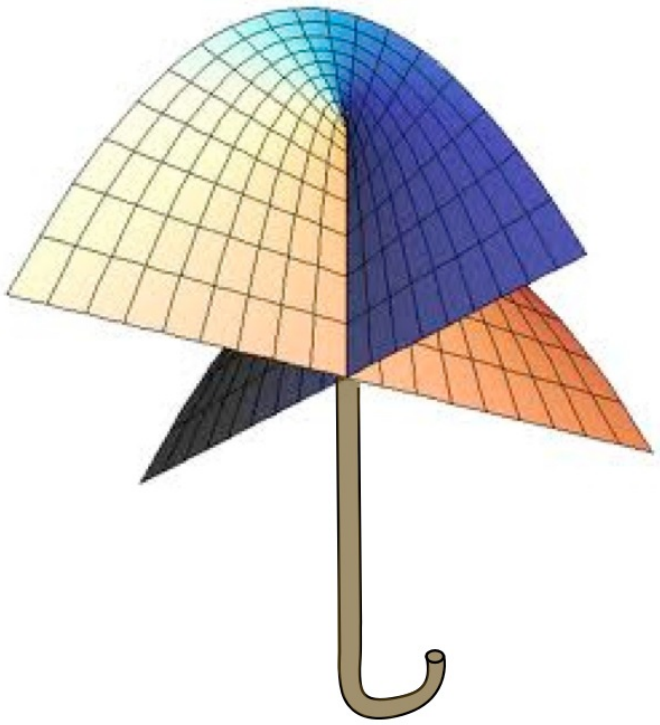
COURSE NOTES MATH 411: COMMUTATIVE ALGEBRA

WILLIAMS COLLEGE
ANDREW BYDLON



CLASS 1, FEBRUARY 4TH: RINGS AND IDEALS

A ring is one of the most fundamental objects in algebra. It has more structure than a group does, which allows for more interesting analysis. When initially realized, the axioms listed below were made up to encapsulate the structure of the integers in a more flexible framework.

Definition 1.1. A ring $(R, +, \cdot)$, more commonly displayed simply as R, is a set R together with two binary operations

$$+, \cdot : R \times R \to R$$

satisfying the following properties:

1) $(R, +)$ is an Abelian (commutative) group. Expanded, this means that there exists an identity, 0, an inverse for any element, $-r$, and that addition is associative.
2) $\cdot$ is an associative operation: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
3) The distributive law holds: $a \cdot (b + c) = a \cdot b + a \cdot c$

Some additional considerations can also be made:

- If $\cdot$ is commutative, $a \cdot b = b \cdot a$, then we call R **commutative**.
- If there exists an identity element for $\cdot$, 1, the R is said to be **unital**.

We will assume throughout (with few exceptions) all rings are commutative and unital.

Example 1.2.

- 0: The ring with 1 element 0 is a ring! It is even unital with $1 = 0$.
- K: A field is a non-zero, commutative, unital ring in which $K^\circ = K \setminus \{0\}$ is a group under $\cdot$. Examples are $\mathbb{Z}/p\mathbb{Z}$, $\mathbb{F}_{p^n}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $K(x)$, etc.
- $\mathbb{Z}$: The integers satisfy these properties, as are thus a commutative unital ring, but NOT a division ring.
- $n\mathbb{Z}$: Does satisfy the properties of being a ring, but has no unit if $n \neq 1$.
- $\mathbb{Z}/n\mathbb{Z}$: The integers $(\mathrm{mod}\, n)$ are a ring! If n is not prime, then it is commutative and unital, but NOT division.
- $K[x]$: Let K be a field (or even any ring!). Then $K[x]$ is notation for polynomials in the variable x with coefficients in K. Then $K[x]$ is a commutative, unital ring which again are NOT division rings.
- $K[\![x]\!]$: The power series in the variable x are also commutative, unital rings which are NOT division rings
- $C_i(\mathbb{R})$: If $i = 0$, the continuous functions from $\mathbb{R}$ to $\mathbb{R}$ form a ring. In addition, if $i > 0$, the i-times differentiable functions also form a ring!

Some immediate consequences of the properties of rings are the following:

- $0 \cdot r = r \cdot 0 = 0$ for any $r \in R$.
- $(-r)s = r(-s) = -(rs)$ for any $a, b \in R$.
- $1 \in R$ is unique, if it is exists.

Ring elements may have specific properties. I now list a few of them:

Definition 1.3. An non-zero element $r \in R$ is called a **zero-divisor** if there exists $s \neq 0$ such that $r \cdot s = 0$. Otherwise r is said to be a **non-zero-divisor**, or **n.z.d.**.

If R has no zero-divisors, and $1 \neq 0$, then R is said to be an **integral domain**.

An element $u \in R$ is called a **unit** if $1 \neq 0$ in R, and there exists $s \in R$ such that $u \cdot s = 1$.

Thus a field is a commutative unital ring in which every non-zero element is a unit.

Next up, we study **Ideals**. They are often used to describe the structure of R in commutative algebra and algebraic geometry.

Definition 1.4. A proper subset $I \subsetneq R$ is called an **ideal** if

1) $(I, +)$ is a closed subgroup of R.
2) I is strongly closed under multiplication: For any element $r \in R$ and $\alpha \in I$, we have that $r \cdot \alpha \in I$.

Example 1.5.
- $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$.
- $xK[x]$ is an ideal of $K[x]$.
- Sums of elements divisible by x **or** y form an ideal of $K[x, y]$.

There is a theme here of divisibility: We can think of all of these ideals as being **generated** by a given element (the smallest ideal containing a given element). In this case, we often refer to them as $\langle n \rangle$, $\langle x \rangle$, or $\langle x, y \rangle$ in the previous cases.

In general,

$$\langle f_1, \ldots, f_n \rangle := \left\{ \sum_{i=1}^{n} r_i \cdot f_i \mid r_i \in R \right\}$$

Next up, I bring up the relationship between ring homomorphisms and ideals. Recall the definition of a ring homomorphism:

Definition 1.6. Let R and S be rings. A map $\varphi : R \to S$ is said to be a **ring homomorphism** if the following criteria are met for any $r, r' \in R$:

1) $\varphi(r + r') = \varphi(r) + \varphi(r')$.
2) $\varphi(r \cdot r') = \varphi(r) \cdot \varphi(r')$.
3) $\varphi(1) = 1$.

The collection (group) of all homomorphisms from R to S is denoted by $\mathrm{Hom}(R, S)$.

This is a very reasonable definition, as it makes addition and multiplication in R compatible with that in S. Additionally, the kernel is defined as in linear algebra.

Definition 1.7. The **kernel** of φ, denoted $\ker(\varphi)$ is the set

$$\ker(\varphi) = \{r \in R \mid \varphi(r) = 0\} \subseteq R$$

The relationship between the 2 ideas is now stated as follows (c.f. Homework 1 #1):

Proposition 1.8. *The kernel of a ring homomorphism is an ideal. Additionally, every ideal is the kernel of some homomorphism.*

CLASS 2, FEBRUARY 6TH: PRIME & MAXIMAL IDEALS

Much like the prime numbers play an important role in describing the structure of the integers, prime ideals play an invaluable role in describing the structure of rings. Recall the following definitions:

Definition 2.1. An ideal $\mathfrak{p} \subsetneq R$ is said to be **prime** if for every $r, r' \in R$ such that $r \cdot r' \in \mathfrak{p}$, either $r \in \mathfrak{p}$ or $r' \in \mathfrak{p}$.

An ideal $\mathfrak{m} \subsetneq R$ is said to be **maximal** if there exists no ideal $I \subsetneq R$ containing $\mathfrak{m}$. That is $\mathfrak{m}$ is maximal with respect to inclusion among ideals.

In Reid, he describes prime ideals as complements of **multiplicative sets**. To realize this comparison, see Homework 1 #3.

Next, I state another way to realize primality and maximality of ideals.

Proposition 2.2. *Let R be a commutative ring.*

- *$\mathfrak{p}$ is a prime ideal if and only if $R/\mathfrak{p}$ is an integral domain.*
- *$\mathfrak{m}$ is a maximal ideal if and only if $R/\mathfrak{m}$ is a field.*

Proof.

- Suppose $\mathfrak{p}$ is not prime. Then there exist $a, b \notin \mathfrak{p}$ such that such that $a \cdot b \in \mathfrak{p}$. But this implies
$$(a + \mathfrak{p}) \cdot (b + \mathfrak{p}) = a \cdot b + \mathfrak{p} = 0 + \mathfrak{p}$$
Implying $R/\mathfrak{p}$ is not an integral domain, since $a + \mathfrak{p} \neq 0 + \mathfrak{p} \neq b + \mathfrak{p}$ in $R/\mathfrak{p}$. The reverse implication is acquired by running through this argument in reverse.

- First note that R is a field if and only if the only ideal of R is the 0 ideal. Indeed, if R is not a field if and only if there exists a non-zero non-unit element $r \in R$, and thus $\langle r \rangle$ is a non-zero ideal.

  Suppose $R/\mathfrak{m}$ is not a field. Therefore, there exists a non-zero ideal $I \subseteq R/\mathfrak{m}$. Considering the natural map
$$\varphi : R \to R/\mathfrak{m}$$
We have that $J = \varphi^{-1}(I) \subsetneq R$ is an ideal, and furthermore $\mathfrak{m} \subsetneq J$. Thus $\mathfrak{m}$ is not maximal.

  If $\mathfrak{m}$ is not maximal, suppose $\mathfrak{m} \subsetneq J \subsetneq R$, where J is an ideal. One can check that $\varphi(J) \subseteq R/\mathfrak{m}$ is a non-zero ideal; this follows directly from the definition of the operations on $R/\mathfrak{m}$. Therefore $R/\mathfrak{m}$ is not a field.

□

Corollary 2.3. *Every maximal ideal is necessarily prime.*

Definition 2.4. Given a ring R, call $\operatorname{Spec}(R)$ the set of all prime ideals of R and $\text{m-}\operatorname{Spec}(R)$ the collection of all maximal ideals.

$\operatorname{Spec}(R)$ has more structure than merely a set. At minimum it is a poset ordered by inclusion. It is in fact a topological space! We will return to this later.

Let's get into some examples:

Example 2.5. 1) If K is a field, then $\mathrm{Spec}(K) = \{0\}$ is a 1-point set.

2) It should be noted that this doesn't define fields: $R = K[x]/\langle x^n\rangle$ has the property that $\mathrm{Spec}(R) = \{\langle x\rangle\}$ is a single point. Of course, R is not even a domain!

3) If K is a field, then $\mathbb{A}^1_K = \mathrm{Spec}(K[x])$ is called the affine line (over K). Let's examine this in a few cases:

- If $K = \mathbb{C}$, or more genereally K is an algebraically closed field, then given the result of Homework 1 #4, we have that $I = \langle f\rangle$. But algebraic closedness implies
$$f = (x-\alpha_1)^{n_1}\cdots(x-\alpha_m)^{n_m}$$
As a result, the only possibility for f to be prime is the case where $m = n_1 = 1$, or f is a linear polynomial. Therefore, we can see that
$$\mathbb{A}^1_K = \{\langle x-\alpha\rangle \mid \alpha \in K\} \cup \{0\}$$
Therefore it is in bijection with K with one additional special point 0. This gives rationale to the name the affine *line*.
- If $K = \mathbb{R}$, then the situation is a bit more complicated. Still $\langle x-\alpha\rangle$ are prime for each $\alpha \in \mathbb{R}$, but now we have new irreducible polynomials, such as x^2+1. In fact, every quadratic polynomial $f = x^2+bx+c$ with $b^2-4c<0$ is irreducible (since it has complex roots). In fact, these are all of the remaining irreducibles:

$$\mathrm{Spec}(\mathbb{R}[x]) = \{\langle x-\alpha\rangle \mid \alpha \in K\} \cup \left\{\langle x^2+bx+c\rangle \mid b^2-4c<0\right\} \cup \{0\}$$

- The situation gets more complicated for other non-algebraically closed fields, such as $\mathbb{Q}$ and $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. In these cases there are in fact irreducible polynomials in every degree! In the case of $\mathbb{Q}$, this can be seen by considering $f = x^n - p$, where p is a prime (or simply square-free) integer. This is irreducible by Eisenstein's Criterion. However, we can be more explicit. Over $\mathbb{C}$,
$$f = (x - \sqrt[n]{p})\cdot(x-\zeta\cdot\sqrt[n]{p})\cdots(x-\zeta^{n-1}\cdot\sqrt[n]{p})$$
where $\zeta = e^{\frac{2\pi i}{n}}$ is an n^{th} root of unity. Of course, if we multiply any less that all of the terms together, then the constant coefficient will have the form
$$\zeta^{m'}p^{\frac{m}{n}}$$
where $m<n$, and therefore cannot possibly be rational.
The case of $\mathbb{F}_p$ can be realized by a counting argument. There are only p many irreducibles of degree 1. Therefore, since x^2+bx+c can have p^2 many values, the ones for which
$$x^2+bx+c = (x-\alpha)(x-\beta)$$
are $\binom{p+1}{2} = \binom{p}{2}+p$-many. But $p^2 - \binom{p+1}{2} = \frac{p^2-p}{2} > 0$ for every prime p. The argument continues in this way. There is a pattern to be found, c.f. the Necklace Polynomial: `https://en.wikipedia.org/wiki/Necklace_polynomial`.

Next time, we will study $\mathrm{Spec}(K[x,y])$ and $\mathrm{Spec}(\mathbb{Z}[x])$.

CLASS 3, FEBRUARY 8TH: $\mathrm{Spec}(K[x,y])$ AND $\mathrm{Spec}(\mathbb{Z}[x])$

Today I intend to compute the spectra of two 2-dimensional (to be interpreted) rings. We will cover this in bigger generality in section 4, but it is very useful to go through the details in a few cases.

Theorem 3.1. $\mathrm{Spec}(K[x,y])$ *is exactly the set of prime ideals of the following form:*

0) 0*, the zero ideal.*
1) $\langle f(x,y)\rangle$*, where* $f = f(x,y)$[1] *is an irreducible polynomial.*
2) The maximal ideals $\mathfrak{m}$*, for which* $\mathfrak{m} = \langle f(x), g(x,y)\rangle$*, and* $f = f(x)$ *is an irreducible polynomial, and* $g = g(x,y)$ *is a polynomial whose reduction* $(\mathrm{mod}\, f)$ *is irreducible in* $(K[x]/\langle f\rangle)[y]$*. This implies* $K[x,y]/\mathfrak{m}$ *is a finite field extension of* K*.*

Definition 3.2. A polynomial $f \in R[x]$, where R is a unique factorization domain (**U.F.D**), is said to be **primative** if $f = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ and a_i share no common factor.

Lemma 3.3 (Gauss's Lemma)**.** *If* R *is a U.F.D,* $f, g \in R[x]$ *are primative polynomials, then so is* $f \cdot g$*.*

Proof. Suppose $f \cdot g$ is not primative, i.e. there exists $p \in R$ such that p divides all the coefficients of $f \cdot g$. Note by assumption, p does not divide all the coefficients of f or g. Let

$$f = a_0 + a_1 x + \ldots + a_n x^n$$
$$g = b_0 + b_1 x + \ldots + b_m x^m$$

and let a_r and b_s be the first coefficients of f and g respectively not divisible by p. Then the x^{r+s} term of $f \cdot g$ reads

$$\alpha = \sum_{i+j=r+s} a_i b_j = a_r b_s + a_{r+1} b_{s-1} + \ldots + a_{r-1} b_{s+1} + \ldots$$

For $i \neq r$ and $j \neq s$, $a_i b_j$ is divisible by p by assumption. However, $a_r b_s$ is not. This implies p does not divide α, a contradiction. □

Proof. Let $R = K[x]$ and $L = K(x)$ be the ring (field) of rational functions in x. Then R is a P.I.D. and L is its field of fractions. The ring of interest is $S = K[x,y] = R[y]$. If $\mathfrak{p} \in \mathrm{Spec}(S)$, then we may assume $f_1, f_2 \in \mathfrak{p}$ are elements with no common factor in S (otherwise, they fall into case 0) or case 1).

1) f_1, f_2 also share no factors in $L[y]$.

   Suppose $f_1 = h \cdot g_1$ and $f_2 = h \cdot g_2$, with $h, g_1, g_2 \in L[y]$, $\deg(h) \geq 1$. We can factor an element of L so that the coefficients of the h, g_1, and g_2 share no common factors: $h = a h_0$, $g_1 = b_1 \gamma_1$, and $g_2 = b_2 \gamma_2$, with $a, b_1, b_2 \in L$. Now as a result of Lemma 3.3, we get that $h_0\gamma_1$ and $h_0\gamma_2$ are also primative. Therefore $f_1 = h g_1 = (a b_1)(h_0 \gamma_1) \in K[x,y]$ implies $a b_1 \in R$. Symmetrically, the same is true of $a b_2$. Therefore h_0 divides f_1 and f_2, a contradiction.

[1] calling the polynomial without variables is notationally convenient

2) If $I = \langle f_1, f_2 \rangle$, then $I \cap R \neq 0$.
   Since $L[y]$ is a P.I.D., and $gcd(f_1, f_2) = 1$, there exists $a, b \in L[y]$ such that $af_1 + bf_2 = 1$. Therefore, clearing denominators by multiplying by $c \in K[x]$,
$$0 \neq c = caf_1 + cbf_2 \in R$$
3) If $\mathfrak{p}$ is a prime ideal of $K[x,y]$, then $R \cap \mathfrak{p}$ is a prime ideal of R. This follows by Homework 1 #2, given the inclusion $R = K[x] \hookrightarrow K[x,y] = S$. By 2), we have that if $\mathfrak{p}$ is not principal, $\mathfrak{p} \cap R \neq 0$. But since R is a P.I.D., we see that $\mathfrak{p} \cap R = \langle f \rangle$ is a maximal ideal. As a result, $K[x]/\langle f \rangle$ is a field, so again
$$(K[x]/\langle f \rangle)[y] = K[x,y]/\langle f \rangle$$
is a P.I.D. Therefore, there is a $g \in K[x,y]$ irreducible so that $\mathfrak{p} = \langle f, g \rangle$.

□

Corollary 3.4. *The prime ideals of $\mathbb{Z}[y]$ are exactly*

0) 0, the zero ideal.
1) $\langle f(y) \rangle$, where $f = f(y)$ is an irreducible polynomial.
2) The maximal ideals $\mathfrak{m}$, for which $\mathfrak{m} = \langle p, f(y) \rangle$, and p is a prime number, and $f(y)$ is a polynomial whose reduction $(\mathrm{mod}\, p)$ is irreducible in $\mathbb{F}_p[y] = (\mathbb{Z}/p\mathbb{Z})[y]$. This implies $\mathbb{Z}[y]/\mathfrak{m}$ is a finite field extension of $\mathbb{F}_p$, and thus of the form $\mathbb{F}_{p^e}$.

Proof. The assertion follows precisely by replacing $R = K[x]$ with $R = \mathbb{Z}$, and $L = K(x)$ by $L = \mathbb{Q}$.[2] □

As a direct application of this result, we can see that geometric interpretation of these 2 rings:

Example 3.5 (The Affine K-Plane)**.** Suppose K is an algebraically closed field. Then we have that every maximal ideal $\mathfrak{m} = \langle f, g \rangle$, with $f \in K[x]$ irreducible, and $g(x,y)$ is irreducible $(\mathrm{mod}\, f)$. Since K is algebraically closed, we have that $f = x - \alpha$ for some $\alpha \in K$ (as in the case of $\mathbb{A}^1_K$). But then $x = \alpha \in K$ inside $(K[x]/\langle f \rangle)[y]$, so $K[x,y]/\langle f \rangle \cong K[y]$. As a result, $g = y - \beta$ (up to subtracting some multiple of f, which is fine in terms of generation of an ideal)!

