i = \operatorname{im} \phi_{i-1}$ for all i.

As we have already seen, tensor products do not preserve exact sequences (since they don't preserve injections, which can be written as exact sequences $0 \longrightarrow M \longrightarrow N$). However, the following is true.

9. Tuesday, September 17th

Proposition 9.1. *If $0 \longrightarrow L \xrightarrow{a} M \xrightarrow{b} N \longrightarrow 0$ is an exact sequence and T is another R-module, then*

$$L \otimes_R T \xrightarrow{\alpha} M \otimes_R T \xrightarrow{\beta} N \otimes_R T \longrightarrow 0$$

is also exact.

This proposition asserts that $\otimes$ is *right-exact* (it takes short exact sequences to sequences that are exact on the right).

Proof. It is easy to see that β is surjective, indeed if $n \otimes t \in N \otimes T$, then since $M \longrightarrow N$ is surjective, there exists $m \in M$ such that $b(m) = n$. Hence $m \otimes t \mapsto n \otimes t$ and it follows that β surjects.

We now need to show that $\ker \beta = \operatorname{im} \alpha$. Let $C = \operatorname{im} \alpha$, we already know that $C \subseteq \ker \beta$ and so we have a map $\gamma : (M \otimes_R T)/C \longrightarrow N \otimes_R T$. It is sufficient to show that this map is injective. Define a map

$$\sigma : N \otimes_R T \longrightarrow (M \otimes_R T)/C$$

by $n \otimes t \mapsto \overline{b_1(n) \otimes t}$ where $b_1(n)$ is *any* $m \in M$ with $b(m) = n$ and $\overline{\bullet}$ denotes the image after modding out by C. We need to show that σ is well defined. Suppose that m and m' are such that $b(m) = b(m') = n$ then we need to show that $\overline{m \otimes t} = \overline{m' \otimes t}$ (this is the same as showing that the obvious bi-linear map from the universal property is well defined). But since $b(m) = b(m')$, there exists $l \in L$ such that $a(l) = m - m'$. Therefore since $a(l) \otimes t \in C$, we see that $\overline{(m - m') \otimes t} = 0$ and $\overline{m \otimes t} = \overline{m' \otimes t}$. This shows σ is well defined. Now, $(M \otimes_R T)/C \xrightarrow{\gamma} N \otimes_R T \xrightarrow{\sigma} (M \otimes_R T)/C$ sends $\overline{m \otimes t}$ back to itself. It follows that γ is injective. □

We'll see another proof later once we understand the relation of $\otimes$ with Hom. Indeed, at least as fundamental as the $\otimes$ functor is the Hom functor. Suppose that M, N are R-modules. Then $\operatorname{Hom}_R(M, N)$ is the set of R-module homomorphisms $M \longrightarrow N$. It is an R-module since $r.\phi$ is defined by $(r.\phi)(m) = r\phi(m) = \phi(rm)$. In other words, r can act on either the domain or the codomain, it doesn't matter. Now suppose that $\eta : L \longrightarrow M$ is a module homomorphism. Then we have an induced R-module homomorphism:

$$\Phi : \operatorname{Hom}_R(M, N) \longrightarrow \operatorname{Hom}_R(L, N)$$

defined by $\big(\Phi(f)\big)(l) = f(\eta(l))$.

On the other and, of $\delta : N \longrightarrow O$ is an R-module homomorphism, then obtain:

$$\Psi : \operatorname{Hom}_R(M, N) \longrightarrow \operatorname{Hom}_R(M, O)$$

which is defined by $\big(\Phi(f)\big)(m) = \delta(f(m))$.

Proposition 9.2. *The functors* $\mathrm{Hom}_R(\bullet, N)$ *and* $\mathrm{Hom}_R(M, \bullet)$ *are both left-exact. In other words, if*

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

is an exact sequence of R*-modules, then*

$$0 \longrightarrow \mathrm{Hom}_R(C, N) \xrightarrow{g'} \mathrm{Hom}_R(B, N) \xrightarrow{f'} \mathrm{Hom}_R(A, N)$$

is exact and

$$0 \longrightarrow \mathrm{Hom}_R(M, A) \xrightarrow{f''} \mathrm{Hom}_R(M, B) \xrightarrow{g''} \mathrm{Hom}_R(M, C)$$

is also exact.

Proof. For the first sequence we handle the injectivity of g' first. Suppose that $\phi \in \mathrm{Hom}_R(C, N)$ and that $B \xrightarrow{g} C \xrightarrow{\phi} N$ is zero (ie, the image of ϕ in $\mathrm{Hom}_R(B, N)$ is zero). But then since g is surjective, we must have ϕ zero as well. Next we handle $\ker f' \subseteq \mathrm{im}\, g'$. Suppose that $\psi \in \mathrm{Hom}_R(B, N)$ is such that $A \xrightarrow{f} B \xrightarrow{\psi} N$ is zero so that there is $\overline{\psi} : C \cong B/A \longrightarrow N$. Consider the composition $B \xrightarrow{g} B/A \xrightarrow{\overline{\psi}} N$, obviously this is the same as ψ and so $g'(\overline{\psi}) = \psi$ which shows that $\ker f' \supseteq \mathrm{im}\, g'$. Finally we need to show $\ker f' \supseteq \mathrm{im}\, g'$. Choose $\theta \in \mathrm{Hom}_R(C, N)$ and consider $g'(\theta) = \theta \circ g \in \mathrm{Hom}_R(B, N)$. Finally we consider $f'(g'(\theta)) = \theta \circ g \circ f \in \mathrm{Hom}_R(A, N)$. But $g \circ f$ is zero, and thus so is $f'(g'(\theta))$.

We now consider the second exact sequence. First suppose that $\phi \in \mathrm{Hom}_R(M, A)$, then $f''(\phi) = f \circ \phi$, ie $M \xrightarrow{\phi} A \xrightarrow{f} B$. Since f is injective, if ϕ is nonzero, then $f \circ \phi = f''(\phi)$ is also nonzero. Next we show that $\mathrm{im}\, f'' \subseteq \ker g''$. Suppose that $\phi \in \mathrm{Hom}_R(M, A)$, then $f''(\phi) = f \circ \phi$. $g''(f''(\phi)) = g \circ f \circ \phi$. Since $g \circ f = 0$, $g''(f''(\phi)) = 0$ which proves what we wanted. Finally we show that $\ker g'' \subseteq \mathrm{im}\, f''$. Suppose $\psi \in \mathrm{Hom}_R(M, B)$ is such that $g''(\psi) = g \circ \psi = 0$. In other words

$$M \xrightarrow{\psi} B \xrightarrow{g} C$$

is zero. Since the kernel of g is equal to $f(A)$, we see that $\psi(M) \subseteq f(A)$. But f is injective and so we have a factorization of ψ

$$\psi : M \xrightarrow{\eta} A \xrightarrow{f} B.$$

But then $\psi = f''(\eta)$ which completes the proof. □

Remark 9.3. Note that in the first part of the proof, we didn't need that f was injective. In the second, we didn't need that g was surjective.

10. Wednesday, September 18th

Example 10.1. We compute some Homs, first over the ring $\mathbb{Z}$. Then

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Z}) = 0$$

since if $\phi(a/b) \neq 0$, then $\phi(c \cdot (a/b)) = c\phi(a/b)$ where all terms are integers. This yields a contradiction if $\gcd(b,c) = 1$ with $b > 1$.

Also note that

$$\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/5, \mathbb{Z}) = 0$$

since the image of any such homomorphism is a finite subgroup of $\mathbb{Z}$, and the only such subgroup is $\{0\}$.

Now we work over a polynomial ring, $R = k[x,y]$. First observe that

$$\operatorname{Hom}_R(\langle x, y\rangle, \langle x, y\rangle)$$

contains the identity morphism, and all multiples of this morphism. It turns out these are the only ones (which can be verified via Macaulay2, or cleverness). In class, we verified that we can't send $x \mapsto y$ and $y \mapsto x$ and keep it a R-module homomorphism since then

$$x^2 = x\phi(y) = \phi(xy) = \phi(yx) = y\phi(x) = y^2.$$

Likewise

$$\operatorname{Hom}_R(\langle x, y\rangle, R) \cong R$$

where the inclusion homomorphism is sent to 1 (and all the others are just multiples of it).

Finally,

$$\operatorname{Hom}_R(R/\langle x, y\rangle, R) = \{0\}$$

since if $z \in R/\langle x, y\rangle, R) \cong k$ is such that $\phi(z) \neq 0$, then $0 \neq x\phi(z) = \phi(x.z) = 0$ since $xz \in \langle x, y\rangle$.

Proposition 10.2. *A sequence $A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ is exact if and only if*

$$0 \longrightarrow \operatorname{Hom}_R(C,N) \xrightarrow{g'} \operatorname{Hom}_R(B,N) \xrightarrow{f'} \operatorname{Hom}_R(A,N)$$

is exact for every R-module N.

Likewise, $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C$ is exact if and only if

$$0 \longrightarrow \operatorname{Hom}_R(M,A) \xrightarrow{f''} \operatorname{Hom}_R(M,B) \xrightarrow{g''} \operatorname{Hom}_R(M,C)$$

is exact for every R-module M.

Proof. We have already done both of the ($\Rightarrow$) directions. So first suppose that $0 \longrightarrow \operatorname{Hom}_R(C,N) \xrightarrow{g'} \operatorname{Hom}_R(B,N) \xrightarrow{f'} \operatorname{Hom}_R(A,N)$ is exact for every R-module N. Set N to be the quotient module $C/g(B)$ and let $\psi : C \longrightarrow N$ be the canonical surjection. If g is not surjective, then ψ is nonzero and hence $g'(\psi) = \psi \circ g$ is non-zero (but that obviously is zero).

Next suppose that $\ker f' = \operatorname{im} g'$ for every N. We'd like to show that $\ker g = \operatorname{im} f$ as well. Since $f' \circ g' = 0$, by setting $N = C$ we have $f' \circ g' \circ \mathrm{id}_C = 0$. But this is just $g \circ f$. Finally, set $N = B/\operatorname{im}(A)$. Then suppose that $\phi \in \operatorname{Hom}_R(B, B/\operatorname{im}(A))$ satisfies $f'(\phi) = \phi \circ f' = 0$. In other words

$$A \xrightarrow{f} B \xrightarrow{\phi} B/\operatorname{im}(A)$$

is the zero map. Then there exists $\overline{\phi} : C \cong B/\operatorname{im}(A) \longrightarrow B/\operatorname{im}(A)$ factoring ϕ. It is easy to see that $g'(\overline{\phi}) = \phi$ which completes this part of the proof.