Therefore, the maximal ideals are exactly given as
$$\text{m-Spec}(K[x,y]) = \{\langle x - \alpha, y - \beta \rangle \mid \alpha, \beta \in K\} \longleftrightarrow K^2.$$
This is canonically a 2-dimensional vector space over K, thus the terminology K-plane! We call
$$\mathbb{A}^2_K = \mathrm{Spec}(K[x,y])$$
the affine K-plane. The more general considerations of
$$\mathbb{A}^n_K = \mathrm{Spec}(K[x_1, x_2, \ldots, x_n])$$
behave similarly (c.f. Hilbert-Nullstellensatz), though the statement of a proposition like Theorem 3.1 is much harder.

[2]The proof can in fact be generalized to *any* P.I.D. R in its field of fractions L!

CLASS 4, FEBRUARY 11TH: EXISTENCE OF MAXIMAL IDEALS

Today we will study Zorn's Lemma, a result from logic, and show that every ring has a maximal ideal (and potentially many).

Lemma 4.1 (Zorn's Lemma)**.** *Let $\mathcal{S}$ be a non-empty partially ordered set, with the property that every ascending chain has an upper bound. Then there exists a maximal element.*

There is a little bit of information to unravel here. I state the definitions formally for your convenience.

Definition 4.2. A **partially ordered set**, or **poset**, is a collection $\mathcal{S}$ with an binary relation $\leq$ (not applicable to all elements, thus *partially*) on $\mathcal{S} \times \mathcal{S}$ satsfying the following properties for every $a, b, c \in \mathcal{S}$:

1) $a \leq a$
2) If $a \leq b$ and $b \leq a$, then $a = b$.
3) If $a \leq b$ and $b \leq c$, then $a \leq c$.

An **ascending chain** in a poset $\mathcal{S}$ are elements $a_i \ldots \in \mathcal{S}$ satisfying

$$a_1 \leq a_2 \leq a_3 \leq \ldots$$

An **upper bound** for such a chain is an element $b \in \mathcal{S}$ such that $a_i \leq b \; \forall i \in \mathbb{N}$. Finally, a **maximal element** of $\mathcal{S}$ is an element $M \in \mathcal{S}$ such that the only $N \in \mathcal{S}$ such that $M \leq N$ is $N = M$.

The result of Zorn's lemma is quite general and has applications throughout mathematics. However, instead of doing a deep dive into transfinite induction, we simply use this result to show the following result:

Theorem 4.3. *If $R \neq 0$ is a ring, then there exists $\mathfrak{m} \subsetneq R$ a maximal ideal.*

Setup 4.4. Let $\mathcal{S} = \{I \subsetneq R \text{ an ideal}\}$, and let $\leq$ denote inclusion of ideals; i.e. $I \leq J$ if and only if $I \subseteq J$. For simplicity I will refer in the following proof only to the latter operation $\subseteq$.

Proof. Note that for any ring $R \neq 0$, the set $\mathcal{S}$ is non-empty. Given $I_1 \subseteq I_2 \subseteq \ldots$ an ascending chain of ideals in $\mathcal{S}$, consider the set

$$I = \bigcup_{i=1}^{\infty} I_i$$

I claim that this is an ideal. Suppose $a, b \in I$. Then $a \in I_i$ and $b \in I_j$ for some $i, j \in \mathbb{N}$, and therefore $a, b \in I_{\max(i,j)}$. But this is an ideal, and therefore, $a + b \in I_{\max(i,j)} \subseteq I$.

Similarly, if $r \in R$ and $a \in I_i \subseteq I$, then $r \cdot a \in I_i \subseteq I$ since I_i is an ideal.

Finally, note that a subset $I \subseteq R$ satisfying these properties is *equal* to R if and only if it contains 1. Since I_i are ideals, none of them contain 1, and therefore I also doesn't contain 1. Therefore I is an upper bound for the above chain.

As a result of Lemma 4.1, we see that the set $\mathcal{S}$ contains a maximal element, which is exactly the definition of a maximal ideal. $\square$

Note that with a subtle manipulation to our setup, we can prove a greater result.

Theorem 4.5. *Given $I \subsetneq R$ an ideal, there exists $\mathfrak{m} \subsetneq R$ a maximal ideal containing I.*

Proof. The same proof goes through replacing $\mathcal{S} = \mathcal{S}_I = \{J \subsetneq R \text{ an ideal} \mid I \subset J\}$. □

This gives us a very nice way to break up the structure of a ring:

Corollary 4.6. *Given $R \neq 0$ a ring, we have that*

$$R = R^\times \cup \bigcup_{\mathfrak{m} \in m\text{-}\operatorname{Spec}(R)} \mathfrak{m} = R^\times \cup \bigcup_{\mathfrak{p} \in \operatorname{Spec}(R)} \mathfrak{p}$$

The $\cup$ are in fact disjoint unions.

Here I am denoting by $R^\times$ the set of (multiplicative) units in R.

Proof. Given $f \in R$, f is a unit if and only if $f \cdot g = 1$ for some $g \in R$, which occurs if and only if $\langle f \rangle = R$.

As a result, if $f \notin R^\times$, then $\langle f \rangle \neq R$ is an ideal. Thus there exists some maximal ideal $\mathfrak{m}$ containing $\langle f \rangle$. So $f \in \bigcup_{\mathfrak{m} \in \text{m-}-\operatorname{Spec}(R)} \mathfrak{m}$.

The second equality is trivial, since each $\mathfrak{p} \subseteq \mathfrak{m}$ for some $\mathfrak{m} \in \text{m-} - \operatorname{Spec}(R)$. □

As one final application of Zorn's Lemma, we have a powerful result that will tell us the structure of certain *localized* rings later on.

Theorem 4.7. *Let $R \neq 0$ be a ring, and S a multiplicative subset (c.f. Homework 1 #3). Then if I is an ideal of R disjoint from S (meaning $I \cap S = \emptyset$), then there exists a prime ideal $\mathfrak{p} \in \operatorname{Spec}(R)$ such that $\mathfrak{p}$ is disjoint from S and $I \subseteq \mathfrak{p}$.*

Proof. First, consider the set $\mathcal{S} = \{I \subsetneq R \text{ an ideal} \mid S \cap I = \emptyset\}$. It is clear that this set is non-empty, since it contains I. Similar to the previous proof, given $I_1 \subseteq I_2 \subseteq \dots$ an ascending chain in $\mathcal{S}$, we have that $I = \cup_{i=1}^{\infty} I_i$ is again an ideal in $\mathcal{S}$. Therefore, there exists a maximal element $\mathfrak{p} \in \mathcal{S}$.

I assert that $\mathfrak{p}$ is a prime ideal. Suppose $f, g \notin \mathfrak{p}$ but $f \cdot g \in \mathfrak{p}$. Then we can consider

$$\mathfrak{p} + \langle f \rangle = \{a + r \cdot f \mid r \in R, a \in \mathfrak{p}\}$$

and similarly $\mathfrak{p} + \langle g \rangle$. These are again ideals, and they contain $\mathfrak{p}$. Therefore, by assumption of maximality, we have that $\exists a + rf \in S \cap \mathfrak{p} + \langle f \rangle$ and $\exists b + r'g \in S \cap \mathfrak{p} + \langle g \rangle$. But S is a multiplicative set, so

$$(a + rf)(b + r'g) = ab + ar'g + brf + rr'fg \in S$$

Note that $ab, ar'g, brf \in \mathfrak{p}$ since $a, b \in \mathfrak{p}$. Similarly, $rr'fg \in \mathfrak{p}$ since $fg \in \mathfrak{p}$ by assumption. So $(a + rf)(b + r'g) \in \mathfrak{p} \cap S$, contradicting our assumptions. This proves the result. □

Example 4.8. $R = K[x, y]$ and $S = \{1, x, x^2, x^3, x^4, \dots\}$. Then an example of an ideal disjoint from S not contained in a larger ideal is $\langle y - \alpha \rangle$ and $\langle x - \beta \rangle$ for $\beta \neq 0$, which are indeed prime. Other examples are also possible, and in fact one can detect that

$$\{\mathfrak{p} \in \operatorname{Spec}(R) \mid S \cap \mathfrak{p} = \emptyset\} = \{\mathfrak{p} \in \operatorname{Spec}(R) \mid x \notin \mathfrak{p}\}$$

CLASS 5, FEBRUARY 13TH: RADICALS AND ZERO DIVISORS

Next up we will study the radical of a given ideal, and see how it relates to zero divisors generally speaking. We will also study a particular case of the radical, the nilradical, and see how it relates to prime ideals.

Definition 5.1. Given $I \subsetneq R$ an ideal, the **radical** of I is

$$\sqrt{I} := \{f \in R \mid f^n \in I \text{ for some } n \in \mathbb{N}\}$$

Note the following easy consequences:

- If $\mathfrak{p}$ is prime, then $\sqrt{p} = \mathfrak{p}$.
- If $I \subseteq J$, then $\sqrt{I} \subseteq \sqrt{J}$

There is also a special version of the radical, which gets its own name:

Definition 5.2. The **nilradical** of R is the radical of 0:

$$nil(R) = \sqrt{0} = \{f \in R \mid f^n = 0 \text{ for some } n \in \mathbb{N}\}$$

As its name incurs, it is precisely the set of nilpotent elements of R. It turn out that we only need to study the nilradical of rings to acquire information about the radical of more arbitrary ideals.

Proposition 5.3. *Given the quotient map $\varphi : R \to R/I$, we can compute the radical of I as*

$$\sqrt{I} = \varphi^{-1}(nil(R/I)) = nil(R/I) + I$$

Proof. On the right-hand side, we have elements $f+I$ such that $(f+I)^n = f^n + I = 0 + I$. This is exactly saying the $f^n \in I$. The result is immediately clear. □

As a result, we are able to more easily focus on the nilradical and derive results about the radical under this relationship. The first interesting result concerns how prime ideals relate to the nilradical:

Theorem 5.4. *The nilradical is the intersection of prime ideals:*

$$nil(R) = \bigcap_{\mathfrak{p} \in \mathrm{Spec}(R)} \mathfrak{p}$$

Proof. The result follows by application of Theorem 4.7 from last class.

For the easy direction, note that if $f^n = 0$, then since $0 \in \mathfrak{p}$ for any *ideal* $\mathfrak{p}$, if $\mathfrak{p}$ is prime we see that either $f \in \mathfrak{p}$ or $f^{n-1} \in p$. Induction allows us to conclude that $f \in \mathfrak{p}$ in either case. Therefore, $f \in nil(R)$ implies $f \in \bigcap_{\mathfrak{p} \in \mathrm{Spec}(R)} \mathfrak{p}$.

Now suppose f is not nilpotent. It suffices to check that there exists $\mathfrak{p} \in \mathrm{Spec}(R)$ such that $f \notin \mathfrak{p}$ as this will imply $f \notin \bigcap_{\mathfrak{p} \in \mathrm{Spec}(R)} \mathfrak{p}$. Note that being non-nilpotent implies that

$$0 \notin S = \{1, f, f^2, f^3, \ldots\}$$

and therefore S satisfies the properties of a multiplicative set. Since 0 is an ideal in any ring, and $S \cap 0 = \emptyset$, there exists a prime ideal $\mathfrak{p}$ of R disjoint from S. Thus $f \notin \mathfrak{p}$ as asserted. □

We can 'upgrade' this to a statement about radicals if we examine more carefully the statement of Homework 1 #2. We know that the map $\mathrm{Spec}(R/I) \hookrightarrow \mathrm{Spec}(R)$ is injective. It's image is exactly

$$\varphi^{\#}(\mathrm{Spec}(R/I)) = \{\mathfrak{p} \in \mathrm{Spec}(R) \mid I \subseteq \mathfrak{p}\}$$

This can be realized directly by considering what the preimage of an ideal is.

Corollary 5.5. *The radical of an ideal is the intersection of the prime ideal containment:*

$$\sqrt{I} = \bigcap_{I \subseteq \mathfrak{p} \in \mathrm{Spec}(R)} \mathfrak{p}$$

Proof. Following the realization above, we see that by Theorem 5.4

$$\sqrt{I} = \varphi^{-1}(nil(R/I)) = \varphi^{-1}\left(\bigcap_{\mathfrak{p} \in \mathrm{Spec}(R/I)} \mathfrak{p}\right) = \bigcap_{\mathfrak{p} \in \mathrm{Spec}(R/I)} \varphi^{-1}(\mathfrak{p}) = \bigcap_{I \subseteq \mathfrak{p} \in \mathrm{Spec}(R)} \mathfrak{p}$$

□

Lastly, I would like to talk about other types of zero divisors than nilpotents.

Example 5.6. The ring $R = K[x,y]/\langle xy \rangle$ is a ring with no nilpotents (called a **reduced ring**). However, we can clearly multiply x and y, both non-zero in the ring, and end up with zero!

By the realization above, $\mathrm{Spec}(R) = \{\mathfrak{p} \in \mathrm{Spec}(K[x,y]) \mid \langle xy \rangle \subseteq \mathfrak{p}\}$. By definition of primality, this implies either $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$ (or both). These can be described respectively as $\mathrm{Spec}(K[x,y]/\langle x \rangle) = \mathrm{Spec}(K[y])$ and $\mathrm{Spec}(K[x,y]/\langle y \rangle) = \mathrm{Spec}(K[x])$. By our computation of $\mathrm{Spec}(K[x,y])$ from Class 3, this implies $\mathrm{Spec}(R)$ can be decomposed as follows:

$$\mathrm{Spec}(R) = \mathrm{Spec}(K[y]) \cup \mathrm{Spec}(K[x]) = \mathbb{A}^1_K \cup \mathbb{A}^1_K$$

Their intersection is prime ideals containing both x and y, i.e. $\langle x, y \rangle$!

This example is a specific case of the following Proposition:

Proposition 5.7. *If R is a ring containing zero divisors, then either $nil(R) \neq 0$ or R has more than one minimal prime.*

Finally, a quick word about **idempotent** elements. Recall these are elements $e \in R$ such that $e^2 = e$. The canonical example is a projection operator in linear algebra. The neat thing about these elements is as follows:

Proposition 5.8. *R has an idempotent element $e \neq 0, 1$ if and only if R is a direct sum/cartesian product of 2 rings R_1, R_2.*

Proof. I claim $R \cong eR \oplus (1-e)R$. This is seen by taking homomorphisms

$$\varphi : R \to eR \oplus (1-e)R : r \mapsto (e \cdot r, (1-e)r)$$
$$\psi : eR \oplus (1-e)R \to R : (r,s) \mapsto r + s$$

The only thing to note here is that

$$\varphi(r \cdot s) = (ers, (1-e)rs) = (e^2rs, (1-2e+e^2)rs) = (er \cdot es, (1-e)r(1-e)s)$$
$$= (er, (1-e)r) \cdot (es, (1-e)s) = \varphi(r) \cdot \varphi(s)$$

□

CLASS 6, FEBRUARY 18TH: LOCAL RINGS

Today we will look at a certain classification of rings determined by the shape of $\mathrm{Spec}(R)$. Local rings determine the structure of rings near a given prime ideal. We will see this comparison in more detail later on.

Definition 6.1. A ring is said to be **local** if there exists only a single maximal ideal $\mathfrak{m} \subsetneq R$. In this case, we often write $(R, \mathfrak{m})$ to indicate the ring, of even $(R, \mathfrak{m}, k)$, where $k = R/\mathfrak{m}$ is the residue field at $\mathfrak{m}$ of R.

There are a few methods to detect when a ring is local:

Proposition 6.2. *Let R be a ring. Then TFAE:*

1) *R is a local ring with maximal ideal $\mathfrak{m}$.*
2) *$R \setminus R^\times$, the complement of the set of units of R, forms a proper ideal (namely $\mathfrak{m}$).*
3) *Everything of the form $1 + \alpha$, with $\alpha \in \mathfrak{m}$, is a unit.*

Proof. 1) $\leftrightarrow$ 2) : Note that the units form a multiplicative set, so there exists a maximal ideal containing the ideal generated by every non-unit. As a result, since there is only 1 maximal ideal, $\mathfrak{m}$ contains every non-unit! Of course $\mathfrak{m}$ contains no units, so $\mathfrak{m} = R \setminus R^\times$ is an ideal.

2) $\rightarrow$ 3) : If $\alpha \in \mathfrak{m}$, then $1 + \alpha \notin \mathfrak{m}$. Otherwise, $1 \in \mathfrak{m}$ by additive closure. Therefore, by 2), $1 + \alpha$ is a unit.

3) $\rightarrow$ 2) : Suppose the condition of 2) is not satisfied. Namely, suppose there exist r, r' non-units such that $r + r'$ is a unit. Let u be its multiplicative inverse. Then

$$u(r + r') = ur + ur' = 1$$

But as a result, we have $1 - ur = ur'$, and $ur \in \mathfrak{m}$ since r is. As a result, since r' was not itself a unit, we note neither is ur' and thus $1 - ur$ is a non-unit. This implies 3) is false as claimed.

□

Now we turn to the idea of localization, at least in the case of an integral domain.

Definition 6.3. If R is an integral domain, $\mathfrak{p}$ is a prime ideal of R, then we define

$$R_\mathfrak{p} = \left\{ \frac{f}{g} \in Frac(R) \mid f, g \in R, g \notin \mathfrak{p} \right\}$$

with the standard method of adding and multiplying such fractions.

Note that these group structures are well defined, c.f. Homework 3 #1. In addition, everything outside of $\mathfrak{p}$ is made invertible! Therefore, by Proposition 6.2, $\mathfrak{p} \cdot R_\mathfrak{p}$ is the unique unique maximal ideal of $R_\mathfrak{p}$!

First, the integers.

Example 6.4. Consider the ring $R = \mathbb{Z}$, and let $\mathfrak{p}$ be a prime ideal. If $\mathfrak{p} = 0$, then we invert every non-zero element. As a result,

$$\mathbb{Z}_{\langle 0 \rangle} = \mathbb{Q}$$

If $\mathfrak{p} = \langle p \rangle$, where p is a prime number, then we invert everything not divisible by p. The effect is

$$\mathbb{Z}_{\langle p \rangle} = \mathbb{Z}\left[\frac{1}{2}, \frac{1}{3}, \frac{1}{5}, \ldots, \widehat{\frac{1}{p}}, \ldots\right]$$

Here the *hat*-symbol $\widehat{\cdot}$ denotes 'omit this element from the list'. By Homework 3 #2,$\mathbb{Z}_{\langle p \rangle}$ is an integral domain with exactly 2 prime ideals:

$$\operatorname{Spec}(\mathbb{Z}_{\langle p \rangle}) \cong \{0, \langle p \rangle\}$$

Next polynomial rings:

Example 6.5. Consider $R = K[x, y]$ and $\mathfrak{m} = \langle x, y \rangle$. Then

$$R_{\mathfrak{m}} = \left\{ \frac{p(x,y)}{q(x,y)} \mid q(x,y) \notin \mathfrak{m} \right\}$$

It is easy to check that $q(x, y) \notin \mathfrak{m}$ if and only if $q(0, 0) \neq 0$. Again utilizing Homework 3 #2, we see that

$$\operatorname{Spec}(R_{\mathfrak{m}}) \cong \{\mathfrak{p} \in \operatorname{Spec}(R) \mid \mathfrak{p} \subseteq \mathfrak{m}\}$$

So again $R_{\mathfrak{m}}$ has one minimal prime ideal and one maximal ideal. Here however, there are many primes in between. If we reduce our attention to $\mathbb{C}$, then an example of such polynomials are $x^2 - y^3$ and $y^2 - x(x + 1)(x - 1) = y^2 - x^3 - x$. I leave it to you as Homework 3 #3 to verify this statement.

The final example I would like to study is that of a power series ring.

Example 6.6. Recall that $R = K[\![x_1, x_2, \ldots, x_n]\!]$ is the ring of formal power series in K. That is to say, it has elements of the form

$$f = \sum_{\boldsymbol{\alpha} \geq \mathbf{0}} c_{\boldsymbol{\alpha}} \boldsymbol{x}^{\boldsymbol{\alpha}}$$

Here a quick word about multi-indices. $\boldsymbol{x}$ denotes $(x_1, x_2, \ldots, x_n)$, and $\boldsymbol{\alpha}$ denotes $(\alpha_1, \alpha_2, \ldots, \alpha_n)$, a set of non-negative integers. $c_{\boldsymbol{\alpha}}$ is simply an element of K, and $\boldsymbol{x}^{\boldsymbol{\alpha}} = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. In particular, power series allow terms to have non-zero coefficients indefinitely, unlike the case of polynomials.

I claim that R is already a local ring, with maximal ideal $\mathfrak{m} = \langle x_1, \ldots, x_n \rangle$. This is proved, using Proposition 6.2, by demonstrating that $f \in R$ with non-zero constant coefficient is a unit. This is the content of Homework 3#4.

The procedure of creating R from $K[x_1, x_2, \ldots, x_n]$ is called completion at the maximal ideal $\langle x_1, \ldots, x_n \rangle$. This should be thought of as an even more local version of localization.

Next time, we will begin to study modules.

CLASS 7, FEBRUARY 20TH: MODULES

As with many fields of the mathematics, many times the objects of interest are really the structures you can put on top of another more common object. This immediately makes modules an intellectually profitable realm of study.

Definition 7.1. A **module** over a commutative ring R is an abelian group $(M, +)$ with multiplication $\cdot : R \times M \to M$, such that for all $r, s \in R$ and $m, m' \in M$:

1) R**-Distributive:** $(r + s) \cdot m = rm + sm$.
2) M**-Distributive:** $r \cdot (m + m') = rm + rm'$.
3) **Associative:** $(rs)m = r(sm)$.
4) **Unital:** $1 \cdot m = m$.

M is often referred to as an R**-module**.

The next few examples show the prevalence of R-modules:

Example 7.2 (**Vector Spaces).** If V is a vector space over a field K, then V is also a module over K. So you can view $\mathbb{R}^n$ as a $\mathbb{R}$-module. In fact, every K-module is a vector space!

More generally, every vector space is a free K-module:

Definition 7.3. A module M of R is called **free** if

$$M = R^{\oplus\Lambda} = R^{\Lambda} = \{(r_\lambda)_{\lambda\in\Lambda} \mid r_\lambda \in R,\ r_\lambda = 0 \text{ for all but finitely many } \lambda\}$$

Modules also unify the notions of this class so far!

Example 7.4 (**Ideals).** If I is an ideal of R, then I is naturally an R-module. In fact, it inherits all of the above properties from R! In particular, R is an R-module. We can say I is a **submodule** of R if we want to keep track of where it lives.

Example 7.5 (**Ring Homomorphisms).** Let $\varphi : R \to S$ be a ring homomorphism. Then S can be viewed as an R-module via the following action:

$$r \cdot s = \varphi(r)s$$

where the second multiplication is simply multiplication in S. One checks respectively:

1) $(r + r') \cdot s = \varphi(r + r')s = (\varphi(r) + \varphi(r'))s = \varphi(r)s + \varphi(r')s = r \cdot s + r' \cdot s$.
2) $r \cdot (s + s') = \varphi(r)(s + s') = \varphi(r)s + \varphi(r)s' = rs + rs'$
3) It is associative since S-multiplication is.
4) $\varphi(1_R) = 1_S$.

More generally, this shows that every S-module can naturally be made into an R-module.

An additional example is in fact a subset of a major theorem.

Example 7.6 (**Abelian groups).** There is a natural bijection between the set of Abelian groups and the set of $\mathbb{Z}$-modules. Given an Abelian group G, we have a $\mathbb{Z}$-action given by

$n \cdot g = ng \in G$, given by applying the G group operation n times to g: $ng = g+g+\ldots+g$. In addition, the conditions of being a module at all are to be an abelian group under $+$.

Because for any unital ring R we have a natural map $\mathbb{Z} \to R : 1 \mapsto 1_R$, every R-module is a $\mathbb{Z}$-module by Example 7.5.

Next up, we study maps of modules, and what the compatible structure should be.

Definition 7.7. Let M and N be R-modules. Then an **R-module homomorphism** from M to N is a map $\varphi : M \to N$ such that

- $\varphi(m + m') = \varphi(m) + \varphi(m')$
- $\varphi(rm) = r\varphi(m)$

In addition, we define the following quantities to a module homomorphism:

- $\ker(\varphi)$ to be the set of $m \in M$ such that $\varphi(m) = 0$.
- $\mathrm{im}(\varphi)$ is the set of $n \in N$ such that there exists $m \in M$ with $\varphi(m) = n$.

In the case that $\ker(\varphi) = 0$ and $\mathrm{im}(\varphi) = N$, we call φ an **isomorphism**. Finally, we call the group of module homomorphisms $\mathrm{Hom}_R(M, N)$.

We can immediately say even more:

Proposition 7.8. *The set* $\mathrm{Hom}_R(M, N)$ *has the structure of an R-module.*

Proof. We give it the structure of an R-module as follows: We define

$$\varphi + \psi : M \to N : m \mapsto \varphi(m) + \psi(m)$$
$$r\varphi : M \to N : m \mapsto r\varphi(m)$$

One quickly verifies the axioms of a module based on that of M and N. □

Example 7.9. There is a natural isomorphism of R-modules between $\mathrm{Hom}_R(R, M)$ and M, given by $\varphi \mapsto \varphi(1)$ and $m \mapsto (\varphi : R \to M : 1 \mapsto m)$.

Next up, I summarize a few results which are very similar to the case of rings.

Definition 7.10. A subset $N \subseteq M$ is called a **submodule** of M if N is a module in it's own right. That is, $rn_1 + n_2 \in N$ if $n_1, n_2 \in N$ and $r \in R$.

We can then consider M/N to be the set of cosets of N inside M (as abelian groups). This is a R-module in it's own right.

Proposition 7.11. *If $N, N' \subseteq M$ are submodules, then $N + N'$ and $N \cap N'$ are also submodules.*

Proof. Homework 3, #6. □

Finally, this allows us to write down the module isomorphism theorems. The proofs of each are almost identical to the case of rings/groups.

Theorem 7.12. *1) If $\varphi : M \to N$, then $M/\ker(\varphi) \cong Im(\varphi)$.*

2) If $N, N' \subseteq M$ are submodules, then

$$(N + N')/N' \cong N/N \cap N'$$

3) If $N \subseteq N' \subseteq M$ are a chain of submodules, then

$$(M/N)/(N'/N) \cong M/N'$$

4) If $N \subseteq M$, then there is a natural bijection

$$\{\textit{submodules of } M \textit{ containing } N\} \leftrightarrow \{\textit{submodules of } M/N\}$$

CLASS 8, FEBRUARY 22TH: GENERATION & CAYLEY-HAMILTON

As with groups, we have a notion of generators and relations upon which we can devise the structure of any given module. We can show this directly using some of the isomorphism theorems for modules:

Proposition 8.1. *Every module M can be described by a set of generators m_α and some corresponding relations:*

$$M = \langle m_\alpha \rangle = \left\{ \sum_\alpha r_\alpha m_\alpha \mid r_\alpha \in R, \text{ all but finitely many } = 0 \right\} / \{\textit{Relations in } M\}$$

Proof. Consider the free module $R^{\oplus M}$, which has as elements

$$\{(r_m)_{m \in M} \mid r_m \in R, \text{ all but finitely many } = 0\}$$

Then there exists a natural surjection

$$\varphi : R^{\oplus M} \to M : (r_m) \to r_m \cdot m$$

It is surjective because $\varphi(1_m) = m$. In fact, by the first isomorphism theorem, we have

$$R^{\oplus M} / \ker(\varphi) \cong \mathrm{im}(\varphi) = M.$$

So $\ker(\varphi)$ is exactly the set of relations in the module M. This completes the proof. □

In practice, this is very overkill for describing the module M. Usually the number of generators is much smaller than the size of M itself :)

Example 8.2. $\mathbb{Q}$ has the natural structure of a $\mathbb{Z}$-module. It has generators $\frac{1}{n}$ for $n \in \mathbb{N}$. However, there are relationships, like

$$5 \cdot \frac{1}{10} = \frac{1}{2}$$

So again, some (most?) of the generators are superfluous.

Definition 8.3. Let Λ be a set. R is **$|\Lambda|$-generated** if there exists a surjection $R^\Lambda \to M$. If Λ can be made finite, we say M is **finitely-generated**.

Most modules of interest are finitely generated. This is because, much like in the case of linear algebra, finitely generated modules (finite dimensional vector spaces) behave much more reasonably than infinitely generated ones (infinite dimensional VSs).

Example 8.4. We can consider the ring $R = \mathbb{F}_p[x]$, and consider the Frobenius map $F : R \to R : f \mapsto f^p$. This is a ring homomorphism, which makes R into an R module with the funny structure $x \cdot y = F(x)y = x^p y$. To avoid confusion, call this module $F_* R$.

It is a simple check that $F_* R$ is a finitely-generated free module, with exactly p-generators: $1, x, \ldots, x^{p-1}$. This can be seen as follows: if $f = \sum_{i=0}^n c_i x^i$, then we can rewrite this as

$$f = \sum_{m=0}^{\lfloor n/p \rfloor} \sum_{l=0}^{p-1} c_{mp+l} x^{mp+l} = \sum_{l=0}^{p-1} \left(\sum_{m=0}^{\lfloor n/p \rfloor} c_{mp+l} x^m \right) \cdot x^l =$$

This phenomenon is the basis of a great deal of (my own) research.

Now, for the rest of class I would like to build up a beautiful result, known as the determinant trick, which will provide the building blocks to prove Nakayama's Lemma next class.

Theorem 8.5 (The Determinant Trick)**.** *Suppose M is an n-generated R-module, and $\varphi : M \to M$ is an R-linear map. If there exists an ideal I with $\varphi(M) \subseteq IM$, then there is a (monic!) polynomial*

$$p(x) = x^n + a_1 x^{n-1} + \ldots + a_n \in R[x]$$

with $a_i \in I^i$ for each i and such that $p(\varphi) = 0$ as an operator on M.

I recommend comparing this with the Cayley-Hamilton Theorem from linear algebra:

Theorem 8.6 (Cayley-Hamilton)**.** *If M is a $n \times n$ matrix with entries in a field K, then*

$$p(x) = \det(x \cdot I_n - M)$$

is a polynomial of degree n such that $p(M) = 0$ as an operator on K^n.

The determinant trick not only upgrades this theorem to allow K an arbitrary ring, but also the free module can be ANY module! Note that if we allow $I = R$ in the Determinant Trick, then Cayley-Hamilton is returned.

Proof. Given that $M = \langle m_1, \ldots, m_n \rangle$, and $\varphi(m) \in IM$ for every $m \in M$, we have

$$\varphi(m_i) = \sum_{j=1}^{n} r_{ij} m_j$$

where $r_{ij} \in I$. Therefore, we can write $\sum_{j=1}^{n} \varphi \circ \delta_{i,j} - r_{ij}$ applied to m_i is 0, where $\delta_{i,j}$ is the Dirac delta function: $\delta_{i,j} = 1$ if $i = j$ and is 0 otherwise.

Therefore, we can form an $n \times n$ matrix Λ where the (i,j)-entry is exactly $\varphi \circ \delta_{i,j} - r_{ij}$. This matrix multiplies the vector $m = (m_1, \ldots, m_n)^T$ to zero by design.

Definition 8.7. The **adjugate** of an $n \times n$ matrix M has its (i,j)-entry as $(-1)^{i+j}$ times the determinant of the matrix M with the j^{th} row and i^{th} column omitted.

If we multiply $Adj(\Lambda) \cdot \Lambda$, we get $\det(\Lambda) Id$. Therefore, this has a wonderful property that the inverse of a matrix Λ is given by $\frac{1}{\det(\Lambda)} Adj(\Lambda)$ (if it exists). However, in our case this shows that

$$\det(\Lambda) Id \cdot m = Adj(\Lambda) \cdot \Lambda \cdot m = Adj(\Lambda) \cdot 0 = 0$$

Therefore, since m_i are generators, either $M = 0$ (and we are done) or $m_i \neq 0$ and we get $\det(M) = 0$. But $\det(M)$ is a degree n polynomial in φ. This proves the claim. $\square$

CLASS 9, FEBRUARY 25TH: NAKAYAMA'S LEMMA

Last time we proved the determinant trick. This allows us to determine a sufficient condition as to whether a module is annihilated by a given element of R.

Theorem 9.1 (Nakayama's Lemma 1)**.** *If I is an ideal of R and M is a finitely generated module such that $IM = M$, then $\exists r \equiv 1 \pmod{I}$ such that $rM = 0$.*

Proof. Consider the map $\varphi = Id_M$. The assumption of Nakayama's lemma ensures that $Id(M) \subseteq IM$, so we get a polynomial

$$p(1) = 1 + r_1 + \ldots + r_n$$

for which $p(1)m = 0$ for every $m \in M$. But $p(1) \equiv 1 \pmod{I}$, since each $r_i \in I$. This completes the proof. □

As a quick side note, the term **annihilated** above is actually a standard term in commutative algebra.

Definition 9.2. If M is an R-module, then we define the annihilator of M as

$$\mathrm{Ann}_R(M) = \{r \in R \mid r \cdot M = 0\}$$

That is to say $r \in \mathrm{Ann}_R(M)$ iff $r \cdot m = 0$ for every $m \in M$

It should be checked that $\mathrm{Ann}_R(M)$ is a proper ideal of R. In fact, we can naturally give M the structure of an $R/\mathrm{Ann}_R(M)$-module! Thus Nakayama implies the existence of $1 + \alpha \in \mathrm{Ann}_R(M)$ for $\alpha \in I$. Next, I state come other corollaries of Theorem 9.1.

Corollary 9.3 (Nakayama's Lemma 2)**.** *If $(R, \mathfrak{m})$ is a local ring and M is a finitely generated R-module, then $M = \mathfrak{m}M$ implies $M = 0$.*

Proof. We know that $(R, \mathfrak{m})$ is local if and only if everything of the form $1 + m$ is a unit, with $m \in \mathfrak{m}$. As a result, if $M = \mathfrak{m}M$, Theorem 9.1 implies some unit $1 + m$ annihilates M. But this implies

$$M = 1M = (1 + m)^{-1}(1 + m) \cdot M = (1 + m)^{-1} \cdot 0 = 0$$

□

Corollary 9.4 (Nakayama's Lemma 3)**.** *If $(R, \mathfrak{m})$ is a local ring and $N \subseteq M$ are finitely generated R-modules, then $M = \mathfrak{m}M + N$ implies $M = N$.*

The proof of this is left as a Homework 4 #4. As a direct result, we see the following:

Theorem 9.5 (Nakayama's Lemma 4)**.** *Let $(R, \mathfrak{m})$ be a local ring and M a finitely generated R-module. If $m_1, \ldots, m_n \in M$ are such that $\langle \bar{m}_1, \ldots, \bar{m}_n \rangle = M/\mathfrak{m}M$, then $M = \langle m_1, \ldots, m_n \rangle$.*

Proof. Given the setup, we note that $M = \langle m_1, \ldots, m_n \rangle + \mathfrak{m}M = \mathfrak{m}M + \langle m_1, \ldots, m_n \rangle$. By Corollary 9.4, the result is implied directly: $M = \langle m_1, \ldots, m_n \rangle$. □

One other neat application of Theorem 9.5 is the following, which is known in general due to Vasconcelos.

Proposition 9.6. *If $\varphi : M \to M$ is a surjective R-module homomorphism, then it is also injective.*

This is very similar to the case of finite dimensional vector spaces.

Proof. We can give M the structure of an $R[x]$-module by allowing x to act by φ:

$$(r_n x^n + \ldots + r_1 x + r_0)m := r_n \varphi^n(m) + \ldots + r_1 \varphi(m) + r_0$$

The surjectivity assumption is stating that $I = \langle x \rangle$ has the property that $M = IM$. Theorem 9.1 now implies that $\exists p(x) \in R[x]$ such that $1 - p(x) = x \cdot q(x)$ and $p(x) \cdot m = 0$ for every $m \in M$. Note that $x \cdot q(x)m = m$. Therefore, $x \cdot m = \varphi(m) \neq 0$ for every $m \in M$. This is an equivalent formulation of injectivity! □

This allows us to conclude a wonderful result about finite free R-modules similar to the case of Vector spaces.

Theorem 9.7 (Invariance of Rank)**.** *If R is an integral domain, and $R^n \cong R^m$ as R-modules for $n, m \in \mathbb{N}$, then $n = m$.*

Proof. I start by assuming that R is a local ring with maximal ideal $\mathfrak{m}$. In this case, note that if $R^n \cong R^m$ as R-modules, then we can conclude that $(R/\mathfrak{m})^n \cong (R/\mathfrak{m})^m$ as $R/\mathfrak{m}$-modules. This follows precisely by Theorem 9.5. But this is an isomorphism of finite dimensional vector spaces! As a result, $m = n$.

Now to get to the case of general rings, we use the fact that there exists a maximal ideal for any ring R. So we can localize everything in sight at $\mathfrak{m}$. This reduces us to the previous case and proves the claim. □

Note: Once we develop the notion of localization in full generality (e.g. for non-domains and for arbitrary modules), we can remove the 'domain' condition from the previous result. We can also make similar statements to Nakayama's Lemma for any ring.

Finally, this result allows us to define the rank of a free R-module.

Definition 9.8. The **rank** of a free module $M \cong R^n$ is n.

CLASS 10, FEBRUARY 27TH: EXACTNESS AND SPLITTINGS

To finish up with an introduction to modules, we turn to the idea of an exact sequence. This unifies several important notions into one compact clause, including injectivity, surjectivity, and an isomorphism theorem.

Definition 10.1. Let $\varphi : M \to N$ be a module homomorphism.

$$\ker(\varphi) = \{m \in M \mid \varphi(m) = 0\}$$

$$\operatorname{im}(\varphi) = \{n \in N \mid \exists m \in M \text{ such that } \varphi(m) = n\}$$

$\ker(\varphi) \subseteq M$ and $\operatorname{im}(\varphi) \subseteq N$ are submodules, so we can also quotient:

$$\operatorname{coim}(\varphi) = M/\ker(\varphi)$$

$$\operatorname{coker}(\varphi) = N/\operatorname{im}(\varphi)$$

Now for the definition of exactness:

Definition 10.2. If $\varphi : M' \to M$ and $\psi : M \to M''$ are 2 homomorphisms, we say that the **sequence**

$$M' \xrightarrow{\varphi} M \xrightarrow{\psi} M''$$

is **exact** if $\ker(\psi) = \operatorname{im}(\varphi) \subseteq M$. We can do this at infinitum:

$$\ldots \xrightarrow{\varphi_{-2}} M_{-2} \xrightarrow{\varphi_{-1}} M_{-1} \xrightarrow{\varphi_0} M_0 \xrightarrow{\varphi_1} M_1 \xrightarrow{\varphi_2} M_2 \xrightarrow{\varphi_3} \ldots$$

is an **exact sequence** if $\ker(\varphi_i) = \operatorname{im}(\varphi_{i-1})$ for every $i \in \mathbb{Z}$.