For the second part the proof is much easier, we begin by setting $M = R$, then the exact sequence of Homs becomes simply $0 \longrightarrow A \longrightarrow B \longrightarrow C$ which is also exact. □

We spent the rest of the time in Macaulay2.

11. Friday, September 18th

The functors of Hom and tensor are closely related.

Theorem 11.1 (Hom $-\otimes$ adjointness)**.** *If L, M, N are R-modules, then there is an R-module isomorphism:*

$$\operatorname{Hom}_R(L \otimes_R M, N) \cong \operatorname{Hom}_R(L, \operatorname{Hom}_R(M, N))$$

Proof. Given $\phi \in \operatorname{Hom}_R(L, \operatorname{Hom}_R(M, N))$ we need to construct $\Phi(\phi) \in \operatorname{Hom}_R(L, \operatorname{Hom}_R(M, N))$. We an action of ϕ on elements of $L \otimes_R M$. Given $\sum l_i \otimes m_i$ we define

$$\phi(\sum l_i \otimes m_i) = \sum (\phi(l_i))(m_i)$$

Note that each $\phi(l_i) \in \operatorname{Hom}_R(M, N)$ so it makes perfect sense to act upon m_i. Thus we have defined Φ.

To go the other way, suppose that $\psi \in \operatorname{Hom}_R(L \otimes_R M, N)$, and we will define $\Psi(\psi) \in \operatorname{Hom}_R(L, \operatorname{Hom}_R(M, N))$. So choose $l \in L$. Then $\Psi(\psi)(l) = \psi(l \otimes \_\_)$ where the blank is to be filled in from M.

We should verify that $\Psi \circ \Phi$ and $\Phi \circ \Psi$ are the identities. But I will leave this to you (I think we'll do one direction as a class). □

Now we discuss a proof of the right exactness of $\otimes$ via the left exactness of Hom.

Lemma 11.2. *$\otimes_R M$ is right exact for any R-module M.*

Proof. We suppose that $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ is exact and we want to show that

$$A \otimes_R M \longrightarrow B \otimes_R M \longrightarrow C \otimes_R M \longrightarrow 0$$

is exact. It is sufficient to show that

$$0 \longrightarrow \operatorname{Hom}_R(C \otimes_R M, N) \longrightarrow \operatorname{Hom}_R(B \otimes_R M, N) \longrightarrow \operatorname{Hom}_R(A \otimes_R M, N)$$

is exact for any R-module N. But that is exact if and only if

$$0 \longrightarrow \operatorname{Hom}_R(M, \operatorname{Hom}_R(C, N)) \longrightarrow \operatorname{Hom}_R(M, \operatorname{Hom}_R(B, N)) \longrightarrow \operatorname{Hom}_R(M, \operatorname{Hom}_R(A, N))$$

is exact by the adjointness of tensor and Hom (we also need to know that the adjointness isomorphism is compatible with morphisms in the M variable, but it is, I won't check it though). But this is exact if

$$0 \longrightarrow \operatorname{Hom}_R(C, N) \longrightarrow \operatorname{Hom}_R(B, N) \longrightarrow \operatorname{Hom}_R(A, N)$$

is exact, which follows if $A \longrightarrow B \longrightarrow C \longrightarrow 0$ is exact (which it is). □

Finally, I want to explain a key relation between tensor and Hom. Suppose that M, N, L are R-modules. Then it is easy to see that there is an R-module homomorphism

$$\mathrm{Hom}_R(M,N) \longrightarrow \mathrm{Hom}_R(M \otimes_R L, N \otimes_R L),$$

simply send $(\phi : M \longrightarrow N) \otimes l$ to the induced morphism $M \otimes_R L \longrightarrow N \otimes_R L$. In general this is not an isomorphism. There is another key variant of this, suppose that L is now an R-algebra, then

$$M \otimes_R L \longrightarrow N \otimes_R L$$

is a map of L-modules. In particular, we get a map

$$\mathrm{Hom}_R(M,N) \longrightarrow \mathrm{Hom}_L(M \otimes_R L, N \otimes_R L).$$

If we tensor the left side of the map by L, we get an L-linear map

$$\mathrm{Hom}_R(M,N) \otimes L \longrightarrow \mathrm{Hom}_L(M \otimes_R L, N \otimes_R L).$$

Definition 11.3. Recall an R-module L is called flat if $\bullet \otimes_R L$ is an exact functor (ie, it preserve injectivity). Remember $W^{-1}R$ is a flat R-module for any multiplicative set W.

Proposition 11.4. *If M is a finitely presented R-module (meaning it can be generated by finitely many elements subject to finitely many relations), N is any R-module and S is a flat R-algebra (in particular, it is an R-algebra which is flat as an R-module), then*

$$\mathrm{Hom}_R(M,N) \otimes_R S \longrightarrow \mathrm{Hom}_S(M \otimes_R S, N \otimes_R S)$$

is an isomorphism.

Proof. Since M is finitely presented, we can write an exact sequence

$$R^m \longrightarrow R^n \longrightarrow M \longrightarrow 0$$

Since S is flat, the functors $\mathrm{Hom}_R(\bullet, N) \otimes_R S$ and $\mathrm{Hom}_R(\bullet \otimes_R S, N \otimes_R S)$ are both left-exact. Hence we have the following diagram

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{Hom}_R(M,N) \otimes_R S & \longrightarrow & \mathrm{Hom}_R(R^m,N) \otimes_R S & \longrightarrow & \mathrm{Hom}_R(R^m,N) \otimes_R S \\
 & & \downarrow f & & \downarrow g & & \downarrow h \\
0 & \longrightarrow & \mathrm{Hom}_S(M \otimes_R S, N \otimes_R S) & \longrightarrow & \mathrm{Hom}_S(R^m \otimes_R S, N \otimes_R S) & \longrightarrow & \mathrm{Hom}_S(R^n \otimes_R S, N \otimes_R S) \\
 & & \updownarrow \sim & & \updownarrow \sim & & \updownarrow \sim \\
0 & \longrightarrow & \mathrm{Hom}_S(M \otimes_R S, N \otimes_R S) & \longrightarrow & \mathrm{Hom}_S(S^m, N \otimes_R S) & \longrightarrow & \mathrm{Hom}_S(S^n, N \otimes_R S)
\end{array}$$

The bottom row of isomorphisms just comes from the fact that $R^a \otimes_R S = S^a$.

It is now straightforward to verify that the maps g and h are isomorphisms. Indeed, they are both homomorphisms from free modules and so you just need to decide where each basis element goes in each case (note $\mathrm{Hom}_R(R^a, M) = M^a$ as well). It follows that f is an isomorphism as well (it is two different ways to interpret the kernel of the same map). $\square$

12. Monday, September 23rd

Using the fact that localization can be written in terms of (flat) tensor product, we have that:

Corollary 12.1. *Suppose R is a ring, A is a finitely presented R-module and B is any R-module. If $W \subseteq R$ is any multiplicative set, then*

$$W^{-1}\operatorname{Hom}_R(A,B) \cong \operatorname{Hom}_{W^{-1}R}(W^{-1}A, W^{-1}B).$$

12.1. **Nakayama's Lemma.** We now switch gears entirely.

Theorem 12.2 (The determinant trick)**.** *Suppose M is an R-module generated by n-elements and $\phi \in \operatorname{Hom}_R(M,M)$. If $I \subseteq R$ is such that $\phi(M) \subseteq I \cdot M$ then there is a relation of the form*

$$\phi^n + a_1\phi^{n-1} + \cdots + a_{n-1}\phi + a_n \cdot \mathrm{id}_M = 0 \in \operatorname{Hom}_R(M,M) \tag{12.2.1}$$

where $a_i \in I^i$.

Proof. Write $M = \langle m_1, \ldots, m_n \rangle$. We can write each $\phi(m_i) = \sum_{j=1}^n a_{ij}m_j$. In other words:

$$\sum_{j=1}^{n} (\delta_{ij} \cdot \phi - a_{ij} \cdot \mathrm{id}_M)(m_j) = 0 \in M$$

holds for each i (where δ_{ij} is the Kronekcer delta). We view this is a square matrix

$$\Delta = [(\delta_{ij} \cdot \phi - a_{ij} \cdot \mathrm{id}_M)]$$

and note that

$$\Delta \begin{bmatrix} m_1 \\ m_2 \\ \cdots \\ m_n \end{bmatrix} = 0.$$

Let B be the classical adjoint matrix of Δ, and recall that $B\Delta = \det(\Delta) I_{n\times n}$ so that

$$\det(\Delta)(m_j) = 0 \in M$$

for each m_j. Since these generate M we see that $\det(\Delta) = 0 \in \operatorname{Hom}_R(M,M)$. Expanding out the determinant gives the result. □

13. Wednesday, September 25th

We first spent a fair amount of time discussing the homework.

We now prove Nakayama's lemma (in fact, all of the results below are frequently referred to as Nakayama's lemma).

Theorem 13.1 (Nakayama's Lemma 1)**.** *Suppose that R is a ring, $I \subseteq R$ is an ideal and that M is a finitely generated R-module. If $M = I \cdot M$ then there exists $x \in R$ such that $x \cdot m = 0$ for all $m \in M$ and that $x - 1 \in I$.*

Proof. Set $\phi = \mathrm{id}_M$. Then by the determinant trick, $\phi(M) = M \subseteq I \cdot M$ and so there exist $a_i \in I^i$ such that

$$\mathrm{id}_M + a_1 \mathrm{id}_M + \ldots + a_n \mathrm{id}_M = 0$$

In particular, $x = (1 + a_1 + \ldots + a_n)$ kills every element of M. Furthermore, certainly $x - 1 \in I$. □

Corollary 13.2 (Nakayama's Lemma 2)**.** *If R is local, M is an R-module and $I \subsetneq R$ is a proper ideal such that $M = I \cdot M$, then $M = 0$.*

Proof. Since I is proper, $I \subseteq \mathfrak{m}$ where $\mathfrak{m}$ is the unique maximal ideal of R. Since $x - 1 \in \subseteq \mathfrak{m}$, we see that x is not contained in $\mathfrak{m}$ and hence is a unit. But then $xm = 0$ for all $m \in M$ implies that $M = 0$. □

Corollary 13.3 (Nakayama's Lemma 3)**.** *Suppose that $(R, \mathfrak{m})$ is a local ring. If $f : M \longrightarrow N$ is a map of R-modules with N finitely generated. Then f is surjective if and only if the composition*

$$\overline{f} : M \longrightarrow N \longrightarrow N/(\mathfrak{m} \cdot N)$$

is surjective.

14. Friday, September 27th

We prove Nakayama's lemma version 3.

Proof. Certainly if f is surjective so is $\overline{f}$. Conversely suppose that $\overline{f}$. The fact that $\overline{f}$ is surjective implies that $f(M) + (\mathfrak{m} \cdot N) = N$. It follows that $\mathfrak{m} \cdot (N/f(M)) = (\mathfrak{m} \cdot N + f(M))/f(M) = N/f(M)$. Thus $N/f(M) = 0$ and so f is surjective. □

Corollary 14.1 (Nakayama's Lemma 4)**.** *Suppose that $(R, \mathfrak{m}, k = R/\mathfrak{m})$ is a local ring, M is a finite R-module and $\overline{M} = M/(\mathfrak{m} \cdot M)$. Then $\overline{M}$ is a finite dimensional vector space of dimension n. Furthermore,*

(a) *If $\overline{m}_1, \ldots, \overline{m}_n$ are a k-basis for $\overline{M}$, then any set of pre-images $m_1, \ldots, m_n$ form a minimal generating set for M.*
(b) *Every minimal generating set for M is obtained in this way, and so they all have n elements.*

Proof. We begin with the proof of (a). It is easy to see that the m_i are a generating set, indeed consider the map $R^n \longrightarrow M$ which sends e_i to m_i. Then this map is certainly surjective by Nakayama's Lemma 3. We just need to show that this set is minimal. However, if it was not minimal, we could remove an element, and still have a generating set. Without loss of generality let us remove m_n. But then $R^{n-1} \longrightarrow M$ would be surjective and thus so would $k^{n-1} \cong (R/\mathfrak{m})^{n-1} \longrightarrow \overline{M}$, which is impossible since $\overline{M}$ has dimension M.

Now suppose that $m_1, \ldots, m_l$ is another generating set for M with $l > n$ (the case of $l < n$ is ruled out by the argument immediately above). It follows that some set of n elements within $\{\overline{m}_1, \ldots, \overline{m}_l\}$ span $\overline{M}$, say $\overline{m}_1, \ldots, \overline{m}_l$

span the vector space $\overline{M}$. Hence $m_1, \ldots, m_n$ also generate M and so every minimal generating set of M is obtained this way. □

14.1. **Noether normalization and finite extensions.** Our goal is to prove the following theorem.

Theorem (Noether normalization)**.** *Suppose that k is a field and that R is an integral domain which is also a finitely generated k-algebra. Then there exists algebraically independent elements $a_1, \ldots, a_t \in R$ such that $k[a_1, \ldots, a_t] \subseteq R$ is a polynomial ring over k. Furthermore, R is a finitely generated $k[a_1, \ldots, a_t]$-module.*

15. Monday, September 30th

Suppose that R is a ring of finite type over a field. Frequently one wishes that R is a polynomial ring (but we only know it is a quotient of a polynomial ring). One way to try to fix this is with a tool called Noether normalization. First we need a couple definitions.

Definition 15.1. Suppose that elements $r_1, \ldots, r_n$ are elements in a k-algebra R. We say that $\{r_i\}$ are *algebraically independent* if the k-algebra map

$$k[X_1, \ldots, X_N] \longrightarrow R$$

sending X_i to r_i is injective. Less formally, $\{r_i\}$ are algebraically independent if there are no non-trivial relation between them.

Definition 15.2. Suppose that $A \subseteq B$ is an extension of rings. Then we say an element $b \in B$ *is integral over* A if $b^n + a_{n-1}b^{n-1} + \ldots + a_1 b + a_0 = 0$ for some $a_i \in A$. If every element of B is integral over A then we say that B *is integral over* A.

Lemma 15.3. *If $y \in B$ is integral over A, then $A[y]$ is a finitely generated A-module.*

Proof. If the monic relation on y has degree d, then $1, y, \ldots, y^{d-1}$ form a generating set for $A[y]$ over A. □

And now a lemma.

Lemma 15.4. *Suppose that A is a domain and finitely generated k-algebra (generated by $y_1, \ldots, y_n$) is such that for some $0 \neq F \in k[Y_1, \ldots, Y_n]$ we have $F(y_1, \ldots, y_n) = 0$. Then there exist elements $z_1, \ldots, z_{n-1}$ such that y_n is integral over $B = k[z_1, \ldots, z_{n-1}] \subseteq A$ and $A = B[y_n]$.*

Proof. I only prove this claim in the case that k is infinite, for a proof in the general case see any of your usual texts.

We will set $z_i = y_i - \alpha_i y_n$ for some $\alpha_i \in k$ (to be chosen momentarily). Then

$$F(z_1 + \alpha_1 y_1, \ldots, z_{n-1} + \alpha_{n-1} y_{n-1}, y_n) = F(y_1, \ldots, y_n) = 0.$$

Consider the polynomial $G(z_1, \ldots, z_{n-1}, y_n) := F(z_1 + \alpha_1 y_1, \ldots, z_{n-1} + \alpha_{n-1} y_{n-1}, y_n)$. If F has degree d, then

$$G = H(\alpha_1, \ldots, \alpha_{n-1}, 1) y_n^d + \text{lower } y_n\text{-degree terms}.$$

It is easy to see that H is not the zero polynomial.

Claim 15.5. *There exist $\alpha_1, \ldots, \alpha_{n-1}$ such that $H(\alpha_1, \ldots, \alpha_{n-1}, 1) \neq 0 \in k$.*

Proof of claim. We use the fact that k is infinite here and proceed by induction on $n-1$. Write $H(Y_1, \ldots, Y_{n-1}, 1)$ as a polynomial in the variable Y_1,

$$H(Y_1, \ldots, Y_{n-1}, 1) = f_{l_1}(Y_2, \ldots, Y_{n-1}) \cdot Y_1^{l_1} + \ldots + f_0(Y_2, \ldots, Y_{n-1}) \cdot Y_1^0.$$

Note that $f_{l_1}(Y_2, \ldots, Y_{n-1})$ is a polynomial in fewer variables, so by induction for some choice of $Y_2 = \alpha_2, \ldots, Y_{n-1} = \alpha_{n-1}$, this polynomial is non-zero. Choosing these values, we then have a non-zero polynomial in Y_1 which can have at most finitely many root. This allows us to choose $Y_1 = \alpha_1$ as well. This proves the claim. □

We return to the proof of the main theorem. Choosing the α_i as in the claim we then have that

$$G = \lambda y_n^d + \text{lower } y_n\text{-degree terms}$$

for some non-zero $\lambda \in k$. Dividing by λ proves that y_n is integral over $k[z_1, \ldots, z_{n-1}]$. □

Theorem 15.6 (Noether normalization)**.** *Suppose that k is a field and that R is an integral domain which is also a finitely generated k-algebra. Then there exists algebraically independent elements $a_1, \ldots, a_t \in R$ such that $k[a_1, \ldots, a_t] \subseteq R$ is a polynomial ring over k. Furthermore, R is a finitely generated $k[a_1, \ldots, a_t]$-module.*

Proof. Choose $x_1, \ldots, x_n$ to be a generating set for R as a k-algebra. We proceed by induction on n. If $x_1, \ldots, x_n$ are algebraically independent over k, we are done. So we suppose not and apply the lemma. We see that we can choose linear combinations $y_1, \ldots, y_{n-1}, y_n = x_n$ of the x_i so that y_n is integral over $y_1, \ldots, y_{n-1}$. In particular, R is a finite $k[y_1, \ldots, y_{n-1}]$-module. We continue in this way until we end up with an algebraically independent set. Note that a chain of finitely generated modules is a finitely generated module. □

Now, let us talk a little bit more about the formalities of finite maps.

Lemma 15.7. *Suppose that $A \subseteq B$ is a ring extension. Choose $b \in B$. Then b is integral over A if and only if $A[b]$ is a finite b-module. Even more, if B is a finite A-module, then every element of B is integral over A.*

Proof. If b is integral then it satisfies a monic relation $b^n + a_{n-1}b^{n-1} + \ldots + a_0$, and so obviously $b^{n-1}, \ldots, b^1, 1$ generate $A[b]$ as an A-module. Conversely, suppose that B is a finitely generated A-module with n-generators. We need

to show that each $b \in B$ is integral over A. We use the determinant trick. Consider the A-module homomorphism $B \xrightarrow{\times b} B$ which we denote by ϕ. Then we see that the image of this map contains $A \cdot B = B$. Hence there exists $a_1, \ldots, a_n$ such that $\phi^n + a_1\phi^{n-1} + \ldots + a_0 \operatorname{id}_B = 0$. But noting that $\phi = b \cdot \operatorname{id}_B$, we can factor out id_B and so obtain

$$\left(b^n + \ldots + a_1 b^1 + a_0\right) \operatorname{id}_B = 0 \in \operatorname{Hom}_A(B, B).$$

But then $b^n + \ldots + a_1 b^1 + a_0 = 0 \in B$, which proves the theorem. □

Lemma 15.8. *Suppose $A \subseteq B$ is a ring extension and that $C \subseteq B$ is the set of elements of B which are integral over A (note elements of A are integral over A, $x - a$ is a monic polynomial). Then C is a ring. (Of course, C need not be a finite ring extension of A.*

Proof. Suppose that $b, b' \in C$. Then obviously b is integral over A so that $A[b]$ is a finite extension of A. Furthermore, $A[b, b']$ is a finite extension of $A[b]$. Thus $A[b, b']$ is a finite extension of A. Hence $b \cdot b'$ and $b + b'$ are integral over A as desired. □

16. Wednesday, October 2nd

We did the going up theorem in class.