This notion gives a proper generalization of several notions we have already spoken about:

Proposition 10.3 (Exactness vs other properties of maps)**.**

1) *A sequence* $0 \to M \xrightarrow{\varphi} N$ *is exact if and only if* φ *is injective.*
2) *A sequence* $M \xrightarrow{\varphi} N \to 0$ *is exact if and only if* φ *is surjective.*
3) *A sequence* $0 \to M \xrightarrow{\varphi} N \to 0$ *is exact if and only if* φ *is an isomorphism.*
4) *A sequence* $0 \to M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \to 0$ *is exact if and only if* φ *is injective,* ψ *is surjective, and* $M' = \ker(\psi)$ *(or equivalently* $M'' = \operatorname{coker}(\varphi) = M/M'$*). This is special enough to give it's own name, a* **short exact sequence***. We also call* M *an* **extension** *of* M'' *by* M'*.*

Proof. 1) $0 \to M \xrightarrow{\varphi} N$ is exact if and only if $\ker(\varphi) = \operatorname{im}(0 \to M) = 0$ if and only if φ is injective.

2) $M \xrightarrow{\varphi} N \to 0$ is exact if and only if $N = \ker(N \to 0) = \operatorname{im}(\varphi)$ if and only if φ is surjective.

3) This follows directly from the previous 2 parts.

4) The only new piece of information here is that $M'' = M/M'$. Since $M \xrightarrow{\psi} M''$ is a surjective map, we know that

$$M'' \cong M/\ker(\psi) \cong M/\operatorname{im}(\varphi) \cong M/M'.$$

□

Example 10.4.
- Given ANY R-modules M, N, we can form the exact sequence
$$0 \to M \to M \oplus N \to N \to 0$$
where we send m to $(m, 0)$ and (m, n) to n.
- The following is an exact sequence of $\mathbb{Z}$-modules:
$$0 \to \mathbb{Z} \xrightarrow{\cdot n} \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \to 0$$
- As $\mathbb{Z}$ or $\mathbb{Z}/n\mathbb{Z}$ modules, we can form the SES (by the 2nd isomorphism theorem)
$$0 \to \mathbb{Z}/m\mathbb{Z} \xrightarrow{\psi} \mathbb{Z}/n\mathbb{Z} \xrightarrow{\varphi} \mathbb{Z}/(n/m)\mathbb{Z} \to 0$$
where $m|n$, $\psi(1) = \frac{n}{m}$, and $\varphi(1) = \bar{1}$.
- More generally, given any ideal $I \subseteq R$, we can form the SES
$$0 \to I \to R \to R/I \to 0$$
- By the 1st isomorphism theorem, given any R-module homomorphism $M \xrightarrow{\psi} N$, we have a SES
$$0 \to \ker(\psi) \to M \to \mathrm{im}(\psi) \to 0$$

Finally, we give the definition of a split exact sequence:

Definition 10.5. A SES $0 \to M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \to 0$ is said to be **split exact** if one of the following equivalent conditions is met:

1) $M \cong M' \oplus M''$.
2) There is a homomorphism $\varphi' : M \to M'$ such that $\varphi' \circ \varphi = Id_{M'}$.
3) There is a homomorphism $\psi' : M'' \to M$ such that $\psi \circ \psi' = Id_{M''}$.

Proof. 1) $\Rightarrow$ 2) or 3): Given $M \cong M' \oplus M''$, we get a natural projection and inclusion map
$$\varphi' : M \to M' : m = (m', m'') \mapsto m'$$
$$\psi' : M'' \to M : m'' \mapsto (0, m'')$$
These are clearly the desired maps.

2) $\Rightarrow$ 1): We can construct the map $\Phi : M \to M' \oplus M''$ explicitly:
$$\Phi : M \to M' \oplus M'' : m \to (\varphi'(m), \psi(m))$$
It suffices to check that this is injective and surjective.

Injectivity: Suppose $\Phi(m) = 0$. Then $\psi(m) = 0$ and $\varphi'(m) = 0$. But exactness implies $m \in \ker(\psi) = \mathrm{im}(\varphi)$. As a result, $m = \varphi(m')$ for some $m' \in M'$. As a result, we conclude
$$0 = \varphi'(m) = \varphi'(\varphi(m')) = m'$$
So $m' = 0$, and therefore $m = \varphi(0) = 0$.

Surjectivity: Let $m' \in M'$ and $m'' \in M''$. Since ψ is surjective, there exists $m \in M$ such that $\psi(m) = m''$. Furthermore, we can consider $\varphi(m') \in M$. Note that
$$\varphi'(m + \varphi(m')) = \varphi'(m) + m'$$
So we need an adjustment factor: Consider $m_0 = \varphi(m') + m - \varphi(\varphi'(m))$. Then
$$\psi(m_0) = \psi(m) + (\psi \circ \varphi)(m' - \varphi'(m)) = \psi(m) = m''$$
$$\varphi'(m_0) = \varphi'(\varphi(m')) + \varphi'(m) - \varphi'(\varphi(\varphi'(m))) = m' + \varphi'(m) - \varphi'(m) = m'$$
This completes the proof as 3) $\Rightarrow$ 1) is similar. $\square$

CLASS 11, MARCH 1ST: NOETHERIAN RINGS

We already discussed how to generate an ideal by select elements. The notation was

$$\langle A \rangle = \langle f_\alpha \rangle$$

We saw the importance of finite generation in the statement of Nakayama's Lemma. And indeed, it (and some of the corollaries on the homework) are not even true if the module isn't finitely generated.

Example 11.1. Consider the ring $R = \mathbb{F}_p[x, x^{\frac{1}{p}}, x^{\frac{1}{p^2}}, \ldots] = K[x]_{perf}$. This ring has a maximal ideal

$$\mathfrak{m} = \langle x, x^{\frac{1}{p}}, x^{\frac{1}{p^2}}, \ldots \rangle$$

So we can produce a local ring $R_{\mathfrak{m}}$. Note that $\mathfrak{m} = \mathfrak{m}^2$, as $f \in \mathfrak{m}$ has the form

$$f = \sum_{n=1}^{N} c_n x^{\frac{n}{p^e}} = \sum_{n=1}^{N} c_n x^{\frac{np}{p^{e+1}}} = x^{\frac{1}{p^{e+1}}} \sum_{n=1}^{N} c_n x^{\frac{np-1}{p^{e+1}}}$$

and both sides of the product are in $\mathfrak{m} \neq 0$, violating the assertion of Nakayama.

Definition 11.2. A ring R is called **Noetherian** if every ideal is finitely generated.

This is a fantastic property, named after the great mathematician Emmy Noether. We can already see that Example 11.1 is an example of a non-Noetherian ring. Here some equivalent ways to specify it:

Proposition 11.3. *TFAE:*

1) *R is a Noetherian ring.*
2) *Every ascending chain of ideals of R eventually* **stabilizes***: if*

$$I_1 \subseteq I_2 \subseteq \ldots$$

the $\exists n > 0$ such that $I_n = I_{n+1} = I_{n+2} = \ldots$.
3) *Every non-empty collection of Ideals $\{I_\alpha\}_{\alpha \in \Lambda}$ contains a maximal element. That is to say that there exists $\beta \in \Lambda$ such that there are no $\alpha \in \Lambda$ such that $I_\beta \subsetneq I_\alpha$.*

Proof.

- 1) $\Rightarrow$ 2): Suppose $I_1 \subseteq I_2 \subseteq \ldots$ is an ascending chain of ideals. We know by our proof of existence of maximal ideals that $I = \cup_{i=1}^{\infty} I_i$ is an ideal. By 1), $I = \langle f_1, \ldots, f_n \rangle$ is finitely generated. But this implies $f_i \in I_{j_i}$ for some j_i, since I is a union. As a result,
$$I = I_{\max\{j_1, \ldots, j_n\}}$$
i.e. the chain stabilized.
- 2) $\Rightarrow$ 3): 2) states that every ascending chain of ideals has an upper bound; namely where it stabilizes. As a result, Zorn's lemma implies 3) is true.
- 3) $\Rightarrow$ 1): Let I be an ideal of R. Consider the collection
$$\mathcal{S} = \{J \subseteq I \mid J \text{ an ideal, } J \text{ finitely generated}\}.$$
This set is of course non-empty, since it contains the ideal generated by any single element of I. By 3), we see that $\mathcal{S}$ has a maximal element, say $\mathfrak{m}$ (not a maximal ideal). Suppose $f \in I \setminus \mathfrak{m}$. Then $I + \langle f \rangle \in \mathcal{S}$ is a finitely generated ideal since we only

added 1 generator to a finite set. This contradicts maximality of $\mathfrak{m}$, and therefore no such f can exist, i.e. $I = \mathfrak{m}$ is finitely generated.

□

Definition 11.4. Property 2) in Proposition 11.3 is called the **ascending chain property**, or sometimes the **A.C.C**.

The opposite property, called the **descending chain property**, or the **D.C.C**., states that every descending chain of ideals eventually stabilizes:

$$I_1 \supseteq I_2 \supseteq \ldots \supseteq I_n = I_{n+1} = \ldots$$

A ring with this property is called **Artinian**, for Emil Artin.

We will focus on Noetherian rings, as Artinian is a very restrictive condition that can even be shown to imply Noetherian!

Here is a nice property which allows us to generate many Noetherian rings from known ones.

Proposition 11.5. *If R is a Noetherian ring, and $\varphi : R \to S$ is a surjective map, then S is a Noetherian ring. If R is also a domain, and $\mathfrak{p} \in \mathrm{Spec}(R)$, then $R_{\mathfrak{p}}$ is Noetherian.*

Proof. Let $I_1 \subseteq I_2 \subseteq \ldots$ be an ascending chain of ideals of S. Then

$$\varphi(I_1)^{-1} \subseteq \varphi^{-1}(I_2) \subseteq \ldots$$

is an ascending chain of ideals in R. Therefore it stabilizes. But the correspondence of *ideals* of S to that of R is injective, so the same stabilization occurs for the original chain.

The same proof goes through for localizations as well! □

Example 11.6.

1) Every P.I.D., e.g. $K[x]$ or $\mathbb{Z}$, is Noetherian. This follows by the original definition of Noetherian.
2) $K[x_1, x_2, x_3, \ldots]$ is non-Noetherian, since it has the ascending chain
$$\langle x_1 \rangle \subsetneq \langle x_1, x_2 \rangle \subsetneq \langle x_1, x_2, x_3 \rangle \subsetneq \ldots$$
3) The ring $R = K[x, xy, xy^2, xy^3, \ldots]$ of Homework 4, #1 is a non-Noetherian ring.
4) Consider the ring $C(\mathbb{R})$ of continuous functions from $\mathbb{R}$ to itself. This is certainly non-Noetherian. Even if we localize, i.e. consider functions which are equivalent near 0, we get a quotient of this ring by a relation $f \sim g$ if and only if $f = g$ in an open neighborhood of $0 \in \mathbb{R}$. In fact it is a local ring with maximal ideal those functions for which $f(0) = 0$.

   I claim it is still non-Noetherian. Indeed, suppose $f_1, \ldots, f_n$ generate the maximal ideal. Note that $g = \sum_{i=1}^n a_i f_i$ has the property that $g(x) < C \cdot \max\{|f_i(x)|\}$ as $x \to 0$. There are functions vanishing more slowly. I.e. functions like $G(x) = \sqrt{\max\{|f_i(x)|, |x|\}}$. This would imply
$$\frac{G(x)}{\max\{|f_i(x)|, |x|\}} \to \infty$$

Next week we will cover the Hilbert Basis Theorem, which will give a great deal more examples of Noetherian rings.

CLASS 12, MARCH 4TH: NOETHERIAN MODULES

Today, we will talk about a natural generalization of the Noetherian property to modules. This allows us a greater amount of flexibility as well as allows us to get a handle of finite generation for modules.

Definition 12.1. M an R-module is said to be **Noetherian** if for every ascending chain of submodules

$$M_0 \subseteq M_1 \subseteq \cdots \subseteq M$$

eventually stabilizes. That is to say M has the A.C.C. for submodules.

Clearly a ring R is Noetherian if and only if it is a Noetherian R-module. An identical proof to the case of rings yields the following result:

Corollary 12.2. *TFAE:*

1) *M is Noetherian.*
2) *Every submodule of M is finitely generated.*
3) *Every collection of submodules of M has a maximal element.*

Next up, we can get a neat result for modules connected by a short exact sequence.

Proposition 12.3. *If the following sequence is a S.E.S., then M is Noetherian if and only if M' and M'' are Noetherian:*

$$0 \to M' \xrightarrow{i} M \xrightarrow{j} M'' \to 0$$

Proof. $\Rightarrow$: Ascending chains of submodules in M' and M'' correspond directly to ascending chains in M, and therefore stabilize.

$\Leftarrow$: Let $M_0 \subseteq M_1 \subseteq \ldots \subseteq M$ be an ascending chain of submodules of M. Since $M' \subseteq M$, we can consider

$$M_0 \cap M' \subseteq M_1 \cap M' \subseteq \ldots \subseteq M'$$

an ascending chain of submodules of M'. Since M' is assumed Noetherian, this chain stabilizes, say at $M_n \cap M'$. Similarly, since the image of a module is a module, we can also consider

$$j(M_0) \subseteq j(M_1) \subseteq \ldots \subseteq M''$$

which stabilizes, say at $j(M_m)$.

Let $l = \max\{m, n\}$. I claim the original chain stabilizes at M_l. Indeed, suppose $l' > l$ is such that there exists $m \in M_{l'} \setminus M_l$. Since $j(m) \in j(M_l)$, there exists $n \in M_l$ such that $j(n) = j(m)$. Therefore, $n - m \in \ker(j)$, i.e. $i(m') = n - m$. But since $M_l \cap M' = M_{l'} \cap M'$, we see that $m' \in M_l \cap M'$. But since $n \in M_l \cap M'$, this implies $m \in M_l$, contradicting our choice of m. □

This produces many of the desirable properties of Noetherian Modules:

Corollary 12.4.

1) *If M_i are Noetherian modules, then so is $\oplus_{i=1}^n M_i$.*
2) *If R is a Noetherian ring, then M is a Noetherian R-module if and only if it is finitely generated. As a result, if $N \subseteq M$, then N is also Noetherian/finitely generated.*
3) *If R is a Noetherian ring, and $\varphi : R \to S$ is a ring homomorphism such that S is a finitely generated R-module, then S is a Noetherian ring.*

Proof. 1) This follows by induction on n. The case of $n = 1$ is trivial. We also have a natural exact sequence

$$0 \to M_n \to \oplus_{i=1}^{n} M_i \to \oplus_{i=1}^{n-1} M_i \to 0$$

Our inductive hypothesis yields the outer modules to be Noetherian, so the inner is as well by Proposition 12.3.

2) If M is Noetherian, then every submodule is n-generated, including M. On the other hand, if M is finitely generated, we can produce an exact sequence

$$0 \to \ker(\varphi) \longrightarrow R^{\oplus n} \xrightarrow{\varphi} M \to 0$$

By the previous part, R is Noetherian so $R^{\oplus n}$ is Noetherian, so Proposition 12.3 implies M is Noetherian. The second part follows from Corollary 12.2.

3) Note that if $I \subseteq S$ is an ideal, it is also an R-module. This follows since if $\alpha \in I$ and $r \in R$, then $r \cdot \alpha = \varphi(r)\alpha$, and $\varphi(r)$ is simply an element of S. Therefore I is a finitely generated R-module (as every R-submodule of S is necessarily finitely generated), and at worst the same generating set works as an S-module/ideal.

□

So one should think of Noetherian modules as a strengthening of the notion of finitely generated. Of course, the homework due today contains an example of a non-Noetherian ring, namely $R = K[x, xy, xy^2, \ldots]$ which has the property that R is finitely generated, and yet $\mathfrak{m} = \langle x, xy, xy^2, \ldots \rangle$ is not finitely generated. So Noetherian modules are more restrictive than finitely generated modules. Here is another such example:

Example 12.5. Consider our ring $R = \mathbb{F}_p[x]_{perf} = \mathbb{F}_p[x, x^{\frac{1}{p}}, x^{\frac{1}{p^2}}, \ldots]$. One funny thing about this ring is that the natural inclusion map $\mathbb{F}_p[x] \to \mathbb{F}_p[x]_{perf}$ induces a bijection at the level of Spec. On the other hand, every non-zero prime ideal of R_{perf} is not finitely generated. This is because prime ideals are radical, and finitely many $\frac{1}{p^e}$ can also be made smaller.

One final consequence to mention is the following about Homs.

Theorem 12.6. *If R is Noetherian and M and N are finitely generated modules, then $\mathrm{Hom}_R(M, N)$ is also finitely generated.*

Proof. Given $R^n \to M \to 0$ the generating map, we see that any map $M \to N$ yields a map $R^n \to N$ by composition. As a result, $\mathrm{Hom}_R(M, N) \subseteq \mathrm{Hom}_R(R^n, N)$. The latter module can be identified by where it sends each of its coordinates (i.e. $(1, 0, \ldots, 0)$, $(0, 1, 0, \ldots)$, $\ldots$). This realization allows us to conclude that

$$\mathrm{Hom}_R(M, N) \subseteq \mathrm{Hom}_R(R^n, N) \cong \mathrm{Hom}_R(R, N)^n \cong N^n$$

Since N is finitely generated, so is N^n. This implies N^n is Noetherian, so $\mathrm{Hom}_R(M, N)$ is finitely generated. □

CLASS 13, MARCH 6TH: HILBERT BASIS THEOREM

Finally, we come to the standard tool to detect whether a ring is a Noetherian ring; The Hilbert Basis Theorem. It allows us to ensure that many of our common rings of interest are in fact Noetherian. Therefore, we needn't worry about infinitely generated ideals in these cases!

Theorem 13.1 (Hilbert Basis Theorem)**.** *If R is a Noetherian ring, then $R[x]$ is also Noetherian.*

Example 13.2. By induction, we can conclude that $K[x_1, \ldots, x_n]$, $\mathbb{Z}[x_1, \ldots, x_n]$, and any quotient or localization of such a ring is a Noetherian ring, where K is a field. This is most of the rings we have encountered which weren't specifically labeled as non-Noetherian!

It should be noted that the proof indicated here is a much cleaner version of the proof that Hilbert originally demonstrated:

Proof. Suppose $I \subseteq R[x]$ is an ideal. It suffices to check that I is finitely generated. We can define an auxiliary ideal of R as follows:

$$J_n = \{r \in R \mid f(x) = rx^n + a_{n-1}x^{n-1} + \ldots + a_0 \in I\}$$

That is to say J is the set of leading coefficients of elements of I. This is an ideal of R. In addition, this gives a chain of ideals in R:

$$I \cap R = J_0 \subseteq J_1 \subseteq J_2 \subseteq \ldots$$

This is due to the fact that we can multiply $f(x)$ as above by x^{m-n} to get the desired leading coefficient in J_m.

Now, we can use the fact that R is assume to be Noetherian to conclude that $J_N = J_{N+1} = \cdots$ for some $N \in \mathbb{N}$. Additionally, each J_i is finitely generated, say by $r_1^{(i)}, \ldots, r_{m_i}^{(i)}$. Let $f_{j,i}$ for $i = 1, \ldots, n$ and $j = 1, \ldots, m_i$ be an element with leading coefficient $r_j^{(i)}$.

Finally, I claim that the collection $f_{j,i}$ generate I. Assume $f \in I$ has degree M.

Assume $M \geq N$. Then f has leading coefficient in $J_M = J_N$, so we can choose $f_{j,N}$ and $r_j \in R$ such that

$$f - \sum_{j=1}^{m_N} r_j x^{M-N} f_{j,N}$$

has degree smaller than M. But we can do this for ANY $M \geq N$. So we may assume that $M < N$ by continued reduction.

If $M < N$, then we know our leading coefficient is in J_M. But as a result, we can do the same trick, selecting $r_j \in R$ such that

$$f - \sum_{j=1}^{m_M} r_j f_{j,M}$$

has degree smaller than M. Once we reduce to the case of a 0 degree polynomial, we can conclude that the element is in $I \cap R = J_0$, and conclude that it is a finite sum of our generators $f_{j,0}$.

This procedure implies that any f is expressible as a finite sum of the elements $f_{j,i}$ showing $I = \langle f_{j,i} \rangle$. □

Corollary 13.3. *Any finitely generated R-algebra A, with R Noetherian, can be expressed as*

$$A \cong R[x_1, \ldots, x_n]/I$$

Additionally, the corresponding relations are finitely generated! I.e. the free resolution of A as an $R[x_1, \ldots, x_n]$-module is given as

$$\ldots \to R[x_1, \ldots, x_n]^{\oplus m_1} \to R[x_1, \ldots, x_n] \to A \to 0$$

Proof. Note that when we say generated as an R-algebra, we mean we allow multiplication of elements to generate new elements like x_1^2 or $x_1^{m_1} \cdots x_n^{m_n}$.

The only thing to say here is that since $R[x_1, \ldots, x_n]$ is a Noetherian ring by Theorem 13.1, I is a finitely generated ideal. So the kernel of the generation map needs only finitely many generators.[1] □

One can also perform a similar style of proof for power series rings. To finish off our study of the Noetherian property, we prove a result of I.S. Cohen:

Theorem 13.4. *If R is a ring in which every prime ideal is finitely generated, then R is Noetherian.*

This is pretty neat, since it seems like a vast weakening of the condition, but is enough to conclude the desired result.

Proof. Suppose R is not Noetherian. Consider the set

$$\mathcal{S} = \{I \subseteq R \mid I \text{ is not finitely generated}\}$$

Since R is not Noetherian, this set is non-empty. Suppose that

$$I_1 \subseteq I_2 \subseteq \cdots$$

is an ascending chain of ideals in $\mathcal{S}$. Then we already know that $I = \bigcup_{i \geq 1} I_i$ is an ideal, and furthermore it is not finitely generated. If it were, by $r_1, \ldots, r_n$, then we could find i_j such that $r_j \in I_{i_j}$, and conclude that $I_{\max\{i_1, \ldots, i_n\}}$ is a finitely generated ideal equal to I.

Therefore, $I \in \mathcal{S}$ is an upper bound, and therefore $\mathcal{S}$ contains a maximal element $\mathfrak{p}$ by Zorn's Lemma. I claim $\mathfrak{p}$ is a prime ideal.

Suppose $a \cdot b \in \mathfrak{p}$ but $a, b \notin I$. Then it must be true that $\langle a \rangle + \mathfrak{p}$ is a finitely generated ideal, say by a and $f_1, \ldots, f_n \in \mathfrak{p}$. Moreover, if we consider

$$\mathfrak{p} : a = \{r \in R \mid ra \in \mathfrak{p}\}$$

is an ideal which contains b and $\mathfrak{p}$, so must also be finitely generated, say by $g_1, \ldots, g_m$. I claim that this implies

$$\mathfrak{p} = \langle f_1, \ldots, f_n, ag_1, \ldots, ag_n \rangle$$

which would contradict $\mathfrak{p} \in \mathcal{S}$. Indeed, all of these elements are chosen inside $\mathfrak{p}$. Moreover, if $f \in \mathfrak{p} \subseteq \mathfrak{p} + \langle a \rangle$, then we know

$$f = r_1 f_1 + \ldots + r_n f_n + r_0 a$$

But $f_1, \ldots, f_n \in \mathfrak{p}$, so $r_0 a \in \mathfrak{p}$, implying $r_0 \in \mathfrak{p} : a = \langle g_1, \ldots, g_n \rangle$, which proves the claim. □

[1] One should note that this continues to higher parts of the resolution.

CLASS 14, MARCH 8TH: INTEGRAL RING EXTENSIONS

Today we will shift toward a study of containments of rings $R \subseteq S$. As with all of our objects so far, a notion of finiteness is important and useful for actually acquiring results. Our notion of interest in turns out will be exactly the one that defines algebraic extensions.

Definition 14.1. If R is a ring, A is called an **R-algebra** if A is itself a ring and there exists a ring homomorphism $R \to A$.

A is a **finite** R-algebra if it is a finitely generated R-module.

$a \in A$ is said to be **integral over** R if there exists a monic polynomial $p(x) \in R[x]$ such that

$$p(a) = a^n + r_1 a^{n-1} + \ldots + r_{n-1}a + r_n = 0$$

A is said to be **integral** over R if every element is integral.

Note that for an R-algebra A, we can consider the image of R under the homomorphism. Call it R'. Then we are merely considering $R' \subseteq A$, which is an extension of rings.

Example 14.2.

- $\mathbb{Z}[\frac{1}{m}]$ is not integral over $\mathbb{Z}$ for $m > 1$. We can check this easily by noting
$$\frac{1}{m^n} + a_1 \frac{1}{m^{n-1}} + \ldots + a_n = \frac{1 + m(a_1 + \ldots + m^{n-1}a_n)}{m^n}$$
The numerator of this fraction is $\equiv 1 \pmod m$, therefore can not be 0. This procedure generalizes to R any UFD, with algebra $A = R[f]$ where $f \in Frac(R) \setminus R$.
- $K[x^n] \subseteq K[x]$ is an integral extension.
- $\mathbb{Z} \subseteq \mathbb{Z}[\tau]$, where $\tau = \frac{1+\sqrt{5}}{2}$ is the golden ratio. Then τ satisfies $\tau^2 - \tau - 1 = 0$. Therefore τ is an integral element. On the otherhand, if $\tau = \frac{1+\sqrt{3}}{2}$, then τ satisfies $\tau^2 - \tau - \frac{1}{2}$. This makes it non-integral upon further inspection.
- $\mathbb{Q} \subseteq \bar{\mathbb{Q}}$ is an example of an integral extension which is not finite.

Now we will work through a comparison of the integral and finite extensions. This is typically realized through the following proposition:

Proposition 14.3. *If A is an R-algebra, and $a \in A$, then TFAE:*

(a) *a is integral over R.*
(b) *The subring $R'[a]$ is a finite R'-algebra.*
(c) *There exists $B \subseteq A$ an R'-subalgebra containing a such that B is a finite R'-algebra.*

Proof. $(a) \Rightarrow (b)$: Note $R'[a]$ is generated as an R'-module by $1, a, a^2, \ldots$. a being integral ensures that

$$a^n + r_1 a^{n-1} + \ldots + r_n = 0$$

which is to say $a^n \in \langle 1, a, \ldots, a^{n-1} \rangle$. This implies that $a^m \in \langle 1, a, \ldots, a^{n-1} \rangle$ for all $m \geq n$. As a result,,

$$R'[a] = \langle 1, a, \ldots, a^{n-1} \rangle$$

$(b) \Rightarrow (c)$: Let $B = R'[a]$.

$(c) \Rightarrow (a)$: Consider $B \xrightarrow{\cdot a} B$. Note that this is an R-module homomorphism. Since B is assumed finite as an R- (or R'-)module. By the determinant trick, we get a relation of the form

$$(\cdot a)^n + r_1(\cdot a)^{n-1} + \ldots + r_{n-1}(\cdot a) + r_n$$

Applying this function to $1 \in B$, we get the desired relation on a. □

Next up, we see a set of so-called 'tower laws'. These regard how these properties hold up under 2 (or a finite number of) successive extensions.

Proposition 14.4. (a) *If $A \subseteq B \subseteq C$ are extensions of rings, and C over B is a finite extension, and B over A is a finite extension, then C over A is a finite extension.*

(b) *If $A \subseteq B \subseteq C$ are extensions of rings, and C over B is an integral extension, and B over A is an integral extension, then C over A is an integral extension.*

(c) *If A is an R-algebra, and $a_1, \ldots, a_n$ are integral over R, then $R[a_1, \ldots, a_n]$ is a finite R-algebra.*

(d) *The subset $\tilde{R} \subseteq A$ given by*

$$\tilde{R} = \{a \in A \mid a \text{ is integral over } R\}$$

forms a subring of A. If $a \in A$ is integral over $\tilde{R}$, then it is integral over R, thus in $\tilde{R}$.

Proof. (a): Let $B = \langle b_1, \ldots, b_n \rangle$ as an A-module, and $C = \langle c_1, \ldots, c_m \rangle$ as a B-module. Then for $c \in C$,

$$c = \sum_{j=1}^{m} b_j c_j$$

for some $b_j \in B$. As a result, we can conclude that $b_j = \sum_{i=1}^{n} a_{ij} b_i$ for $a_{ij} \in A$. Thus

$$c = \sum_{j=1}^{m} \left(\sum_{i=1}^{n} a_{ij} b_i \right) c_j = \sum_{j=1}^{m} \sum_{i=1}^{n} a_{ij} (b_i c_j)$$

which is to say $b_i c_j$ form a finite generating set for C over A.

(c): This follows by induction using Proposition 14.3 (b).

(b): We can use (c) and (a) to show this. If $c^n + b_1 c^{n-1} + \ldots + b_n = 0$, then we note that this is a relation in $A[b_1, \ldots, b_n]$. As a result, we can conclude by (a) that

$$A[b_1, \ldots, b_n][c] = A[b_1, \ldots, b_n, c]$$

is a finite A algebra by (c). Therefore, c is integral over A by Proposition 14.3 (c), and thus C is integral over A.

(d): The claim that it is a subring follows by consideration of the finite algebra $R[\alpha, \beta]$ for $\alpha, \beta \in A$. Note in contains $\alpha + \beta$ and $\alpha \cdot \beta$. From (b) we acquire the second assertion. □

CLASS 15, MARCH 11TH: INTEGRAL CLOSURES

Recall that last time we proved the following result:

Proposition 15.1. *The subset $\tilde{R} \subseteq A$ given by*

$$\tilde{R} = \{a \in A \mid a \text{ is integral over } R\}$$

forms a subring of A. If $a \in A$ is integral over $\tilde{R}$, then it is integral over R, thus in $\tilde{R}$.

This is an extremely excellent result, as it tells us that $\tilde{\cdot}$ is a **closure-operation**; applying it twice gives back the result of applying it once! Thus we give it a special name:

Definition 15.2. If $R \subseteq A$, then we call $\tilde{R}$ obtained as in Proposition 15.1 the **integral closure** of R in A. If $\tilde{R} = R$, then R is said to be **integrally closed**. If R an integral domain is integrally closed inside of $\mathrm{Frac}(R)$, then R is said to be **normal**.

Example 15.3.

- If $\mathbb{Q} \subseteq K$ is a finite extension of fields, then we can consider the integral closure of $\mathbb{Z}$ inside K. This is how one obtains the *ring of integers* of K, named $\mathcal{O}_K = \tilde{Z}$.
- In line with the previous example, if we consider $K = \mathbb{Q}(\sqrt{n})$, then

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{n}] & n \equiv 2, 3 \,(\mathrm{mod}\, 4) \\ \mathbb{Z}[\frac{\sqrt{n}+1}{2}] & n \equiv 1 \,(\mathrm{mod}\, 4) \end{cases}$$

  For a fairly accessible write up of this result I invite you to check out

  `https://math.stackexchange.com/questions/654202/determining-ring-of-integers-for-mathbbq-sqrt17`.

- Last time we showed that if R is a UFD, then R is integrally closed in its field of fractions. Thus we acquire the result all UDFs are normal!
- If R is an integral domain, another important closure is the *absolute integral closure*, often denoted by R^+. It is precisely the integral closure inside $\overline{\mathrm{Frac}(R)}$.

Example 15.4. $R = K[x, y]/\langle y^2 - x^3 \rangle$: You showed that this is an integral domain on Homework 3. Therefore we can consider its integral closure inside $\mathrm{Frac}(R)$.

First, let's check that $Frac(R) = K(\frac{y}{x})$. Note that

$$x = \frac{x^3}{x^2} = \frac{y^2}{x^2} = \left(\frac{y}{x}\right)^2$$

$$y = \frac{y \cdot x^3}{x^3} = \frac{y^3}{x^3} = \left(\frac{y}{x}\right)^3$$

Set $t = \frac{y}{x}$, and consider the map $\iota : R \hookrightarrow K(t)$ with $\iota(x) = t^2$ and $\iota(y) = t^3$. Note t is integral in R, since it satisfies $t^2 - x = 0$. Additionally, $K[t]$ is itself normal (since it is a PID, thus a UFD). Therefore the **normalization** of R (i.e. the integral closure of R in $Frac(R)$) is $K[t]$. Thinking about this on Spec yields an interesting interpretation of normalizations of 'curves'.

Next, we move toward the Noether Normalization Theorem. This allows us to think of K-algebras as integral extensions of polynomial rings! Let A be a K-algebra throughout.

Definition 15.5. Elements $z_1, \ldots, z_n \in A$ are **algebraically independent** if the surjection

$$K[x_1, \ldots, x_n] \to K[z_1, \ldots, z_n] : x_i \mapsto z_i$$

is an isomorphism.

The kernel being 0 is simply saying there exist no polynomial relations on the z_i; i.e. if $F \in K[x_1, \ldots, x_n]$, then

$$F(z_1, \ldots, z_n) = 0 \quad \Longrightarrow \quad F = 0$$

Theorem 15.6 (Noether Normalization)**.** *If $A \cong K[x_1, \ldots, x_N]/I$ is a finitely generated K-algebra, then there exists $z_1, \ldots, z_n \in A$ algebraically independent over K such that A is a finite $B = K[z_1, \ldots, z_n]$-module.*

Example 15.7. In the case of Example 15.4, we can let $z_1 = x$ (or y). Then we can view

$$R = (K[x])[y]/\langle y^2 - x^3 \rangle$$

But y is integral over $K[x]$ by the relation defining the ideal. Thus $K[x]$ is *a* Noether Normalization of R.

We prove this theorem by a sort of descending induction argument, stating that if there is an algebraic relation on a finite set of generators, then we can cleverly reduce to a smaller collection:

Lemma 15.8. *Given the set up of Theorem 15.6, if $z_1, \ldots, z_n \in A = K[z_1, \ldots, z_n]$ are not algebraically independent, then there exists $z_1^*, \ldots, z_{n-1}^*$ such that z_n is integral over $A^* = K[z_1^*, \ldots, z_{n-1}^*]$. Moreover, $A = A^*[z_n]$.*

I will now prove Theorem 15.6 assuming Lemma 15.8. We will return to the proof of Lemma 15.8 next time.

Proof. (of Theorem 15.6): We proceed by induction on N. If $N = 0$, then there is nothing to do. Suppose the result is true for up to $N - 1$ generated algebras. If there does not exist any polynomial relation on the x_i, i.e. $I = 0$, then we are also done; let $z_i = x_i$ as A is already a polynomial ring. Let F be a non-zero algebraic relation on the generators of A:

$$F(x_1, \ldots, x_N) = 0$$

Lemma 15.8 implies that there exist $x_1^*, \ldots, x_{N-1}^* \in A$ such that $A = A^*[x_N] = K[x_1^*, \ldots, x_{N-1}^*][x_N]$ and x_N is integral over A^*. By the inductive hypothesis, we can conclude the existence of elements $z_1, \ldots, z_n$ such that A^* is a finite extension of $K[z_1, \ldots, z_n]$. But by our tower laws, this further implies that

$$K[z_1, \ldots, z_n] \subseteq A^* \subseteq A$$

are 2 finite extensions, thus so is their composition. This proves the result.

□

CLASS 16, MARCH 13TH: NN & INTEGRAL FIELD EXTENSIONS

Recall that last time we proved Noether Normalization using the following result:

Lemma 1. *Given the set up of Theorem 15.6, if $z_1, \ldots, z_n \in A = K[z_1, \ldots, z_n]$ are not algebraically independent, then there exists $z_1^*, \ldots, z_{n-1}^*$ such that z_n is integral over $A^* = K[z_1^*, \ldots, z_{n-1}^*]$. Moreover, $A = A^*[z_n]$.*

Today, we will prove this statement (in the case that K is an infinite field) and talk about integrality with respect to fields. The statement for non-infinite fields K is more technical and is due to Nagata. It is available in section 4.7 of the book for those interested.

Proof. (of Lemma 1) We will pick elements of the field $\alpha_1, \ldots, \alpha_{n-1} \in K$ such that

$$z_i^* = z_i - \alpha_i z_n$$

play the desired role. Define

$$G(z_1^*, \ldots, z_{n-1}^*, z_n) = F(z_1^* + \alpha_1 z_n, \ldots, z_{n-1}^* + \alpha_{n-1} z_n, z_n) = 0$$

achieved simply by substituting for z_i using our new equation. Let

$$F = \sum_m a_m z^m = \sum_m a_m z_1^{m_1} \cdots z_n^{m_n}$$

Then

$$G = \sum_m a_m (z_1^* + \alpha_1 z_n)^{m_1} \cdots (z_1^* + \alpha_1 z_n)^{m_{n-1}} z_n^{m_n}$$

Let $d = \deg(F)$ be the largest number such that there exists m such that $|m| = m_1 + \ldots + m_n = d$ with $a_m \neq 0$. Then notice that the coefficient in $K[z_1^*, \ldots, z_{n-1}^*]$ of z_n^d of G is given by

$$F_d(\alpha_1, \ldots, \alpha_{n-1}, 1) = \sum_{|m|=d} a_m \alpha_1^{m_1} \cdots \alpha_{n-1}^{m_{n-1}}$$

which is simply an element of K! So it only goes to ensure we can choose α_i such that $F_d(\alpha_1, \ldots, \alpha_{n-1}, 1)$ is a unit, or equivalently non-zero.

This can rephrased as follows; $f \in K[x_1, \ldots, x_n]$ where K is an infinite field is zero if and only if $f(\alpha_1, \ldots, \alpha_n) = 0$ for any choice of $\alpha_i \in K$. When $n = 1$, this is clear (f has only finitely many roots in $\bar{K}$, thus also in K). Assume we have proved this for up to n variables. But

$$f \in K[x_1, \ldots, x_n] \subseteq K(x_1, \ldots, x_{n-1})[x_n]$$

So there are only finitely many roots $x_n = \alpha$ for which $f(x_1, \ldots, x_{n-1}, \alpha) = 0$. Choose β not one of these roots, and notes that

$$0 \neq f(x_1, \ldots, x_{n-1}, \beta) \in K[x_1, \ldots, x_{n-1}]$$

As a result, we can conclude by induction that there exist $\alpha_1, \ldots, \alpha_{n-1} \in K$ such that

$$0 \neq f(\alpha_1, \ldots, \alpha_{n-1}, \beta)$$

as desired. □

We will finish up with one neat consideration for integral extensions:

Proposition 16.1. *Let $A \subseteq B$ be an integral extension of integral domains. Then*

$$A \text{ is a field} \quad \iff \quad B \text{ is a field}$$

Of course, the same is not true if we weaken our assumptions:

Example 16.2. $K \subseteq K[x]/\langle x^n \rangle$ is an integral extension, but $K[x]/\langle x^n \rangle$ is not even a domain! If we try to drop the integral assumption, examples such as $\mathbb{Z} \subseteq \mathbb{Q}$ and $K \subseteq K[x]$ provide natural counterexamples.