17. Friday, October 4th

17.1. **The Nullstellensatz and $\mathfrak{m}$-Spec of polynomial rings.** Previously we have talked about $V(J)$. If $k = \overline{k}$ is an algebraically closed field and $J \subseteq k[x_1, \ldots, x_n]$, then $\mathbf{V}(J)$ is the subset of k^n where all the functions of J vanish. On the other hand, given any subset $Z \subseteq k^n$ we define $I(Z)$ to be the set of functions in $k[x_1, \ldots, x_n]$ which vanish at every point of Z.

Theorem 17.1. *Let k be an algebraically closed field and $J \subseteq k[x_1, \ldots, x_n]$.*

(a) *If $J \neq k[x_1, \ldots, x_n]$ then $\mathbf{V}(J) \neq \emptyset$.*
(b) $I(\mathbf{V}(J)) = \sqrt{J}$.
(c) $\mathbf{V}(I \cap J) = \mathbf{V}(I) \cup \mathbf{V}(J)$
(d) $\mathbf{V}(I + J) = \mathbf{V}(I) \cap \mathbf{V}(J)$

Proof. For the first part, choose $\mathfrak{m} \supseteq J$ a maximal ideal. Then $\mathfrak{m} = \langle x_1 - \alpha_1, \ldots, x_n - \alpha_n \rangle$ from what we've seen before (see our work on the $\mathfrak{m}$-Spec of tensor products). Then every function of J vanishes at $(\alpha_1, \ldots, \alpha_n)$.

Now for the second part, suppose $f \in I(\mathbf{V}(J))$, hence $f(Q) = 0$ for all $Q \in \mathbf{V}(J)$. We consider the larger ring $S = k[x_1, \ldots, x_n, Y]$. Consider $J' = J \cdot S + \langle fY - 1 \rangle$. Consider $(a_1, \ldots, a_n, b) \in \mathbf{V}(J')$. Then $f(a_1, \ldots, a_n) = 0$ and also $bf(a_1, \ldots, a_n) - 1 = 0$. In particular, $\mathbf{V}(J') = \emptyset$. Then $J' = k[x_1, \ldots, x_n, Y]$. Hence we can write

$$1 = g_0 \cdot (fY - 1) + \sum_{i=1}^{l} g_i \cdot h_i$$

where $g_i \in S$ and $h_i \in J$.

Choose m at least as large as the Y degree of all the g_i. Multiplying through by f^m gives us

$$f^m = G_0(x_1, \ldots, x_n, fY) \cdot (fY - 1) + \sum_{i=1}^{l} G_i(x_1, \ldots, x_n, fY) \cdot h_i$$

for some G_i (obtained from g_i). Modding out by $fY - 1$ (ie, substituting $fY = 1$) gives us

$$f^m = \sum_{i=1}^{l} G_1(x_1, \ldots, x_n, 1) \cdot h_i \in J$$

It follows that $f \in \sqrt{J}$ so that $I(\mathbf{V}(J)) \subseteq \sqrt{J}$. But obviously $\sqrt{J} \subseteq I(\mathbf{V}(J))$ and so the result is proven. □

18. Monday, October 7th

We complete the proof of the Nullstellensatz.

Proof. For the third part, if $x \in \mathbf{V}(I \cap J)$, then everything in $I \cap J$ vanishes at x. Now if P is the set of functions which vanish at x, then $I \cap J \subseteq P$ so that I or J is in P. In the first case $x \in \mathbf{V}(I)$, in the second $x \in \mathbf{V}(J)$ so $\subseteq$ holds. Conversely if $x \in \mathbf{V}(I) \cup \mathbf{V}(J)$ then $x \in \mathbf{V}(I)$ or in $\mathbf{V}(J)$. In either case $x \in \mathbf{V}(I \cap J)$.

For the final part, suppose $x \in \mathbf{V}(I + J)$, then $x \in \mathbf{V}(I)$ and $x \in \mathbf{V}(J)$ so $x \in \mathbf{V}(I) \cap \mathbf{V}(J)$. On the other hand, if $x \in \mathbf{V}(I) \cap \mathbf{V}(J)$, then choose $f \in I$ and $g \in J$ so that $f(x) = g(x) = 0$ and so $(f + g)(x) = 0$. Hence $\mathbf{V}(I + J) = 0$. □

Now we talk about a geometric interpretation of any ring. Set R to be a commutative ring. For each $Q \in \operatorname{Spec} R$, set $k(Q) = R_Q/(Q \cdot R_Q)$. This is called the the *residue field of* Q. We define $f(Q)$ to be the image $\overline{f}$ in $k(Q)$.

We can now view f as a function on $\operatorname{Spec} R$, it just happens to take values (in possibly different fields).

For instance, in $\mathbb{C}[x]$, $f(x)$ evaluates to $f(\alpha) \in \mathbb{C} = k(\langle x - \alpha)$.

On the other hand, $-13 \in \mathbb{Z}$ evaluates to $[2]$ at $\langle 5 \rangle$ in $\mathbb{F}_5$. It evaluates to $[1]$ at $\langle 7 \rangle$ in $\mathbb{F}_7$, etc.

Lemma 18.1. *Suppose R is a ring and $f, g \in R$. If $\overline{f} = \overline{g} \in k(Q)$ for all $Q \in \operatorname{Spec} R$, then $f - g$ is nilpotent. In particular if R is a domain or even just reduced, the $f = g$..*

Proof. It is sufficient to show that the kernel of the canonical map $R \longrightarrow \prod_{Q \in \operatorname{Spec} R} k(Q)$ is the nilradical. But the kernel is simply the intersection of all the $Q \in \operatorname{Spec} R$. □

Now we move on to a worksheet for the remainder of the class, that will demonstrate a variant of the Nullstellensatz that works for any ring.

19. Wednesday, October 9th

Definition 19.1. Suppose R is a ring. We say that R is *Noetherian* if its ideals satisfy the ascending chain condition. That is, if

$$I_1 \subseteq I_2 \subseteq ...$$

is an ascending chain of ideals, then $I_n = I_{n+1}$ for all $n \gg 0$.

Likewise we say that R is *Artinian* if its ideals satisfy the descending chain condition. That is if

$$I_1 \supseteq I_2 \supseteq ...$$

is a descending chain of ideals, then $I_n = I_{n+1}$ for all $n \gg 0$.

Lemma 19.2. *R is Noetherian if and only if every ideal of R is finitely generated.*

Proof. I leave it to you to write it down carefully. □

Example 19.3. Clearly a field is both Artinian and Noetherian, but of course most rings we encounter are not Artinian. For instance $k[x]$ and $\mathbb{Z}$ are Noetherian but not Artinian.

Proposition 19.4. *Every Artinian ring is Noetherian (this is* NOT *true for modules).*

Proof. Suppose R is an Artinian ring. □

Next we prove Hilbert's basis theorem.

Theorem 19.5 (Hilbert's basis theorem)**.** *If R is Noetherian, then so is $R[x]$.*

Proof. Let $J \subseteq R[x]$ be an ideal. We need to show that J is finitely generated. Set $J_n = \{r \in R | rx^n + r_{n-1}x^{n-1} \dots r_0 \in J\}$. We note that J_n is an ideal of R. Furthermore, $J_n \subseteq J_{n+1}$ (since we can multiply elements of J by x and stay in J). Hence $J_n = J_{n+1}$ for all $n \geq n_0$.

For each $0 \leq i \leq n_0$ write $J_i = \langle r_{i,1}, \dots r_{i,d} \rangle$ (we can use the same d for all if we desire). Choose $f_{i,j} \in J$ of degree i whose leading coefficient is $r_{i,j}$. We will show that $\langle f_{i,j} \rangle = J$. Now choose $f \in J$. We will show that $f \in \langle f_{i,j} \rangle$ by induction on $\deg f$ (degree 0 being obvious). Indeed, write $f = rx^n + \dots$. Note that $r \in J_n$ and hence there exists $g \in \langle f_{i,j} \rangle$ with $g = rx^n + \dots$. Thus $f - g \in J$ has lower degree and we are done. □

Corollary 19.6. *Finitely generated algebras over $\mathbb{Z}$ or a field k are Noetherian.*

Now we move on to modules.

Definition 19.7. We say that an R-module M is *Noetherian* if its submodules satisfy the ascending chain condition.

Note that submodules (and quotient modules) of Noetherian modules are clearly Noetherian.

Lemma 19.8. *M is Noetherian if and only if every submodule of M is finitely generated as an R-module.*

Proof. Obviously a Noetherian module is finitely generated. And if every submodule is finitely generated, the ascending chain condition holds by the usual argument. □

20. Friday, October 11th

Lemma 20.1. *If $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ is a short exact sequence then B is Noetherian if and only if A and C are Noetherian.*

Proof. We only need to handle the ($\Rightarrow$) direction, the other containment is obvious. Suppose that $M \subseteq B$ is a submodule. Then $g(M)$ is a finitely generated submodule of C. Likewise, $f^{-1}(M) \subseteq A$ is finitely generated. But notice $0 \longrightarrow f^{-1}(M) \longrightarrow M \longrightarrow g(M) \longrightarrow 0$ is exact and so M is finitely generated by the homework problem. □

Corollary 20.2. *If R is a Noetherian ring, then R^n is a Noetherian module for every $n \geq 0$.*

Proof. We have short exact sequences $0 \longrightarrow R^i \longrightarrow R^{i+j} \longrightarrow R^j \longrightarrow 0$ and induction. □

Proposition 20.3. *Suppose R is a Noetherian ring. Then an R-module M is finitely generated if and only if it is Noetherian. In particular, every submodule of a finitely generated module over a Noetherian ring is finitely generated.*

Proof. We only have to show that if M is finitely generated then it is Noetherian. First since M is finitely generated there exists a surjection $R^n \longrightarrow M$. But then M is a quotient of a Noetherian module and hence Noetherian. □

20.1. **Support, annihilators and associated primes.** We are going to follow Reid's book closely here.

Definition 20.4 (Annihilators)**.** Given a ring R, an R-module M and a subset $S \subseteq M$, we define the *annihilator of S* to be the set

$$\operatorname{Ann}_R S = \{r \in R \mid rx = 0 \text{ for all } x \in S\}.$$

It is easy to see that this is an ideal.

Lemma 20.5. *If M is finitely generated, then the formation of $\operatorname{Ann}_R M$ commutes with localization. In particular if $W \subseteq R$ is a multiplicative set then $W^{-1} \operatorname{Ann}_R M = \operatorname{Ann}_{W^{-1}R} W^{-1}M$.*

Proof. Suppose that M has generators $\{x_1, \ldots, x_n\}$ and so $\{x_1/1, \ldots, x_n/1\}$ generate $W^{-1}M$. Suppose that $r \in \operatorname{Ann}_R M$ and so $rx_i = 0$ for all i. But then obviously $(r/1)(x_i/1) = (rx_i)/1 = 0$ as well so $\subseteq$ is easy. Conversely, suppose that (r/w) annihilates $W^{-1}M$. Then $(r/w)(x_i/1) = 0$ for all i.

Thus there exist $v_i \in W$ such that $v_i r x_i = 0 \in M$ for all i. Letting $v = \prod v_i$ we see that $v r x_i = 0$ for all i. Thus $vr \in \operatorname{Ann}_R M$ and so $r/w \in W^{-1}(\operatorname{Ann}_R M)$. □

Also recall the dimension of support.

Definition 20.6 (Support)**.** Given a ring R and an R-module M, we define $\operatorname{Supp} M$ to be the set of primes $Q \in \operatorname{Spec} R$ with $M_Q \neq 0$.

$$\operatorname{Supp} M = \{Q \in \operatorname{Spec} R \mid M_Q \neq 0\}.$$

Lemma 20.7. *Suppose that M is a finitely generated R-module. Then $V(\operatorname{Ann}_R M) = \operatorname{Supp} M$. In particular $\operatorname{Supp} M$ is closed.*

Proof. Suppose that $I = \operatorname{Ann}_R M$. Choose $Q \in \operatorname{Supp} M$. Since the formation of I commutes with localization, it is sufficient to show the statement in the case that $R = R_Q$ is a local ring with maximal ideal Q. Then since $M = M_Q$ we see that $Q \in \operatorname{Supp} M$ is simply the assertion that $\operatorname{Supp} M$ is non-empty. We need to show that $V(\operatorname{Ann}_R M)$ is also non-empty in this case. But since $M \neq 0$, $1 \notin \operatorname{Ann}_R M$ and so $\operatorname{Ann}_R M$ is a proper ideal contained in Q. The result follows. □

Definition 20.8 (Associated primes)**.** Let A be a ring and M an A-module. An *associated prime* (or *assassin*) of M is a prime ideal $P \in \operatorname{Spec} R$ such that there exists $x \in M$ with

$$\operatorname{Ann}_R x = Q.$$

This condition is equivalent to requiring that $R/Q \cong \langle x \rangle \subseteq M$ via the first isomorphism theorem. In particular, Q is an associated prime of M if and only if M contains a submodule isomorphic to R/Q.

We write $\operatorname{Ass} M$ to denote the set of assassins of M.

21. Monday, October 14th

Proposition 21.1 (Section 7.4, 7.5 in Reid)**.** *Suppose that M is an R-module, $x \in M$ and $P = \operatorname{Ann}_R x$. Then*

(a) *If $0 \neq y \in xR = \langle x \rangle$, then $\operatorname{Ann}_R y = P$ as well. In particular, $\operatorname{Ann}_R(R/P) = P$.*
(b) *Any maximal proper ideal of the set of ideals $\{\operatorname{Ann}_R y \mid y \in M\}$ is prime and hence in $\operatorname{Ass} M$.*
(c) *If R is Noetherian and $M \neq 0$, then $\operatorname{Ass} M \neq \emptyset$.*
(d) *If $L \subseteq M$ and $N = M/L$ then $\operatorname{Ass} M \subseteq \operatorname{Ass} N \cup \operatorname{Ass} L$.*
(e) *If R is Noetherian and $M \neq 0$, then*

$$\{r \in R \mid rx = 0 \text{ for some } 0 \neq x \in M\} = \bigcup_{Q \in \operatorname{Ass} M} Q$$

(f) *If $Q \in \operatorname{Ass} M$ then $V(Q) \subseteq \operatorname{Supp} M$.*
(g) *If R is Noetherian, then if $Q \in \operatorname{Supp} M$ is a minimal ideal in $\operatorname{Supp} M$, then $Q \in \operatorname{Ass} M$.*

Proof. For (a), simply note that $xR = R/P$.

For (b), suppose that $Q = \operatorname{Ann}_R y$ is a maximal ideal of that set and $ab \in Q$ with $a, b \notin Q$. Hence $aby = 0$ but $by \neq 0$. But notice that $a \in \operatorname{Ann}_R(by) \supsetneq \operatorname{Ann}_R(y) = Q$ which does not contain 1, contradicting the maximality of Q

For (c), simply notice that the set in (b) is non-empty and apply the Noetherian hypothesis to show it has a maximal element.

For (d), choose $x \in M$ with $P = \operatorname{Ann}_R x$. Write $f : M \to N = M/L$ to be the canonical surjection. If $xR \cap L = \{0\}$ then obviously $f|_{xR}$ is injective and $\overline{x}R \cong xR \cong R/P$. On the other hand, if $0 \neq y \in xR \cap L$ then $\operatorname{Ann}_R y \cong R/P$ as well by (a).

For (e), if r is in the left-hand-side, then r is contained in a maximal element in the set from (b), and hence contained in an element of $\operatorname{Ass} M$. The reverse containment is even more trivial.

For (f), we notice that if $Q \in \operatorname{Ass}_M$, then R/Q is isomorphic to a submodule $N \in M$. Hence $R_Q/(QR_Q) \cong N_Q \subseteq M_Q$ and the left side is nonzero and hence so is the right. Hence $Q \in \operatorname{Supp} M$ but then $M_P \neq 0$ for any $P \supseteq Q$ since $(M_P)_Q = M_Q \neq 0$.

22. Wednesday, October 16th

For (g), suppose that Q is minimal as above. Then $M_Q \neq 0$. Furthermore $M_P = 0$ for any $P \subsetneq Q$ so that $\operatorname{Supp}_{R_Q} M_Q = \{QR_Q\}$. Since $\operatorname{Ass} \subseteq \operatorname{Supp}$, we see that $\operatorname{Ass}_{R_Q} M_Q = \{QR_Q\}$ since $M_Q \neq 0$.

But now choose $x/w \in M_Q$, $x \in M$, $w \in R \backslash Q$ with $\operatorname{Ann}_{R_Q}(x/w) = QR_Q$. Optimally $\operatorname{Ann}_R x = Q$ and certainly each $r \in \operatorname{Ann}_R x$ is such that $r/1 \in QR_Q$. This implies that each such $r \in Q$ so $\subseteq$ is always true. But equality might be out of our grasp. Of course, $Q = \langle s_1, \ldots, s_d \rangle$ is finitely generated so that $s_i/1 \in \operatorname{Ann}_{R_Q} M_Q$ and in particular $(s_i/1)(x/w) = 0$ so that $v_i s_i x = 0$ and hence taking the product $v = \prod v_i$ again we see that each s_i annihilates vx so that $\operatorname{Ann}_R(vx) \supseteq Q$. But as before, since $\operatorname{Ann}_{R_Q}(vx/(vw)) = QR_Q$, $\operatorname{Ann}_R(vx) \subseteq Q$. □

Lemma 22.1. *For ideals $I, J \subseteq R$, we have $\sqrt{I \cdot J} = \sqrt{I} \cap \sqrt{J}$.*

Proof. Obviously the intersection of radical ideals is radical, so the containment $\subseteq$ is obvious. Conversely if $x \in \sqrt{I} \cap \sqrt{J}$, then $x^n \in I, J$ for some $n \gg 0$. Hence $x^{2n} = x^n \cdot x^n \in I \cdot J$ which implies that $x \in \sqrt{I \cdot J}$ as desired. □

Lemma 22.2. *Fix R a Noetherian ring and $I \subseteq R$. Then R has finitely many primes in $V(I)$ which are minimal with respect to containment. In particular*

$$\sqrt{I} = P_1 \cap \ldots \cap P_n$$

where the P_i are the finitely many minimal primes containing I.

Proof. Let E be the set of radical ideals who cannot be decomposed as above. We would like to show that the set is empty. Suppose not, then E contains a maximal element J since R is Noetherian. Since J is not itself prime (or else it would not be in E) there exist $a, b \notin J$ with $ab \in J$. Set $J_1 = J + \langle a \rangle$ and $J_2 = J + \langle b \rangle$. Note $J_1 \cdot J_2 = J$ even though $J \subsetneq J_1, J_2$. Hence $J = \sqrt{J_1 \cdot J_2} = \sqrt{J_1} \cap \sqrt{J_2}$. But now J_1, J_2 are not in E since J is maximal in E. Hence J_1 and J_2 are intersections of finitely many primes (minimal over them). But then so is J, a contradiction. □

Corollary 22.3. *Let M be a finite module over a Noetherian ring A, then*

$$\operatorname{Supp} M = \bigcup_{i=1}^{n} V(P_i)$$

where the P_i are the finitely many minimal primes containing $\operatorname{Ann} M$*.*

Proof. We already saw that $\operatorname{Supp} M = V(\operatorname{Ann} M) = V(\sqrt{\operatorname{Ann} M})$. But $\sqrt{\operatorname{Ann} M}$ is an intersection of the finitely many primes minimal over it and then we are done since $V(J_1 \cap J_2) = V(J_1) \cup V(J_2)$. □

Theorem 22.4. *If A is a Noetherian ring and M is a finite A module, there exists a chain of submodules*

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

with $M_i/M_{i-1} \cong A/P_i$ where P_i is prime. Furthermore,

$$\operatorname{Ass} M \subseteq \{P_1, \ldots, P_n\}$$

and so $\operatorname{Ass} M$ *is finite.*

Proof. Since $\operatorname{Ass} M \neq \emptyset$, we see that $M_1 \cong A/P_1$ a subset of M exists. Now repeat the argument and construct $M_2' \subseteq M/M_1$ and let M_2 be the inverse image of M_2'. This chain stops since M is Noetherian. Next we need to show that the associated primes of M are among the P_i. But this follows immediately from Proposition 21.1(d). □

23. Friday, October 18th

23.1. **Primary ideals.** We now define primary ideals.

Definition 23.1 (Primary ideals)**.** An ideal $Q \subsetneq R$ is primary if $fg \in Q$ implies that $f \in Q$ or $g^n \in Q$ for some $n > 0$. (Note this is symmetric since $fg = gf$).