Proof. (of Proposition 16.1) $\Rightarrow$: Suppose $x \in B$ and A is a field. Then

$$x^n + a_1 x^{n-1} + \ldots + a_{n-1}x + a_n = 0$$

implies

$$x \cdot (-a_n^{-1})(x^n + a_1 x^{n-1} + \ldots + a_{n-1}) = 1$$

So x is a unit. Note here we can assume $a_n \neq 0$, as otherwise we could simply factor out by a large enough power of x, which is non-zero since $x \in B$ can be assumed not in A.

$\Leftarrow$: Suppose $x \in A$ and B is a field. Then $x^{-1} \in B$ and

$$x^{-n} + a_1 x^{-(n-1)} + \ldots + a_{n-1}x^{-1} + a_n = 0$$

implies (by multiplying by x^{n-1})

$$x^{-1} = -(a_1 + a_2 x + \ldots + a_n x^{n-1})$$

So $x^{-1} \in A$. □

Corollary 16.3 (Weak Nullstellensatz)**.** *If K/k is a field extension, and K is a finitely generated k-algebra, then K/k is algebraic/integral, and thus is a finite field extension.*

Proof. By Noether Normalization, there exist $z_1, \ldots, z_n$ algebraically independent elements such that $k[z_1, \ldots, z_n] \subseteq K$ is a finite extension of rings. By Proposition 16.1, we know that $k[z_1, \ldots, z_n]$ is a field. This is only possible if $n = 0$ by algebraic independence. And thus K/k is finite. □

Remember, the exam is on Friday!

CLASS 17, APRIL 1ST: GENERAL LOCALIZATION

So far we have only been able to localize integral domains at their prime ideals (or even multiplicative sets). This was ensured by viewing these objects within their fraction field and allowing only denominators in the multiplicative set. This has several advantages, such as the map from a ring to its localization being injective. The general case is not so much more intense to construct when viewed formally, and allows us to also localize modules as well!

Definition 17.1. Let R be a ring and $W \subseteq R$ be a multiplicative set (recall we require $1 \in W$ and $0 \notin W$). Then the **localization of R at W** is the ring

$$W^{-1}R := W \times R/\sim$$

where $(w, r) \sim (w', r')$ if and only if there exists $s \in W$ such that $s(rw' - wr') = 0$ in R. Furthermore, the operations are defined as

$$(w, r) + (w', r') = (ww', rw' + r'w)$$

$$(w, r) \cdot (w', r') = (ww', rr')$$

Lastly, there is also a **localization map**:

$$R \to W^{-1}R : r \mapsto (1, r)$$

Notation is often abused, and we simply write $\frac{r}{s}$ instead of (s, r). It should be noted that often times the elements of the localization do NOT behave like fractions, except perhaps spiritually.

Lemma 17.2. *This new notion of localization is isomorphic to our old notion of localization for integral domains.*

I leave it to you to check this feature of the new method (forever more, simply called localization).

Example 17.3 (Zero Divisors)**.** Suppose $z \in W$ is a zero divisor for R. Note that $(1, 0) \sim (w, 0)$ for any $w \in W$. Therefore, whenever $r \cdot z = 0$, we have that $(1, r) \sim 0$, since $z(r - 0) = 0$. Therefore, any r multiplying with z to 0 **becomes** 0 in $W^{-1}R$. Rephrasing this, if we call $l : R \to W^{-1}R$ the localization map, then

$$\ker(l) = \{r \in R \mid \exists w \in W \text{ such that } rw = 0\}$$

Example 17.4 (Specific Example)**.** Consider the ring $R = K[x, y, z]/\langle xy, xz\rangle$. If we localize at the multiplicative set $W = \{1, x, x^2, \ldots\}$, we see that $(1, y) = (1, z) = 0$ in the localized ring. So $W^{-1}R = K[x, x^{-1}]$.

If we chose instead the multiplicative set $W = \{1, y, z, y^2, yz, z^2, \ldots\}$, then we would get that $x = 0$ in the localization. Therefore

$$W^{-1}R = K[y, y^{-1}, z, z^{-1}]$$

Example 17.5. If we weakened our assumption to allow for multiplicative sets that contain 0, we would simply eliminate every element of the ring: $(0,0) \sim (r,r')$ for any choice of r, r'. As a result, we get

$$W^{-1}R = 0 \iff 0 \in W \iff W \cap nil(R) \neq \emptyset$$

Therefore, since such a case is so boring, I opt to ignore it when declaring a multiplicative set. Some authors don't enforce such a requirement.

We can furthermore upgrade one of our previous homework results without any change to localization:

Proposition 17.6. *If R is a ring and W is a multiplicative set, then*

$$\operatorname{Spec}(W^{-1}R) = \{\mathfrak{p} \in \operatorname{Spec}(R) \mid \mathfrak{p} \cap W = \emptyset\}$$

I leave it to you to check this result, but note the following example:

Example 17.7. Let's examine what the prime ideals of $W^{-1}\mathbb{Z}$ are where $W = \{1, \underline{2}, \underline{3}, 4, \underline{5}, 6, 8, 9, 10, \ldots\}$. By Proposition 17.6, we have that they are in bijection with the primes primes of $\mathbb{Z}$ not intersecting W. So those prime ideals are exactly those generated by prime numbers not 2, 3, or 5. So they are $0, \langle 7\rangle, \langle 11\rangle, \langle 13\rangle, \ldots$. In fact, it is easy to check that $W^{-1}\mathbb{Z} \cong \mathbb{Z}[\frac{1}{2}, \frac{1}{3}, \frac{1}{5}]$.

Two of the most common examples of multiplicative sets are prime ideals $\mathfrak{p}$ and sets focused around an element $f \in R$: $\{1, f, f^2, \ldots\}$. As a result, we give these two localizations special names: $R_{\mathfrak{p}}$ and R_f respectively. Geometrically, this should be thought of as focusing locally around the point $\mathfrak{p} \in \operatorname{Spec}(R)$ and focusing away from primes containing f respectively. In fact, we can formally present R_f:

Proposition 17.8. $R_f \cong R[x]/\langle xf - 1\rangle$.

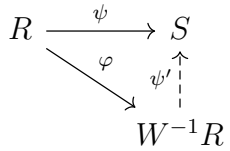
Proof. There is a natural surjective map $\psi : R[x] \to R_f$, where $\psi(r) = (1, r)$ and $\psi(x) = (f, 1)$. It only goes to show (by the isomorphism theorems) that $\ker(\psi) = \langle xf - 1\rangle$. Suppose $h(x) \in \ker(\psi)$. That is to say $h(\frac{1}{f}) = 0$ in R_f. Since h has some finite degree, there exists n such that $f^n h(\frac{1}{f}) \in R$. As a result, $f^n h(x) = g(fx) \in R[x]$ satisfies $g(1) = 0$. By the division algorithm, $g = (y-1)g_1(y)$. But as a result,

$$f^n h(x) = g(fx) = (fx - 1)g_1(fx)$$

Finally, noting that $fx - 1$ and f are coprime, we conclude that $h(x) \in \langle xf - 1\rangle$. This is the desired result. □

Finally, I note a universal property of localization.

Theorem 17.9. *If W is a multiplicative set, and $\psi : R \to S$ is a ring homomorphism for which $\psi(w)$ is a unit for every $w \in W$, then ψ factors through the localization map. That is the following diagram commutes: $\psi = \psi' \circ \varphi$*



Proof. See homework. □

CLASS 18, APRIL 3RD: GOING UP!

Today we will study how primes behave in integral extensions. We have already seen a case of this subtly introduced before the break:

Proposition 1. *Let $A \subseteq B$ be an integral extension of integral domains. Then*

$$A \text{ is a field} \quad \iff \quad B \text{ is a field}$$

In particular, it is stating that if 0 is the only prime of B, then 0 is also the only prime of A! This goes far deeper.

Theorem 18.1 (Going Up Theorem)**.** *If $A \subseteq B$ is an integral extension of rings, and $\mathfrak{p} \in \mathrm{Spec}(A)$ is a prime ideal of A, then there exists a prime ideal $\mathfrak{q} \in \mathrm{Spec}(B)$ such that $\mathfrak{q} \cap A = \mathfrak{p}$. Furthermore, $\mathfrak{q}$ can be chosen to contain any prime ideal $\mathfrak{q}' \in \mathrm{Spec}(B)$ such that $\mathfrak{q}' \cap A \subseteq \mathfrak{p}$.*

Sometimes the first sentence of this result is known as the **Lying Over Theorem**, and the latter sentence is called **Going Up**. This will be explained in slightly more detail later in the corollaries.

Proof. Given $\mathfrak{q}' \in \mathrm{Spec}(B)$ such that $\mathfrak{q}' \cap A \subseteq \mathfrak{p}$, we can consider instead the integral extension

$$A/\mathfrak{q}' \cap A \subseteq B/\mathfrak{q}'$$

Therefore, without loss of generality we may assume $\mathfrak{q}' = 0$. Relabel A and B as these rings. Let $W = A \setminus \mathfrak{p}$. Then we can consider the localization

$$A_{\mathfrak{p}} = W^{-1}A \subseteq W^{-1}B$$

This allows us to assume A is a local ring with maximal ideal $\mathfrak{p}$. Again replace A and B with $A_{\mathfrak{p}}$ and $W^{-1}B$ respectively.

Given a maximal ideal $\mathfrak{m}$ of B that contains $\mathfrak{p} \cdot B$, it necessarily has the property that $\mathfrak{p} = \mathfrak{m} \cap A$. Therefore, it only suffices to check that $\mathfrak{p} \cdot B \neq B$. If it were equal, then 1 can be written as an B-linear combination of elements of $\mathfrak{p}$:

$$1 = b_1 p_1 + \cdots + b_n p_n \qquad\qquad b_i \in B,\ p_i \in \mathfrak{p}$$

Let $B' = A[b_1, \ldots, b_n] \subseteq B$. Then $1 \in \mathfrak{p} \cdot B'$ by the previous equality. But B' is a finitely generated A module! So by Nakayama's Lemma, we have that since $B' = \mathfrak{p}B'$, that $B' = 0$. This is impossible since B' contains A which we assumed had a maximal ideal (i.e. is non-zero). □

Corollary 18.2. *If $\iota : A \hookrightarrow B$ is an inclusion which is an integral extension of rings, then the map on* Spec *is a surjection:*

$$\iota^{\#} : \mathrm{Spec}(B) \to \mathrm{Spec}(A) : \mathfrak{q} \mapsto \mathfrak{q} \cap A$$

This is simply put the *lying over* part of Theorem 18.1. We can also do an induction argument to produce a nice statement about ascending chains of ideals:

Corollary 18.3. *Let $A \subseteq B$ be an integral extension of rings. If $\mathfrak{p}_0 \subseteq \mathfrak{p}_1 \subseteq \ldots \subseteq \mathfrak{p}_n$ is an ascending chain of prime ideals in* $\mathrm{Spec}(A)$*, then there exists a corresponding chain of ideals $\mathfrak{q}_0 \subseteq \mathfrak{q}_1 \subseteq \ldots \subseteq \mathfrak{q}_n$ in* $\mathrm{Spec}(B)$ *such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i$.*

This result is very important regarding an invariant called dimension of a ring. Reinterpreted, this corollary states that dimension can't drop in an integral extension of rings. There is a more complicated theorem as well called the **Going Down Theorem**. This is currently beyond our scope, but I encourage the aspiring commutative algebraist to at least know the statement.

Example 18.4. Consider the integral extension of rings discussed previously: $\mathbb{Z} \subseteq \mathbb{Z}[\tau]$, where $\tau = \frac{1+\sqrt{5}}{2}$ is the so-called golden ratio[1]. What the going up theorem tells us is that every prime ideal $\mathfrak{p} = \langle p \rangle$ of $\mathbb{Z}$ has a corresponding prime ideal in $\mathbb{Z}[\tau]$ intersecting back to $\mathfrak{p}$.

Note that τ is actually a unit:

$$\tau \cdot (\tau - 1) = (\frac{\sqrt{5}+1}{2}) \cdot (\frac{\sqrt{5}-1}{2}) = 1$$

If we consider the prime ideal $\langle 5 \rangle$ of $\mathbb{Z}$, we notice that its extension to $\mathbb{Z}[\tau] \cong \mathbb{Z}[x]/\langle x^2 - x - 1 \rangle$ is NOT prime. This is because $\mathbb{Z}[x]/\langle 5, x^2 - x - 1 \rangle$ is not a domain, i.e. $x^2 - x - 1$ factors in $\mathbb{Z}/5\mathbb{Z}[x]$:

$$(x+2)^2 = x^2 + 4x + 4 \equiv x^2 - x - 1 \,(\mathrm{mod}\, 5)$$

As a result, the prime lying over $\langle 5 \rangle$ in $\mathbb{Z}[\tau]$ is $\langle \tau + 2 \rangle$.

As a final consideration, we can also say a bit more about the primes which lie over a given prime in integral extensions.

Proposition 18.5 (Incomparability)**.** *Suppose $A \subseteq B$ is an integral extension of rings. If $\mathfrak{q}, \mathfrak{q}'$ are 2 prime ideals of B such that $\mathfrak{q} \cap A = \mathfrak{q}' \cap A$, then either $\mathfrak{q} = \mathfrak{q}'$ or $\mathfrak{q} \not\subseteq \mathfrak{q}' \not\subseteq \mathfrak{q}$.*

Proof. Suppose that $\mathfrak{q} \subseteq \mathfrak{q}'$ are prime ideals such that $\mathfrak{p} := \mathfrak{q} \cap A = \mathfrak{q}' \cap A$. We can again consider

$$A/\mathfrak{p} \subseteq B/\mathfrak{q}$$

This is an integral extension of integral domains. Localizing at the multiplicative set $W = R \setminus \mathfrak{p}$, we get an integral extension

$$W^{-1}(A/\mathfrak{p}) = \mathrm{Frac}(A/\mathfrak{p}) \subseteq W^{-1}B/\mathfrak{q}$$

But by Proposition 1, we have that $W^{-1}B/\mathfrak{q}$ is a field. That is to say that $\mathfrak{q}' \cdot W^{-1}B/\mathfrak{q}$ is either 0 or $W^{-1}B/\mathfrak{q}$. In the latter case, we are saying

$$1 = \frac{q'}{a} \qquad\qquad q' \in \mathfrak{q}', a \in W$$

Or equivalently (since $B/\mathfrak{q}$ was a domain), $q' = a$. But $\mathfrak{q}' \notin W$, so this is impossible. □

This result actually shows dimension of rings in an integral extension is *equal*.

[1]Recall that it satisfies the relation $\tau^2 - \tau - 1 = 0$

CLASS 19, APRIL 5TH: LOCALIZING MODULES

Today we will naturally extend the notion of localization at a multiplicative set to its modules. This has several advantages, reducing aspects of our study to modules over local rings. Begin by recalling the result of Homework 3, #2:

Proposition 1. $\mathrm{Spec}(W^{-1}R) \longleftrightarrow \{\mathfrak{p} \in \mathrm{Spec}(R) \mid \mathfrak{p} \cap W = \emptyset\}$

We can immediately extend this to modules.

Proposition 19.1. *Let Mod_R be the collection of R-modules for a ring R. Then*

$$Mod_{W^{-1}R} = \{M \in Mod_R \mid M \xrightarrow{\cdot w} M \text{ is bijective } \forall w \in W\}$$

Proof. If M is a $W^{-1}R$-module, then it gets the structure of an R-module via the localization map $R \to W^{-1}R : r \mapsto (1, r)$. Also, clearly $\cdot w$ is bijective with inverse $\cdot(w, 1)$. This yields $\subseteq$.

For the reverse, we can give M a $W^{-1}R$-module structure by multiplication $(w, r) \cdot m = r \cdot m'$, where m' is the unique element in the preimage of m under $\cdot w$. □

If M is any R-module, then we can still produce a $W^{-1}R$-module via localization. It is defined analogously to the procedure for rings:

Definition 19.2. The **localization of M at W** is the $W^{-1}R$-module given as

$$W^{-1}M = W \times M/\sim$$

where $(w, m) \sim (w', m')$ if and only if there exists $s \in W$ such that $s(wm' - w'm) = 0$ in M. The multiplicative and additive structure are identical to the case of rings.

I leave it to you to check that this yields a well defined $W^{-1}R$-module, though it is identical to the case of rings. As usual, in the special cases of $W = R \setminus \mathfrak{p}$ and $W = \{1, f, f^2, \ldots\}$, it is common to write $M_{\mathfrak{p}}$ and M_f. We can also localize homomorphisms:

Definition 19.3. If $f : M \to N$ is an R-module homomorphism, its **localization** is the $W^{-1}R$-module map

$$W^{-1}f : W^{-1}M \to W^{-1}N : (w, m) \mapsto (w, f(m))$$

Again, it is natural to check that this is well defined, but simple to do so. This gives us a way to relate localization of modules and exact sequences in a natural way:

Proposition 19.4. *If $M' \xrightarrow{\alpha} M \xrightarrow{\beta} M''$ is an exact sequence of R-modules, then $W^{-1}M' \xrightarrow{W^{-1}\alpha} W^{-1}M \xrightarrow{W^{-1}\beta} W^{-1}M''$is an exact sequence of $W^{-1}R$-modules.*

Proof. For the $\ker(W^{-1}\beta) \supseteq \mathrm{im}(W^{-1}\alpha)$ direction, note

$$W^{-1}\beta(W^{-1}\alpha(w, m')) = (w, \beta(\alpha(m')) = (w, 0) = 0$$

Now suppose $(w, m) \in \ker(W^{-1}\beta)$. This is to say there exists $s \in W$ such that $0 = s\beta(m) = \beta(sm)$ in M''. Thus $sm \in \ker(\beta) = \mathrm{im}(\alpha)$. Take $m' \in M'$ mapping to sm (by exactness of the original sequence). Then if we consider $(sw, m') \in W^{-1}M'$, we have

$$W^{-1}\alpha(sw, m') = (sw, \alpha(m')) = (sw, sm') = (w, m')$$

This demonstrates the $\subseteq$ direction and proves the claim. □

This result is often stated as **localization is an exact functor** and is central to many corollaries regarding localization.

Corollary 19.5. (a) *$W^{-1}(M/N) \cong W^{-1}M/W^{-1}N$ as $W^{-1}R$-modules. In particular, $W^{-1}(R/I) \cong W^{-1}R/W^{-1}I$ as rings!*

(b) *If $M, M' \subseteq N$, then $W^{-1}(M \cap M') = W^{-1}M \cap W^{-1}M'$.*

(c) *Given a module homomorphism $f : M \to N$, then $\ker(W^{-1}f) = W^{-1}\ker(f)$ and $\operatorname{coker}(W^{-1}f) = W^{-1}\operatorname{coker}(f)$. In particular, surjectivity and injectivity are preserved under localization.*

Proof. Most of these results are acquired by applying Proposition 19.4 appropriately:

(a) Localize the sequence $0 \to N \to M \to M/N \to 0$.