Note that Q is primary if and only if all of R/Q's zerodivisors are nilpotent.

Lemma 23.2. *If Q is primary then $\sqrt{Q}$ is prime.*

Proof. If $ab \in \sqrt{Q}$, then $a^m b^m \in Q$. Hence $a^m \in Q$ or $b^{nm} \in Q$. Hence $a \in \sqrt{Q}$ or $b \in \sqrt{Q}$. □

Remark 23.3. You might be tempted to think that being primary is the same that $\sqrt{Q}$ is prime. This is not true. For instance consider $J = \langle x^2, xy\rangle \in k[x,y]$. Then $\sqrt{J} = \langle x\rangle$. But note that $xy \in J$ but neither $x \in J$ or $y^n \in J$.

Example 23.4 (Powers of primes are not always primary)**.** Obviously prime ideals are primary. If $Q = \langle f\rangle$ is a prime ideal in a domain, then Q^n is always primary. We proceed by induction on n, the base case is obvious so we suppose $n \geq 2$. Now, suppose that $xy \in Q^n = \langle f^n\rangle$ with $y^m \notin \langle f^n\rangle$ for any n. Since $xy = zf^n \in \langle f\rangle$ which is prime, we see that $f|x$ or $f|y$. But the second case is impossible since $y^m \notin \langle f^n\rangle$ for any m. So we write $x = uf$. Hence $ufy = zf^n$ and so $uy = zf^{n-1}$ (since we are in an integral domain). Then $uy \in \langle f^{n-1}\rangle$. Since $y^m \notin \langle f^n\rangle$ for any m, we see also that $y^m \notin \langle f^{n-1}\rangle$ for any m. Hence by induction $u \in \langle f^{n-1}\rangle$ and hence $uf \in \langle f^n\rangle$ as desired.

More generally (and I won't prove this now) if $Q = \langle f_1, \rangle, f_d\rangle \subseteq R$ is an ideal such that $\overline{f_{i+1}}$ is not a zero divisor in $R/\langle f_1, \ldots, f_i\rangle$ for each $i = 1, \ldots, d-1$, then Q^n is primary for all n.

In general however, Q^n is not primary for an arbitrary prime ideal Q. Let us consider an example. $R = k[x,y,z]/\langle xy - z^2\rangle$. $Q = \langle x, z\rangle$. Then $Q^2 = \langle x^2, xz, z^2\rangle = \langle x^2, xz, xy\rangle$. Note that $xy \in Q^2$ but $x \notin Q$ and y^n is not in Q for any n.

Example 23.5 (Inverse images of primary ideals are primary)**.** Suppose $f : R \longrightarrow S$ is a ring map and $Q \subseteq S$ is primary. Then $f^{-1}(Q)$ is primary as well. This is easy, note that $R/(f^{-1}(Q)) \hookrightarrow S/Q$. All of S/Q's zero divisors are nilpotent, and so the same can be said for $R/(f^{-1}(Q))$. This is particularly useful in the case that S is a localization of R.

Lemma 23.6. *Suppose that R is a ring, $J \subseteq R$ is $P = \sqrt{J}$-primary. Then $J \cdot R_P$ is PR_P primary and if $f : R \longrightarrow R_P$ is the natural map, then $f^{-1}(J \cdot R_P) = J$.*

Proof. Suppose that $(x/w)(y/w') = (j/w'') \in J \cdot R_P$. Then $vxy = vww'j \in J$. Hence since $v^n \in R \setminus P \subseteq R \setminus J$ is not in J, we have that $xy \in J$. But then either $x \in J$ or $y^m \in J$. In the first case $(x/w) \in J \cdot R_P$ and in the second $(y/w')^m \in J \cdot R_P$.

Now suppose that $z \in f^{-1}(J \cdot R_P)$. Hence $z/1 \in J \cdot R_P$. It follows that $z/1 = y/w$ for some $y \in J$ and $w = R \setminus P$. Then $zwv = vy \in J$. Since $(wv)^n \notin J$ for any n, $z \in J$ as desired. □

We do have the following though.

Proposition 23.7. *If $Q \subseteq R$ is an ideal such that $\sqrt{Q}$ is maximal, then Q is primary.*

Proof. Suppose that $xy \in Q$. Then $xy \in \sqrt{Q}$. Say $x \notin Q$ and $y^n \notin Q$ for any n. Then consider $Q : x = \{f \in R \mid fx \in Q\}$. Note that this ideal contains Q, and y, but does not contain 1. Then $\sqrt{Q} \subseteq \sqrt{Q : x}$, but the left side is maximal and so $\sqrt{Q : x}$ is also maximal and equal to $\sqrt{Q}$. But now $y \in \sqrt{Q : x} = \sqrt{Q}$. Thus $y^n \in Q$ for some integer n. □

Proposition 23.8. *Let R be Noetherian, $Q \subseteq R$ an ideal. Then Q is P-primary if and only if* $\operatorname{Ass}(R/Q) = \{P\}$.

Proof. Suppose that $\sqrt{Q} = P$ and Q is primary. Then all the zero divisors of R/Q are nilpotent (and all are contained in P/Q). Now suppose that $x \in Q/P$. Then

$$\langle 0 \rangle_{R/Q} = Q/Q \subseteq \operatorname{Ann}_{R/Q} x \subseteq P/Q = \sqrt{Q/Q}$$

Hence if $\operatorname{Ann}_{R/Q} x$ is prime, it is primary and so P/Q-primary and thus equal to P. It follows that $\operatorname{Ass}_{R/Q}(R/Q) = \{P/Q\}$ and so $\operatorname{Ass}_R(R/Q) = \{P\}$.

Now suppose that $\operatorname{Ass}(R/Q) = \{P\}$. We claim that if $0 \neq M \subseteq R/Q$ then $\sqrt{\operatorname{Ann}_R M} = P$. Note $\sqrt{\operatorname{Ann}_R M}$ is the intersection of the (minimal) prime ideals containing $\operatorname{Ann}_R M$, the minimal primes of $\operatorname{Supp} M$. Thus they are in $\operatorname{Ass}_R M \subseteq \operatorname{Ass}_R(R/Q) = \{P\}$ proving the claim.

Next note that since $Q = \operatorname{Ann}_R(R/Q)$, we see that $P = \sqrt{Q}$. We need to show that Q is actually primary. We choose $fg \in Q$, and say $f \notin Q$. Set $\overline{f} = f + Q \in R/Q$. Now $g \in \operatorname{Ann}_R \overline{f} \subseteq \sqrt{\operatorname{Ann}_R \overline{f}} = P = \sqrt{Q}$, so $g^n \in Q$ for some n. This shows that Q is primary. □

24. Monday, October 21st

Definition 24.1. Let R be a ring and $I \subseteq R$. A primary decomposition of I is an expression

$$I = Q_1 \cap \ldots \cap Q_k$$

where each Q_i is primary. It is called *shortest* if

(a) $I \neq \bigcap_{j \neq i} Q_j$ for any i and
(b) If Q_i is P_i primary, then $P_i = P_j$ implies that $i = j$.

If I has a primary decomposition, then it has a shortest primary decomposition by the following lemma.

Lemma 24.2. *If Q, Q' are P-primary, so is $Q \cap Q'$.*

Proof. Suppose that $fg \in Q \cap Q'$ and $g^m \notin Q \cap Q'$ for any m. Then $g \notin \sqrt{Q} = P\sqrt{Q'}$ so that $g^m \notin Q'$ for any m. Hence $f \in Q$ and $f \in Q'$ since Q, Q' are primary. The result follows. □

The next big goal is the existence of primary decompositions.

24.1. **Primary decomposition.** We already know primary decompositions of radical ideals. We can decompose them into intersections of their minimal primes. Likewise ideals in PIDs and Dedekind domains are easy to write as intersections primary ideals.

Definition 24.3. An ideal $J \subseteq R$ is *indecomposable* if $I = J \cap K$ implies that $I = J$ or $I = K$. Note prime ideals are indecomposable.

Lemma 24.4. *In a Noetherian ring, every ideal is a finite intersection of indecomposable ideals.*

Proof. Let Σ be the set of ideals that cannot be written in such a fashion. Choose a maximal element, then it can be decomposed into an intersection of strictly bigger ideals. Those ideals have decompositions since they are not in Σ. □

Lemma 24.5. *In a Noetherian ring B, if $\langle 0\rangle \subseteq B$ is indecomposable then it is primary. More generally, in any ring R, $J \subseteq R$ is indecomposable then it is primary.*

Proof. First suppose that $xy = 0 \in B$. Consider the chain $\operatorname{Ann}_B x \subseteq \operatorname{Ann}_B x^2 \subseteq \ldots$. By the Noetherian hypothesis, we know $\operatorname{Ann}_B(x^n) = \operatorname{Ann}_B(x^{n+1})$. We claim that $\langle x^n\rangle \cap \langle y\rangle = 0$. Obviously if $a \in \langle x^n\rangle \cap \langle y\rangle$ then $xa \in \langle xy\rangle = \langle 0\rangle$. But also $a = bx^n$ so $ax = bx^{n+1}$ so that $b \in \operatorname{Ann} x^{n+1} = \operatorname{Ann} x^n$ so that $a = bx^n = 0$.

For the second part, note that if J is indecomposable, so is $\langle 0\rangle$ in $B = R/J$. Then $\langle 0\rangle$ is primary and so J is primary too. □

By combining the lemmas we get that.

Theorem 24.6. *Primary decompositions exist.*

24.2. **Uniqueness of primary decomposition.** In particular, the associated primes of a primary decomposition are unique (although the individual primary objects in even a shortest decomposition are usually not unique). The following lemma will be crucial in helping us identify the part of the primary decomposition that is unique.

Lemma 24.7. *Suppose $W \subseteq R$ is a multiplicative set and $I = Q_1 \cap \ldots \cap Q_d$ is a shortest primary decomposition of I with $P_i = \sqrt{Q_i}$. Further suppose that $P_1, \ldots, P_r$ have trivial intersection with W and $Q_{r+1}, \ldots, Q_d$ have nonempty intersection with W. Then*

$$W^{-1}I = \bigcap_{i=1}^{r} Q_i(W^{-1}R)$$

is a primary decomposition of $W^{-1}I$. Furthermore, $\phi^{-1}(W^{-1}I) = Q_1 \cap \ldots \cap Q_r$ where $\phi : R \longrightarrow W^{-1}R$ is the canonical map.

Proof. Since localization commutes with finite intersections we see that the above is certainly a primary decomposition. For the second part, the inverse image of an finite intersection is the intersection of the inverse images. The rest is easy. □

25. Wednesday, October 23rd

We easily obtain:

Corollary 25.1. *The primary ideals corresponding to minimal primes in $\operatorname{Ass}_R(R/I)$ in a shortest primary decomposition of I are unique.*

Proof. Set $W = R \setminus P_i$, expand I to $W^{-1}R$ and then pull back. □

We also have:

Theorem 25.2. *Suppose $I = Q_1 \cap \ldots \cap Q_d$ is a shortest primary decomposition. Set $P_i = \sqrt{Q_i}$. Then*

$$\mathrm{Ass}(R/I) = \{P_1, \ldots, P_d\}.$$

Proof. Note that we have an inclusion:

$$f : R/I \hookrightarrow R/Q_1 \oplus \ldots \oplus R/Q_d.$$

Since $\mathrm{Ass}(R/Q_i) = P_i$ we see that the associated primes of the right side are simply $P_1, \ldots, P_d$ and so $\mathrm{Ass}_R(R/I) \subseteq \{P_1, \ldots, P_d\}$.

Next consider $M_j = \bigcap_{i \neq j} Q_i/I \subseteq R/I$. This module cannot be zero since the decomposition is shortest. Of course $f(M_j)$ is zero in each component of $R/Q_1 \oplus \ldots \oplus R/Q_d$ except the jth (where it is not zero). Since $\mathrm{Ass}_R(R/Q_j) = \{P_j\}$ and $f(M_j) \subseteq R/Q_j$, we see that $\mathrm{Ass}(M_j) = \{P_j\}$ and so R/I has P_j as an associated prime as well. □

25.1. **Completion.** We follow Atiyah-MacDonald. One of the "interesting" features of algebraic geometry you have already noticed is that the open sets are really big. Sometimes you want to work with Euclidean open balls. You could try to use localization to do this, but it turns out that R_Q still remembers the "generic" global geometry of $\operatorname{Spec} R$. For instance, it knows the genus (number of holes) if $\operatorname{Spec} R$ is an affine chart of a Riemann surface (it even knows what complex analytic isomorphism class of the Reimann surface you are on). One way around that is to use completion. Whereas localization somehow cuts down the size of Spec from above, completion builds up a ring out of higher-tangency information.

I won't type up these notes. See Atiyah-MacDonald for details.

25.2. **Introduction to dimension theory.** We now discuss dimension theory for rings.

Definition 25.3 (Krull)**.** Given a ring R, the *(Krull) dimension of R* is the maximal length n of a chain of prime ideals:

$$Q_0 \subsetneq Q_1 \subsetneq Q_2 \subsetneq \ldots \subsetneq Q_n \subsetneq R$$

If there is no such maximum, we say that R has *infinite (Krull) dimension.* In either case, we denote the (Krull) dimension by $\dim R$.

More generally, given any prime ideal Q, the *height of Q* is the maximal length n of a chain of prime ideals

$$Q_0 \subsetneq Q_1 \subsetneq \ldots \subsetneq Q_n = Q.$$

This is denoted by $\mathrm{ht}(Q)$ if it exists. In particular, $\dim R = \max\{\mathrm{ht}(Q)\}_{Q \in \operatorname{Spec} R}$.

Obviously a Dedekind domain has dimension 1, and a field has dimension 0. Notice that this is reasonable, $\dim \mathbb{C}[x] = 1$ (one complex dimension).

Lemma 25.4. *Suppose k is a field, then* $\dim k[x_1, \ldots, x_n] = n$.

Proof. Obviously $\dim k[x_1, \ldots, x_n] \geq n$ since we can form the ascending chain of primes:

$$\langle 0 \rangle \subsetneq \langle x_1 \rangle \subsetneq \langle x_1, x_2 \rangle \subsetneq \ldots \subsetneq \langle x_1, \ldots, x_n \rangle.$$

We need to show that there is no longer chain. □

26. Completion

We followed Atiyah-MacDonald closely.

27. Dimension Theory

We followed Atiyah-MacDonald closely.

28. December 5th, 2013

We have so far seen numerous functors which are left or right exact, but not *exact*. For instance

- $\operatorname{Hom}_R(M, \_\_)$ is left exact
- $\operatorname{Hom}_R(\_\_, N)$ is left exact (although contravariant)
- $\otimes$ is right exact
- $\Gamma_I(\_\_)$ is left exact
- we even saw that $\lim_{\leftarrow}$ was left exact when we studied completion.

It turns out there is a nice way to handle all these failures of exactness. Through the use of derived functors.

First a formality.

Definition 28.1. Suppose that $B^\bullet = \ldots \to B^{-1} \to B^0 \to B^1 \to B^2 \to \ldots$ is a complex (ie, $\ker(B_i \longrightarrow B_{i+1}) \supseteq \operatorname{im}(B_{i-1} \longrightarrow B_i)$). We define the ith cohomology of $B^\bullet$ to be

$$\mathbf{h}^i(B^\bullet) = \ker(B_i \longrightarrow B_{i+1}) / \operatorname{im}(B_{i-1} \longrightarrow B_i)$$

28.1. **Tor.**

Definition 28.2 (Projective resolutions)**.** Suppose R is a ring and M is an R-module. A projective resolution of M is a series of projective (ie free) modules P_i, $i = 0, -1, -2, \ldots$ and maps

$$\ldots \xrightarrow{f_n} P^{-n} \xrightarrow{f_{n-1}} P^{-n+1} \xrightarrow{f_{n-2}} \ldots \xrightarrow{f_2} P^{-2} \xrightarrow{f_1} P^{-1} \xrightarrow{f_0} P^0 \to M \longrightarrow 0$$

making the above sequence exact. Such a sequence could be infinite. Since every module is a quotient of a free (and hence projective) module, every module has a projective resolution (although not a unique one).

Definition 28.3 (Tor)**.** Suppose that $P^\bullet \longrightarrow M$ is a projective resolution of M. Note that for any module C, $P^\bullet \otimes C$ is a complex. We define $\operatorname{Tor}_i(M, C)$ to be $\mathbf{h}^i(P^\bullet \otimes C)$. It is not obvious that this is independent of the choice of projective resolution, but it is true.

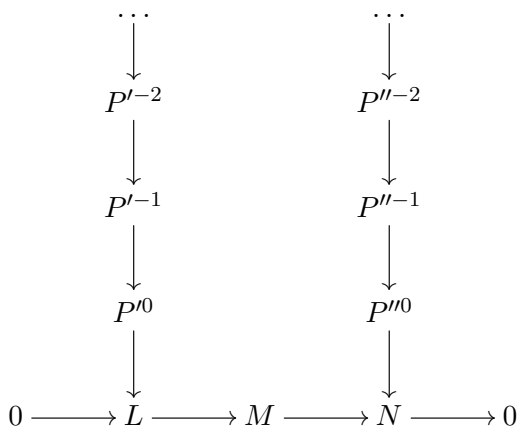
It is easy to see that:

Lemma 28.4. $\mathrm{Tor}_0(M, C) \cong M \otimes C$. *Furthermore, if M is projective then* $\mathrm{Tor}_i(M, C) = 0$ *for all* $i > 0$.

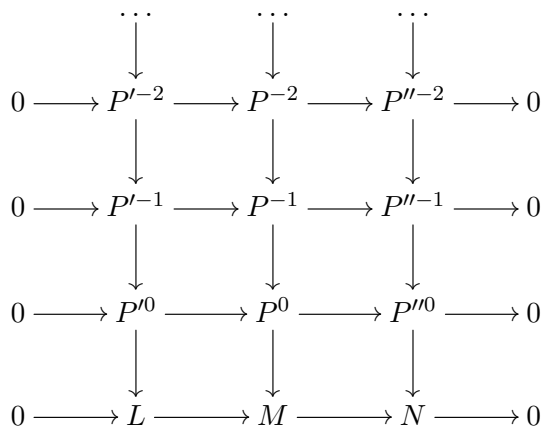
One other fact that is useful, but which we won't prove is that

Lemma 28.5. $\mathrm{Tor}_i(M, C) \cong \mathrm{Tor}_i(C, M)$.

Now suppose that $0 \longrightarrow L \longrightarrow M \longrightarrow N \longrightarrow 0$ is a short exact sequence. We form a projective resolutions of L and N to form the following:



We set $P_i = P'_i \oplus P''_i$ with the canonical short exact sequences $0 \longrightarrow P'_i \longrightarrow P_i \longrightarrow P''_i \longrightarrow 0$. We claim that these combine to form a commutative diagram



where the columns form projective resolutions. This is pretty easy.