(b) The exact sequence of interest is

$$0 \to M \cap M' \to M \to N/M'$$

which yields the localized sequence

$$0 \to W^{-1}(M \cap M') \to W^{-1}(M) \to W^{-1}(N/M') \cong W^{-1}N/W^{-1}M'$$

We can replace $W^{-1}(M \cap M')$ by $W^{-1}M \cap W^{-1}M'$ without changing exactness, so they are isomorphic and thus equal.

(c) Localize the sequences $0 \to \ker(\varphi) \to M \to N$ and $M \to N \to \operatorname{coker}(\varphi) \to 0$.

□

Finally, a neat result which shows that if a module is *locally* zero, then it in fact is zero. One might even say that being 0 is a **local property**.

Proposition 19.6. *If $f : M \to N$ is a map of R-modules such that $f_{\mathfrak{m}}$ is the zero map for every maximal ideal $\mathfrak{m}$, then f was 0 to begin with. In particular, if $M_{\mathfrak{m}} = 0$ for every maximal ideal, then $M = 0$.*

Proof. The first result follows from the second when combined with part (c) of Corollary 19.5. Suppose $m \neq 0$ in M. Then since $1 \cdot m = m \neq 0$, we have that $\operatorname{Ann}_R(m)$ is a proper ideal of R. Let $\mathfrak{m}$ be a maximal ideal containing it. Then $(1, m) \neq 0$ in $M_{\mathfrak{m}}$, since there exists no $s \notin \operatorname{Ann}_R(m) \subseteq \mathfrak{m}$ such that $sm = 0$. □

Corollary 19.7 (Non-local Nakayama II)**.** *If I is an ideal such that*

$$I \subseteq Jac(R) = \bigcap_{\mathfrak{m}\ maximal} \mathfrak{m}$$

and M is a finitely generated module with $M = IM$, then $M = 0$.

$Jac(R)$ is called the **Jacobson Radical** of R.

Proof. Since $I \subseteq \mathfrak{m}$ for each $\mathfrak{m}$, $I_{\mathfrak{m}}$ is a proper ideal of $R_{\mathfrak{m}}$ contained within $\mathfrak{m}R_{\mathfrak{m}}$. Then

$$M_{\mathfrak{m}} \supseteq \mathfrak{m}M_{\mathfrak{m}} \supseteq IM_{\mathfrak{m}} \supseteq M_{\mathfrak{m}}$$

Thus everything is equal. By NL2, we see $M_{\mathfrak{m}} = 0$ for each maximal ideal $\mathfrak{m}$, so Proposition 19.6 yields the desired result. □

CLASS 20, APRIL 8TH: Spec & ALGEBRAIC VARIETIES

We will now transition to a bit of geometric reasoning. Recall that we left off with the following result before break:

Corollary 1 (Weak Nullstellensatz)**.** *If K/k is a field extension, and K is a finitely generated k-algebra, then K/k is algebraic/integral, and thus is a finite field extension.*

We can view this as a statement about polynomial rings as follows: if $\mathfrak{m} \subsetneq K[x_1, \ldots, x_n]$ is a maximal ideal, then $L = K[x_1, \ldots, x_n]/\mathfrak{m}$ is a field extension of K. By the Weak Nullstellensatz, we can conclude that L is in fact a finite field extension. This gives us the following beautiful corollary (which simultaneously handles all of the cases we painstakingly dealt with previously).

Theorem 20.1. *If K is an algebraically closed field, then every maximal ideal of $R = K[x_1, \ldots, x_n]$ has the form*

$$\mathfrak{m} = \langle x_1 - \alpha_1, \ldots, x_n - \alpha_n \rangle$$

where $\alpha_i \in K$. Thus there is a natural bijection of m-Spec(R) with K^n.

Proof. First note that all of the ideals of that form are clearly maximal. Their quotient is K.

Notice that the generators of $L = K[x_1, \ldots, x_n]/\mathfrak{m}$ as a K-algebra are the residue classes $\bar{x_1}, \ldots, \bar{x_n}$. By the analysis above, we can conclude that L/K is a finite/algebraic extension. But we assume K is algebraically closed! I.e. there exist no non-trivial algebraic extensions of K. That is to say $L = K$. As a result, we note that $\bar{x_i} \in K$. I.e. $\bar{x_i} - \alpha_i = 0$ for some $\alpha_i \in K$ □

A nice corollary of this fact coming from one of the exam questions is as follows:

Corollary 20.2. *Given a polynomial $K[x_1, \ldots, x_n]$, we can view*

$$K[x_1, \ldots, x_n] \subseteq \bar{K}[x_1, \ldots, x_n]$$

This is an integral extension, so every maximal ideal has the form

$$\mathfrak{m} = \langle x_1 - \alpha_1, \ldots, x_n - \alpha_n \rangle \cap K[x_1, \ldots, x_n]$$

where $\alpha_i \in \bar{K}$.

This brings about the following nice geometric realization of ideals.

Definition 20.3. A **K-variety** is a set $V \subseteq K^n$ such that

$$V = V(I) = \{(a_1, \ldots, a_n) \in K^n \mid f(a_1, \ldots, a_n) = 0 \ \ \forall f \in I\}$$

where I is an ideal of $K[x_1, \ldots, x_n]$.

Example 20.4. Consider the ideal $J = \langle x^2 + y^2 + z^2 - 1 \rangle \subseteq \mathbb{R}[x, y, z]$. The resulting variety $V(J)$ is the sphere S^2. If we considered instead $J = \langle x^2 + y^2 - z^2 \rangle \subseteq \mathbb{R}[x, y, z]$, then $V(J')$ is the cone!

Since $K[x_1, \ldots, x_n]$ is a Noetherian ring, we get that I is a finitely generate ideal:

$$I = \langle f_1, \ldots, f_m \rangle$$

Therefore, $V(I)$ is the set of points for which $f_1(a) = \ldots = f_m(a) = 0$.

Proposition 20.5. *If K is algebraically closed, and $A = K[x_1, \ldots, x_n]/I$ is a finitely generated K-algebra. Then every maximal ideal has the form $\mathfrak{m} = \langle x_1 - \alpha_1, \ldots, x_n - \alpha_n \rangle$, where $(\alpha_1, \ldots, \alpha_n) \in V(I)$. Thus there is a natural bijection between $V(I)$ and m-Spec(A).*

Proof. This is a culmination of several results from the homeworks:

- The preimage of a prime ideal is a prime.
- The preimage of a maximal ideal under a surjection is maximal.
- $\text{Spec}(A) = \{\mathfrak{p} \in \text{Spec}(K[x_1, \ldots, x_n] \mid I \subseteq \mathfrak{p}\}$

□

The final piece of data to speak about today is the ideal/variety correspondence. This gives a map which provides something like an inverse for the map V described above. We will discuss how close it is to an inverse next time.

Definition 20.6. Given *any* subset $X \subseteq K^n$, we can define

$$I(X) = \{f \in K[x_1, \ldots, x_n] \mid f(x) = 0 \ \ \forall x \in X\}$$

This is an ideal of $K[x_1, \ldots, x_n]$ (it is an easy check).

Proposition 20.7. *Both V and I are inclusion reversing maps: If $J' \subseteq J$, then $V(J') \supseteq V(J)$ and if $Y \subseteq X$, then $I(Y) \supseteq I(X)$.*

$$\{X \subseteq K^n\} \underset{I}{\overset{V}{\rightleftarrows}} \{I \subseteq K[x_1, \ldots, x_n] \text{ an ideal.}\}$$

Proof. For the first statement, if every polynomial $f \in J$ vanishes at some point x, then so does every $f \in J'$! Thus $V(J') \supseteq V(J)$. Similarly, for the second statement, the polynomials which vanish for all $x \in X$ necessarily vanish for all $y \in Y \subseteq X$. □

As an immediate corollary of this fact, we have the following:

Corollary 20.8. *$X \subseteq V(I(X))$ with equality if and only if X is a variety, i.e. $X = V(I)$. Similarly, $J \subseteq I(V(J))$ for any ideal J.*

Proof. $X \subseteq V(I(X))$ is demonstrating by the following; $I(X)$ is the set of all polynomials which vanish on all of X. These functions may vanish elsewhere, but certainly vanish on X! The equality statement follows by definition: $X = V(J)$ is precisely the set of points for which every $f \in J$ vanishes on. Rephrased:

$$V(J) = V(I(V(J)))$$

The other statement also follows via similar analysis; $I(V(J))$ is the set of functions which vanish at all points for which every $f \in J$ vanishes. More functions may exist! □

CLASS 21, APRIL 10TH: HILBERT-NULLSTELLENSATZ THEOREM

Recall last time we ended with this result:

Corollary 1. *$X \subseteq V(I(X))$ with equality if and only if X is a variety, i.e. $X = V(I)$. Similarly, $J \subseteq I(V(J))$ for any ideal J.*

The if and only if part of this corollary is actually the inspiration to define a variety this way; it is precisely the the collection of subsets X for which $X = V(I(X))$. Note the following example demonstrates that it is not always the case:

Example 21.1. Consider $\langle x^n \rangle \subseteq \langle x \rangle \subseteq K[x]$. By Proposition 20.7, we have that $V(x^n) \supseteq V(x)$. On the other hand, both sets are just the point $0 \in K$! Thus $V(x^n) = V(x)$.

Similarly, if we take $X = \mathbb{Z} \subseteq \mathbb{C}$, then the set of functions in $\mathbb{C}[x]$ which vanish at $\mathbb{Z}$ are precisely the zero function. Thus $I(\mathbb{Z}) = 0$. But $V(I(\mathbb{Z})) = \mathbb{C} \neq \mathbb{Z}$! So of course $\mathbb{Z} \subseteq \mathbb{C}$ is not an algebraic variety.

This brings up the following question: what are the set of ideals for which $I(V(J)) = J$? This was resolved by Hilbert:

Theorem 21.2 (Hilbert-Nullstellensatz)**.** *Assume K is an algebraically closed field. If $J \subsetneq K[x_1, \ldots, x_n]$ is an ideal, then $V(J) \neq \emptyset$. Furthermore, $I(V(J)) = \sqrt{J}$.*

Recall the statement that

$$\sqrt{J} = \bigcap_{J \subseteq \mathfrak{p} \text{ prime}} \mathfrak{p}$$

The Nullstellensatz gives an even stronger result: we can take the intersection to be only over maximal ideals containing J!

$$\sqrt{J} = \bigcap_{J \subseteq \mathfrak{m} \text{ maximal}} \mathfrak{m}$$

To see this, note that $V(J)$ is in bijection with the set of maximal ideals containing J, via $a = (a_1, \ldots, a_n) \longleftrightarrow \langle x_1 - a_1, \ldots, x_n - a_n \rangle = \mathfrak{m}_a$. Note $\mathfrak{m}_a$ is precisely the set of functions vanishing at a. Applying I asks what polynomials vanish at each of these points? Well that is exactly the intersection of the polynomials vanishing at each point!

This also extends to non-algebraically closed fields K by Corollary 20.2 from last time, and to quotients of such rings by the ideal correspondence.

Of course, it should be noted that this can not be pushed to arbitrary rings (in general rings with this property are called **Jacobson Rings**). Considerations for a local ring provide counterexamples to this statement more broadly:

Example 21.3. If $R = K[x, y]_{\langle x,y \rangle}$, then the ideal $\langle x^2 + y^2 - 1 \rangle$ is prime (unless $char(K) = 2$). However, it is not equal to the intersection of maximal ideals, since there is only 1: $\langle x, y \rangle$.

Proof. (of Theorem 21.2) For the first statement, notice that $J \subseteq \mathfrak{m}$ for some maximal ideal. Thus

$$V(J) \supseteq V(\mathfrak{m}) = V(\langle x_1 - a_1, \ldots, x_n - a_n \rangle) = (a_1, \ldots, a_n)$$

The second statement is far more interesting. It is easy to see that $I(V(J)) \supseteq \sqrt{J}$, since $f(a_1, \ldots, a_n) = 0$ if and only if $f^n(a_1, \ldots, a_n) = 0$. Suppose $f \in I(V(J))$. That is to say the $f(P) = 0$ for every $P \in V(J)$.

Fix such an $f \in I(V(J))$ and construct an auxiliary polynomial ring $S' = K[x_1, \ldots, x_n, y]$ and consider the ideal $J' = J \cdot S' + \langle fy - 1 \rangle$. If we consider $V(J')$, it necessarily is empty! This is because if $(a_1, \ldots, a_n, b) \in V(J')$, then we have $g(a_1, \ldots, a_n) = 0$ for every $g \in J \subseteq J'$. This is to say $(a_1, \ldots, a_n) \in V(J)$, which implies $f(a_1, \ldots, a_n) = 0$ since $f \in I(V(J))$. However, this yields $f(a)b - 1 = -1 \neq 0$. This contradicts the choice of our point.

By the first part of the Theorem, we have that this implies $J' = K[x_1, \ldots, x_n, y]$. This is to say

$$1 = \sum_i g_i h_i + g_0(fy - 1) \qquad \text{for some } g_i \in K[x_1, \ldots, x_n, y],\ h_i \in J$$

Multiplying this by some sufficiently high power of f, enough to dominate the appearances of y, we get

$$f^m = \sum_i G_i H_i + G_0(fy - 1) \qquad \text{for some } G_i \in K[x_1, \ldots, x_n, fy],\ H_i \in J$$

But since this is a relationship between polynomials, we can set the 'variable' $fy = 1$. Doing so verifies that $f^m \in J$, as desired. □

A corollary is that V and I induce bijections between radical ideals and varieties:

$$\{J = \sqrt{J} \subseteq K[x_1, \ldots, x_n]\} \longleftrightarrow \{X = V(J) \subseteq K^n\}$$

As we have noted previously, prime ideals are themselves radical. Therefore, we can also naturally detect what prime ideals represent under this correspondence.

Definition 21.4. A variety $X \subseteq K^n$ is called **irreducible** if X cannot be expressed as a union of 2 proper subvarieties:

$$X \neq X_1 \cup X_2 \quad \text{where } X_1 \neq X \neq X_2$$

Otherwise, X is called **reducible**.

This is exactly the geometric analog of being prime. We will pick up with the proof of the following statement next time:

Proposition 21.5. *X is irreducible if and only if $I(X)$ is prime:*

$$\mathit{Spec}(K[x_1, \ldots, x_n]) = \{J \subseteq K[x_1, \ldots, x_n] \text{ prime}\} \longleftrightarrow \{V = V(J) \subseteq K^n \text{ irreducible}\}$$

Example 21.6. If we consider the ideal $J = \langle xy \rangle$ in $K[x, y]$, geometrically we get a union of the lines $x = 0$ and $y = 0$ in K^2. Therefore we anticipate that $V(J)$ is reducible. Indeed, it is easy to check that $V(J) = V(x) \cup V(y)$.

So we can already see that the variety associate to a non-prime ideal can be reducible, facilitating Proposition 21.5's plausibility.

CLASS 22, APRIL 12TH: THE ZARISKI TOPOLOGY

Today we will take a dive into topology to develop the fundamentals of a geometric space. This will allow us to properly frame our notion of a variety in the broader geometric landscape. Recall that we left off with

Proposition 1. *X is irreducible if and only if $I(X)$ is prime:*

$$Spec(K[x_1,\dots,x_n]) = \{J \subseteq K[x_1,\dots,x_n] \text{ prime}\} \longleftrightarrow \{V = V(J) \subseteq K^n \text{ irreducible}\}$$

Proof. Suppose $I(X)$ is not prime. Then there exist $f, g \notin I(X)$ such that $fg \in I(X)$. Consider the ideals $I(X) + \langle f\rangle$ and $I(X) + \langle g\rangle$. Then we get that

$$X = V(I(X)) \supseteq V(I(X) + \langle f\rangle) \cup V(I(X) + \langle g\rangle)$$

On the other hand, if $\mathfrak{m}$ is a maximal (or even prime) ideal containing $I(X)$, then it necessarily contains either f or g by primality. As a result, we get the reverse inclusion and realize X as a union of 2 proper subvarieties. Note they are proper since $f, g \notin I(X)$.

If $X = X_1 \cup X_2$ is reducible. Let $I = I(X)$ and $I_i = I(X_i)$. Then the Lemma 22.1 (following this proof) allows us to conclude the result. Indeed,

$$(I(X) + \langle f\rangle) \cdot (I(X) + \langle g\rangle) = I(X)^2 + fI(X) + gI(X) + \langle fg\rangle \subseteq I(X)$$

or rephrased

$$V(I(X) + \langle g\rangle) \cup V(I(X) + \langle g\rangle) = V((I(X) + \langle f\rangle) \cdot (I(X) + \langle g\rangle)) \supseteq V(I(X)) = X$$

□

Lemma 22.1. *If I and J are ideals of $K[x_1,\dots,x_n]$, then*

$$V(I \cdot J) = V(I \cap J) = V(I) \cup V(J)$$

$$V(I + J) = V(I) \cap V(J)$$

Proof. For the first part, '$\supseteq$' follows by the inclusion reversing property of V. On the other hand, if a maximal ideal $\mathfrak{m}$ containing $I \cdot J$ does not contain I, then there exists $f \in I \setminus \mathfrak{m}$. For every $g \in J$, this implies $f \cdot g \in \mathfrak{m}$, and therefore $g \in \mathfrak{m}$ by primality. This is to say $\mathfrak{m} \supseteq J$, thus yielding the '$\subseteq$' containment.

For the second part, I will actually prove that the result holds for general sums (not only of 2 ideals). Recall that $\sum_\alpha I_\alpha$ is the smallest ideal containing each I_α. Therefore, by the inclusion reversing property of V we see that $V(\sum_\alpha I_\alpha) \subseteq V(I_\alpha)$ for all α. This gives the '$\subseteq$' direction.

Now suppose $\mathfrak{m} \in \bigcap_\alpha V(I_\alpha)$. This states that $\mathfrak{m}$ is an ideal containing all of the I_α. Thus by our description above, we get that $\mathfrak{m} \in V(\sum_\alpha I_\alpha)$, as desired. □

Corollary 22.2. *Every variety is of the form*

$$V(I) = V(\langle f_1,\dots,f_m\rangle) = V(\langle f_1\rangle) \cap \dots \cap V(\langle f_m\rangle)$$

Sometimes $V(\langle f_i\rangle)$ is abbreviated to $V(f_i)$. It is commonly called a **hypersurface**.

Example 22.3. Let's check out what our tools imply about $V(I) \subseteq K^2$ for $I = \langle x(y-1), x^2 - 5y^2 \rangle$. Let's assume K is algebraically closed (or at least contains $\sqrt{5}$). We see that

$$V(I) = V(x(y-1)) \cap V(x^2 - 5y^2) = (V(x) \cup V(y-1)) \cap \Big(V(x - \sqrt{5}y) \cup V(x + \sqrt{5}y) \Big)$$

As a result, we see that $V(I) = \{(0,0), (-\sqrt{5}, 1), (\sqrt{5}, 1)\}$ is composed of 3 points.

Lemma 22.1 gives us a natural relationship with topological spaces from geometry:

Definition 22.4. A **topological space** is a set X together with a collection $\tau \subseteq \mathcal{P}(X)$ (the power set of X, i.e. the set of all subsets of X) satisfying the following criteria:

(a) $X, \emptyset \in \tau$
(b) If $X_1, \ldots, X_n \in \tau$, then $X_1 \cup \ldots \cup X_n \in \tau$.
(c) If $\{X_\alpha \mid \alpha \in \Lambda\}$ is any collection of elements of τ (Λ is any set, be it uncountable or not), then so is their intersection

$$\bigcap_\alpha X_\alpha \in \tau$$

An element of τ is called a **closed subset** of X.