Now apply the functor $\otimes_R C$ for some module C to the resolutions $P^\bullet = \dots P^2 \to P^1 \to P^0$ (likewise with $P'^\bullet$ and $P''^\bullet$). We obtain

$$\begin{array}{ccccccccc}
 & & \vdots & & \vdots & & \vdots & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & P'^{-2} \otimes C & \longrightarrow & P^{-2} \otimes C & \longrightarrow & P''^{-2} \otimes C & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & P'^{-1} \otimes C & \longrightarrow & P^{-1} \otimes C & \longrightarrow & P''^{-1} \otimes C & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & P'^{0} \otimes C & \longrightarrow & P^{0} \otimes C & \longrightarrow & P''^{0} \otimes C & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & 0
\end{array}$$

We now apply the snake lemma, first to the diagram

$$\begin{array}{ccccccccc}
 & & P'^{-1} \otimes C/\operatorname{im}(P'^{-2} \otimes C) & \longrightarrow & P^{-1} \otimes C/\operatorname{im}(P^{-2} \otimes C) & \longrightarrow & P''^{-1} \otimes C/\operatorname{im}(P''^{-2} \otimes C) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & P'^{0} \otimes C & \longrightarrow & P^{0} \otimes C & \longrightarrow & P''^{0} \otimes C & \longrightarrow & 0
\end{array}$$

The cokernel below the bottom row is simply

$$L \otimes C \to M \otimes C \to N \otimes C \to 0$$

but this snakes up and connects with the kernels above the top row, which are

$$\operatorname{Tor}_1(L, C) \to \operatorname{Tor}_1(M, C) \to \operatorname{Tor}_1(N, C)$$

connecting these we get a long exact sequence

$$\operatorname{Tor}_1(L, C) \to \operatorname{Tor}_1(M, C) \to \operatorname{Tor}_1(N, C) \to L \otimes C \to M \otimes C \to N \otimes C \to 0.$$

But we don't stop now. We next consider the diagram:

$$\begin{array}{ccccccccc}
 & & P'^{-2} \otimes C/\operatorname{im}(P'^{-3} \otimes C) & \longrightarrow & P^{-2} \otimes C/\operatorname{im}(P^{-3} \otimes C) & \longrightarrow & P''^{-2} \otimes C/\operatorname{im}(P''^{-3} \otimes C) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \ker(P'^{-1} \otimes C \to P'^{0} \otimes C) & \longrightarrow & \ker(P^{-1} \otimes C \to P^{0} \otimes C) & \longrightarrow & \ker(P''^{-1} \otimes C \to P''^{0} \otimes C) & &
\end{array}$$

applying the snake lemma again gets us to the long exact sequence

$$\begin{array}{ccccccccc}
 & & & & & & \dots & \to & \\
\operatorname{Tor}_2(L, C) & \to & \operatorname{Tor}_2(M, C) & \to & \operatorname{Tor}_2(N, C) & \to & & & \\
\operatorname{Tor}_1(L, C) & \to & \operatorname{Tor}_1(M, C) & \to & \operatorname{Tor}_1(N, C) & \to & & & \\
L \otimes C & \to & M \otimes C & \to & N \otimes C & \to & 0. & &
\end{array}$$

28.2. **Ext.** We first consider the functor $\mathrm{Hom}_R(\_, C)$.

Definition 28.6. If $P^\bullet$ is a projective resolution of M, then we define $\mathrm{Ext}^i(M, C)$ to be $\mathbf{h}^i(\mathrm{Hom}_R(P^\bullet, C))$, the ith cohomology of the complex $\mathrm{Hom}_R(P^\bullet, C)$.

Given a short exact sequence

$$0 \longrightarrow L \longrightarrow M \longrightarrow N \longrightarrow 0$$

as above, we again form projective resolutions

$$\begin{array}{ccccccccc}
 & & \vdots & & \vdots & & \vdots & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & P'^{-2} & \longrightarrow & P^{-2} & \longrightarrow & P''^{-2} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & P'^{-1} & \longrightarrow & P^{-1} & \longrightarrow & P''^{-1} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & P'^{0} & \longrightarrow & P^{0} & \longrightarrow & P''^{0} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & L & \longrightarrow & M & \longrightarrow & N & \longrightarrow & 0
\end{array}$$

and apply the functor $\mathrm{Hom}_R(\_, C)$ to the projective resolutions to obtain:

$$\begin{array}{ccccccccc}
 & & \vdots & & \vdots & & \vdots & & \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \longleftarrow & \mathrm{Hom}_R(P'^{-2}, C) & \longleftarrow & \mathrm{Hom}_R(P^{-2}, C) & \longleftarrow & \mathrm{Hom}_R(P''^{-2}, C) & \longleftarrow & 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \longleftarrow & \mathrm{Hom}_R(P'^{-1}, C) & \longleftarrow & \mathrm{Hom}_R(P^{-1}, C) & \longleftarrow & \mathrm{Hom}_R(P''^{-1}, C) & \longleftarrow & 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \longleftarrow & \mathrm{Hom}_R(P'^{0}, C) & \longleftarrow & \mathrm{Hom}_R(P^{0}, C) & \longleftarrow & \mathrm{Hom}_R(P''^{0}, C) & \longleftarrow & 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \longleftarrow & 0 & \longleftarrow & 0 & \longleftarrow & 0 & \longleftarrow & 0
\end{array}$$

Applying the same snake lemma formalisms again, we note that we have diagrams

$$\begin{array}{ccccccccc}
\ker \begin{pmatrix} \mathrm{Hom}_R(P'^{-i-1}, C) \\ \longrightarrow \\ \mathrm{Hom}_R(P'^{-i-2}, C) \end{pmatrix} & \longleftarrow & \ker \begin{pmatrix} \mathrm{Hom}_R(P^{-i-1}, C) \\ \longrightarrow \\ \mathrm{Hom}_R(P^{-i-2}, C) \end{pmatrix} & \longleftarrow & \ker \begin{pmatrix} \mathrm{Hom}_R(P''^{-i-1}, C) \\ \longrightarrow \\ \mathrm{Hom}_R(P''^{-i-2}, C) \end{pmatrix} & \longleftarrow & 0 \\
\uparrow & & \uparrow & & \uparrow & & \\
0 \leftarrow \mathrm{Hom}_R(P'^{-i}, C)/\operatorname{im}(\mathrm{Hom}_R(P'^{-i+1}, C)) & \leftarrow & \mathrm{Hom}_R(P^{-i}, C)/\operatorname{im}(\mathrm{Hom}_R(P^{-i+1}, C)) & \leftarrow & \mathrm{Hom}_R(P''^{-i}, C)/\operatorname{im}(\mathrm{Hom}_R(P''^{-i+1}, C)) & &
\end{array}$$

The snake lemma yields the following long exact sequence.

$$\begin{array}{rcccc} 0 \to & \operatorname{Hom}_R(N,C) & \to & \operatorname{Hom}_R(M,C) & \to & \operatorname{Hom}_R(L,C) \\ \to & \operatorname{Ext}^1_R(N,C) & \to & \operatorname{Ext}^1_R(M,C) & \to & \operatorname{Ext}^1_R(L,C) \\ \to & \operatorname{Ext}^2_R(N,C) & \to & \cdots & & \end{array}$$

However, there isn't just one Ext functor... We also have $\operatorname{Hom}_R(B, \_\_)$. Projective resolutions just aren't good enough any more. We need

Definition 28.7 (Injective resolutions)**.** Suppose that M is a module. We say that

$$\left(0 \to M \to I^\bullet\right) = \left(0 \to M \to I^0 \to I^1 \to I^2 \to \right)$$

is an injective resolution if each I^i is an injective module and the above sequence is a long exact sequence. It is a non-trivial fact that injective resolutions exist (to show it, it is enough to show that for every module N, there is an injective module and an injection $N \hookrightarrow I$).

Definition 28.8. Fix $I^\bullet$ to be an injective resolution of a module M and let $\operatorname{Hom}_R(B, I^\bullet)$ be the corresponding complex. Then we define $\operatorname{Ext}^i_R(B,M)$ to be $\mathbf{h}^i(\operatorname{Hom}_R(B, I^\bullet))$.

There are a couple key facts we won't prove.

- This Ext is also independent of the choice of injective resolution.
- This Ext agrees with the other Ext we defined (which is really useful!) In other words

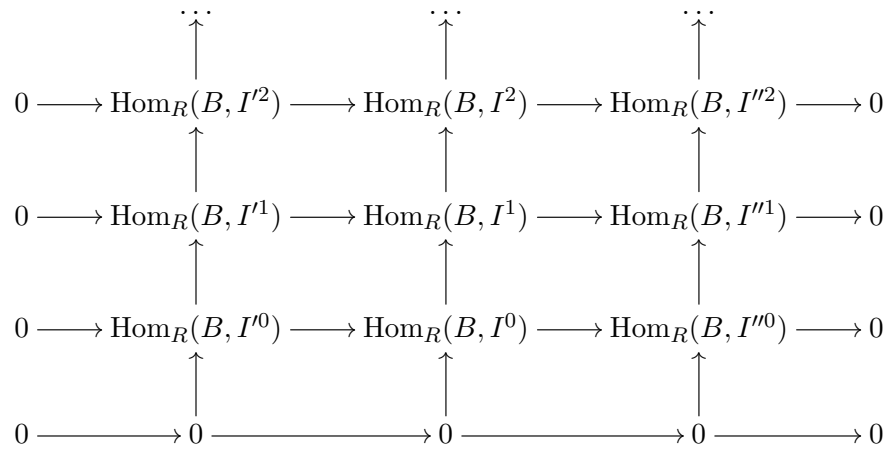
  $$\mathbf{h}^i(\operatorname{Hom}_R(B, I^\bullet)) \cong \mathbf{h}^i(\operatorname{Hom}_R(P^\bullet, M))$$

  where $I^\bullet$ is an injective resolution of M and $P^\bullet$ is a projective resolution of B.

Again, given $0 \to L \to M \to N \to 0$ we can form injective resolutions of L and N and take the direct sum to get an injective resolution of M and so have

$$\begin{array}{ccccccccc} & & \vdots & & \vdots & & \vdots & & \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 0 & \longrightarrow & I'^2 & \longrightarrow & I^2 & \longrightarrow & I''^2 & \longrightarrow & 0 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 0 & \longrightarrow & I'^1 & \longrightarrow & I^1 & \longrightarrow & I''^1 & \longrightarrow & 0 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 0 & \longrightarrow & I'^0 & \longrightarrow & I^0 & \longrightarrow & I''^0 & \longrightarrow & 0 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 0 & \longrightarrow & L & \longrightarrow & M & \longrightarrow & N & \longrightarrow & 0 \end{array}$$

We can apply the covariant functor $\mathrm{Hom}_R(B, \_\_)$ to the I parts and obtain:



The rows are exact and the columns are complexes. Using the snake lemma as before gives us a long exact sequence

$$\begin{array}{ccccccc} 0 & \to & \mathrm{Hom}_R(B,L) & \to & \mathrm{Hom}_R(B,M) & \to & \mathrm{Hom}_R(B,N) \\ & \to & \mathrm{Ext}^1_R(B,L) & \to & \mathrm{Ext}^1_R(B,M) & \to & \mathrm{Ext}^1_R(B,N) \\ & \to & \mathrm{Ext}^2_R(B,L) & \to & \mathrm{Ext}^2_R(B,M) & \to & \mathrm{Ext}^2_R(B,N) \\ & \to & \cdots & & & & \end{array}$$

Department of Mathematics, The Pennsylvania State University, University Park, PA, 16802, USA

E-mail address: schwede@math.psu.edu