The conditions can be labeled as such: (a) is a minimum size criteria for a topology, making it so that there are at least 2 closed sets. (b) states finite unions of closed sets are closed, and (c) states any intersection of closed sets remains closed. This should pair well with your intuition of closed sets from real analysis.

There are also corresponding ways to define a topology based on the **open sets** of X, which are precisely the complements of closed sets.

Corollary 22.5. *The set of varieties*

$$\tau = \{V(J) \mid J \subseteq K[x_1, \ldots, x_n] \text{ an ideal}\}$$

induces a topology on K^n.

Proof. Properties (b) & (c) are guaranteed by Lemma 22.1. The only thing to note is that $X = V(0)$ and $\emptyset = V(K[x_1, \ldots, x_n])$. □

Definition 22.6. The topology described in Corollary 22.5 is the **Zariski Topology**.

One thing to note is that this gives a VERY different interpretation of closed sets from that of Real Analysis. In particular, an 'open ball' of some radius is very much not open in the Zariski Topology. The following example allows us to see that open sets in the Zariski topology are open in the Euclidean Topology:

Example 22.7. If $(a_1, \ldots, a_n) \notin V(I)$, then this is simply saying that if $I = \langle f_1, \ldots, f_m \rangle$, then there is some f_i such that $f_i(a_1, \ldots, a_n) \neq 0$. But since polynomials are continuous in the Euclidean topology, we know that there is a ball B of some radius about $(a_1, \ldots, a_n)$ such that $f_i(b_1, \ldots, b_n) \neq 0$ for every $(b_1, \ldots, b_n) \in B$. As a result, we can conclude that $V(I)$ is closed in the Euclidean topology.

CLASS 23, APRIL 15TH: NOETHERIAN TOPOLOGIES

Today we will cover decomposition into irreducible subvarieties, an accompanying result to our intersection of hypersurfaces result from last time. To begin, I would like to demonstrate that the notion of Noetherian for rings translates nicely into a statement for topological spaces.

Definition 23.1. A topological space is said to be **Noetherian** if either

- Every descending chain of closed subsets must eventually stabilize:
$$V_1 \supseteq V_2 \supseteq \ldots \supseteq V_N = V_{N+1} = \ldots$$
That is to say that closed subsets have the D.C.C.
- Every non-empty set of closed subsets has a minimal element, one containing no other closed subset properly.

Checking that these 2 properties are equivalent is identical to the methods for Noetherian/Artinian rings previously; use Zorn's Lemma. As a result, we get the following:

Proposition 23.2. *The Zariski topology is Noetherian for K^n.*

Proof. The DCC for varieties translates to the ACC for ideals by the inclusion reversing property of the function (functor) I. Then the Hilbert basis theorem allows us to conclude that $K[x_1, \ldots, x_n]$ is a Noetherian ring, and thus the ascending chain of ideals stabilizes. Applying V again and noting that $V(I(X)) = X$ if X is a variety shows the desired statement. □

Next time we will talk about a slightly different style of decomposition using our new notion of irreducible varieties.

Proposition 23.3. *If $X \subseteq K^n$ is a variety, then X can be decomposed as*
$$X = X_1 \cup \ldots \cup X_n$$
where X_i is an irreducible variety. We can make such a decomposition unique by forcing $X_i \not\subseteq X_j$ for any $i \neq j$.

Proof. Let $\mathcal{S}$ be the set of varieties that have no such decomposition. If $\mathcal{S} = \emptyset$, we are done. By the Noetherian property, if $\mathcal{S} \neq \emptyset$, then $\mathcal{S}$ contains a minimal element X. X clearly can't be irreducible, because then $X = X$ is the correct decomposition. Therefore $X = X_1 \cup X_2$ for 2 smaller varieties X_i. These are not in $\mathcal{S}$ by minimality, so each have a finite decomposition. This contradicts the fact that $X \in \mathcal{S}$.

For the uniqueness statement, suppose $X = X_1 \cup \ldots \cup X_n = X_1' \cup \ldots \cup X_m'$. Since each X_i and X_j' are irreducible, we can conclude $X_i \subseteq X_j' \subseteq X_{i'}$ for some j' depending on i and i' depending on j. This can be seen since
$$X_i \subseteq X = X_1' \cup \ldots \cup X_m' \qquad \Longrightarrow \qquad X_i = (X_1' \cap X_i) \cup \ldots \cup (X_m' \cap X_i)$$
Since the right hand side is a union of closed sets (topology!), this would imply X_i is non-irreducible. But this would imply that $X_i \subseteq X_{i'}$, which would mean $X_i = X_j' = X_{i'}$, as asserted. □

By our correspondence of irreducible varieties with prime ideals, we get the following neat corollary:

Corollary 23.4. *If $J \subseteq K[x_1, \ldots, x_n]$ is a radical ideal, then J is an intersection of* **finitely** *many prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$.*

Proof. Applying V yields

$$V(J) = X_1 \cup \cdots \cup X_m = V(\mathfrak{p}_1) \cup \cdots \cup V(\mathfrak{p}_m)$$

Applying I then yields

$$J = I(V(J)) = I(V(\mathfrak{p}_1) \cup \cdots \cup V(\mathfrak{p}_m)) = I(V(\mathfrak{p}_1)) \cap \cdots \cap I(V(\mathfrak{p}_m)) = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_m$$

□

This result is a very important special case of the **associated primary decomposition** which we will discuss in chapter 7 of Reid.

Corollary 23.5. *If J is a radical ideal, and $J = \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_m$ is the resulting minimal decomposition from Corollary 23.4, then the set of minimal primes of R/J is exactly $\mathfrak{p}_1 R/J, \ldots, \mathfrak{p}_m R/J$. Therefore the fraction ring of R/J is given as*

$$\mathrm{Frac}(R/J) = \mathrm{Frac}(R/\mathfrak{p}_1) \times \cdots \times \mathrm{Frac}(R/\mathfrak{p}_m)$$

Where each $\mathrm{Frac}(R/\mathfrak{p}_i)$ is simply the fraction field of an integral domain.

By minimal, I mean that there are not redundant choices of prime ideal.

Proof. Since each $\mathfrak{p}_i \supseteq J$, we have $\cup_i V(\mathfrak{p}_i) \subseteq V(J)$. Similarly, if $\mathfrak{p} \supseteq J$ is prime, then $\mathfrak{p} \supseteq \mathfrak{p}_i$ for some i. This follows by our standard trick; By induction, it suffices to prove the case of $m = 2$. Note that

$$\mathfrak{p}_1 \cdot \mathfrak{p}_2 \subseteq \mathfrak{p}_1 \cap \mathfrak{p}_2 \subseteq \mathfrak{p}$$

Then $\mathfrak{p}_1 \subseteq \mathfrak{p}$ or $\mathfrak{p}_2 \subseteq \mathfrak{p}$. Indeed, if $a \in \mathfrak{p}_1 \setminus \mathfrak{p}$, then $ab \in \mathfrak{p}$ for all $b \in \mathfrak{p}_2$ implies $b \in \mathfrak{p}$ by primality. Finally, since $\mathfrak{p}_i \not\subseteq \mathfrak{p}_j$ for all $i \neq j$, this completes the proof.

□

Example 23.6. Consider the ideal $J = \langle x^2yz^n - z^{n+2} \rangle \subseteq K[x, y, z]$ for some $n \geq 1$. It can be checked that $\sqrt{J} = \langle x^2yz - z^3 \rangle$. Its decomposition into primes can be represented by

$$J = \langle x^2y - z^2 \rangle \cap \langle z \rangle$$

The ideal on the left represents the 'Whitney Umbrella'.

Example 23.7. Consider the ideal

$$J = \langle y^2w, x\,y\,w, x^2w, y^2z, x\,y\,z, x^2z \rangle \subseteq K[x, y, z, w]$$

Computing its corresponding decomposition, we can actually note that

$$J = \langle x, y \rangle^2 \cap \langle u, v \rangle \qquad \Longrightarrow \qquad \sqrt{J} = \langle x, y \rangle \cap \langle u, v \rangle$$

Geometrically, this implies that $V(J)$ looks like $V(\langle x, y \rangle) \cup V(\langle z, w \rangle)$. On the right we have the maximal ideals of $K[u, v]$ and $K[x, y]$ respectively, obtained by modding out by the corresponding ideals. Thus it is a union of K planes meeting at a single point $(0, 0, 0, 0) \in K^4$.

CLASS 24, APRIL 17TH: SCHEME THEORETIC PERSPECTIVE

As we know, there are many rings which aren't (quotients, or localizations, or completions of) polynomial rings over a field. The easiest examples to reconcile are $\mathbb{Z}$ or $\mathbb{Z}_p$, the p-adic integers (power series in p). This gives us a good reason to study a topological space which is very similar to a variety, but with some extra points which represent subvarieties. Recall Proposition 21.5:

Proposition 1. *X is irreducible if and only if $I(X)$ is prime:*

$$Spec(K[x_1, \ldots, x_n]) = \{J \subseteq K[x_1, \ldots, x_n] \text{ prime}\} \longleftrightarrow \{V = V(J) \subseteq K^n \text{ irreducible}\}$$

Definition 24.1. Given a ring R, we can endow the set $X = \mathrm{Spec}(R)$ with the Zariski Topology generated by closed sets

$$V(J) = \{\mathfrak{p} \in \mathrm{Spec}(R) \mid J \subseteq \mathfrak{p}\}$$

We call the resulting topological space an **affine scheme**.

Sometimes the two notions are conflated and people refer to this more modern approach as an affine variety. There are a few advantages to this change.

(a) There exists a map from $V(J)$ to $\mathrm{Spec}(K[x_1, \ldots, x_n]/J)$ sending $(a_1, \ldots, a_n)$ to $\mathfrak{m} = \langle x_1 - a_1, \ldots, x_n - a_n \rangle \in \mathrm{Spec}(K[x_1, \ldots, x_n])$. For those of you who have dealt with topological spaces before, this is an injective continuous map inducing a homeomorphism onto its image. Therefore, it is a topological embedding!
(b) To get any irreducible subvariety of K^n, we simply need to take a *point* (i.e. a prime ideal) of $\mathrm{Spec}(K[x_1, \ldots, x_n])$ and take its closure. Therefore $\mathrm{Spec}(K[x_1, \ldots, x_n])$ contains much more information than K^n itself.
(c) We can produce a natural way of defining a map between varieties: It should look like $\varphi^{\#} : \mathrm{Spec}(S) \to \mathrm{Spec}(R)$ for some ring homomorphism $\varphi : R \to S$. It turns out that this is actually a continuous map when we put the Zariski topology on each Spec.
(d) One doesn't need to view a variety inside K^n. This is a general theme in geometry; you care about the variety itself, not where it lives.
(e) It generalizes naturally to broader rings.

This style of reasoning yields more general results then for varieties without too much hard work.

Proposition 24.2. *Let R be a Noetherian ring with J a proper ideal.*

(a) *$V(J) \subseteq \mathrm{Spec}(R)$ contains only finitely many minimal primes.*
(b) *$\sqrt{J} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n$.*
(c) *Considering $J = 0$ in the previous case, if R is a ring with zero divisors, then either R has nilpotents or R has a finite number $n \geq 2$ of minimal primes.*

Proof. (a) $V(J)$ has an irreducible decomposition $X_1 \cup \cdots \cup X_n$ where each X_i is irreducible and $X_i \not\subseteq X_j$ for all $i \neq j$. Proposition 1 extended to general Noetherian rings (with the same proof) allows us to conclude $I(X_i) = \mathfrak{p}_i$ is prime. Thus $\mathfrak{p}_i$

contains J by the inclusion reversing property of I. The maximal such X_i are minimal among primes containing J, as desired.

(b) This follows from part (a) and the fact that
$$\sqrt{J} = \bigcap_{\mathfrak{p} \supseteq I} \mathfrak{p}$$
which was proved as Corollary 5.5 in our notes.

(c) $\sqrt{0} = 0$ if and only if R is reduced ring. Since R contains zero divisors, 0 is itself not prime. Thus the result of part (b) implies there are at least 2 primes represented in the intersection.

□

Example 24.3. If we consider $V(n) \subseteq \text{Spec}(\mathbb{Z})$, the statement shows there are only finitely many primes (minimally) containing. Let $n = p_1^{e_1} \cdots p_n^{e_n}$ be its prime decomposition. Then
$$\sqrt{\langle n \rangle} = \langle p_1 \rangle \cap \cdots \cap \langle p_n \rangle$$
This recovers a result from an early homework.

Example 24.4. Sometimes the decomposition is less clear. We know $\mathbb{Z}[x, y, z]/I$ is a Noetherian ring by virtue of the Hilbert Basis Theorem. As a result, any radical ideal J has such a decomposition. For example, considering
$$J = \langle -5\,y^5 - 5\,z^3 + 5\,x^2, -5\,y^6 - 5\,y\,z^3 + 5\,x^2y, -y^8 + x^2y^5 - y^3z^3 + x^2y^3 + x^2z^3 - x^4 \rangle$$
It can be checked through hard computation (or by use of a computer) that J is a radical ideal, and it has a decomposition into primes
$$J = \langle x^2 - y^3 - z^5 \rangle \cap \langle 5, x^2 - y^3 \rangle$$

As a corollary, we have the following cool result:

Corollary 24.5. *If R is a reduced Noetherian ring, then R injects into a finite product of integral domains.*

Proof. Given R is Noetherian and reduced, we get
$$0 = \sqrt{0} = \cap_{\mathfrak{p} \text{ prime}} \mathfrak{p} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n$$
Where $\mathfrak{p}_i$ are the finitely many minimal primes of R. Therefore, we see that the kernel of the map $R \to R/\mathfrak{p}_1 \times \cdots \times R/\mathfrak{p}_n$ is the intersection of the primes, which is 0. □

It should be noted that non-reduced elements can't map to non-zero elements of a reduced ring (or domain in particular). So in some sense this is best possible in that regard.

Example 24.6. $R = K[x_1, \ldots, x_n]/\langle x_1 x_2 \cdots x_n \rangle$ is often called the **simple normal crossing** ring, because geometrically it looks like n hyperplanes intersecting with 'perpendicular' crossings. The previous result shows that
$$R \hookrightarrow R/\langle x_1 \rangle \times \cdots \times R/\langle x_n \rangle \cong K[x_2, \ldots, x_n] \times K[x_1, x_2, \ldots, x_n] \times \cdots \times K[x_1, \ldots, x_{n-1}]$$
So we can view $\text{Spec}(R) \leftarrow \mathbb{A}_K^{n-1} \cup \overset{n-\text{times}}{\cdots\cdots} \cup \mathbb{A}_K^{n-1}$ as a nice surjective map. This map is in fact always surjective, since every prime ideal or R contains some minimal prime.

CLASS 25, APRIL 19TH: MACAULAY2 & SUPPORT OF MODULES

Today's class will be divided into two parts; first, I will do a small tutorial on Macaulay2, a computer algebra system which can be used to verify examples and thus hypotheses for general theorems. Then we will move on to the support of a module (chapter 7 of Reid). Here are some of the important websites to associate with Macaulay2 (M2):

- `http://www2.macaulay2.com/Macaulay2/`: This is the official webpage for M2. It contains the installable binaries for many popular distributions, such as OSX and Ubuntu, under the appended /Downloads/ url. There are also a few guides under /GettingStarted/ written by some prolific M2 programmers and mathematicians.
- `https://github.com/Macaulay2/M2`: The GitHub repository for Macaulay2, containing the most up-to-date code. There may be some compiler optimizations available if you compile the packages on your own, which may increase speed of code execution.
- `http://habanero.math.cornell.edu:3690/`: Cornell (in particular Mike Stillman) provide a remote web client version of Maculay2. It is currently at version 1.12 (as of April 9^{th}, 2019) which is nearly the newest version (1.13). This can be helpful if there isn't a pre-compiled version for your distribution.

The code executed in class will be made available as Class25.M2.pdf on GLOW.

Now we will begin to focus our attention on the structure of ideals. We have seen in the last section that radical ideals in Noetherian rings can be decomposed into finite intersections of prime ideals. Of course, such a thing can't be expected to hold for more general ideals (such as powers of a single prime ideal). We will begin this story by studying the support of a module.

Definition 25.1. Given an R-module M, the **support of** M is the set

$$\mathrm{Supp}_R(M) = \{\mathfrak{p} \in \mathrm{Spec}(R) \mid M_{\mathfrak{p}} \neq 0\}$$

Recall the **annihilator of** M is the ideal

$$\mathrm{Ann}_R(M) = \{r \in R \mid rM = 0\}$$

If the context is clear, sometimes the R subscript is omitted in these notations. Finally, $r \in R$ is called a **zero divisor** for M if $rm = 0$ for some $m \neq 0$.

This has a clear geometric significance. $M_{\mathfrak{p}}$ should be viewed as the structure of M near a point $\mathfrak{p} \in \mathrm{Spec}(R)$. The support tells us where the module has local significance (i.e. is non-zero). Thus, by the dicussion of Class 19, $\mathrm{Supp}(M) = \emptyset$ if and only if $M = 0$. The following theorem tells us that in most cases of interest, modules are interesting most of the time.

Proposition 25.2. (a) *If* $\mathfrak{p} \in \mathrm{Supp}(M)$, *then* $V(\mathfrak{p}) \subseteq \mathrm{Supp}(M)$.
(b) *If* $M = \langle x \rangle$ *is principal, then* $\mathrm{Supp}(M) = V(\mathrm{Ann}(M))$.
(c) *If* $M = \sum_i M_i$, *then* $\mathrm{Supp}(M) = \bigcup_i \mathrm{Supp}(M_i)$.
(d) *If* M *is finitely generated, then* $\mathrm{Supp}(M) = V(\mathrm{Ann}(M))$.

(e) *If* $0 \to M' \to M \to M'' \to 0$ *is a SES, then* $\operatorname{Supp}(M) = \operatorname{Supp}(M') \cup \operatorname{Supp}(M'')$.

Proof. (a) If $\mathfrak{p}' \supseteq \mathfrak{p}$ is a prime ideal, then

$$M_{\mathfrak{p}} = (M_{\mathfrak{p}'})_{\mathfrak{p}}$$

As a result, we have that if $M_{\mathfrak{p}'} = 0$, then $M_{\mathfrak{p}} = 0$.

(b) If $Ann(x) \not\subseteq \mathfrak{p}$, then let y be in their difference. We have that $(w, rx) \sim (1, 0)$:

$$y(rx - 0w) = r(yx) = r0 = 0$$

Thus $M_{\mathfrak{p}} = 0$. If $\operatorname{Ann}(x) \subseteq \mathfrak{p}$, for the same reason we can conclude $(1, x) \not\sim (1, 0)$.

(c) Localization is exact, so $(M_i)_{\mathfrak{p}} \subseteq M_{\mathfrak{p}}$. This shows the $\supseteq$ direction. For $\subseteq$, if

$$m = m_{i_1} + \cdots + m_{i_n}$$

where $m_{i_j} \in M_{i_j}$, and $x_j \notin \mathfrak{p}$ is such that $x_j \cdot m_{i_j} = 0$, then $x_1 \cdots x_n \cdot m = 0$.

(d) $M = \langle m_1, \ldots, m_n \rangle = \langle m_1 \rangle + \ldots + \langle m_n \rangle$, then

$$\operatorname{Supp}(M) = \bigcup_{i=1}^{n} \operatorname{Supp}(\langle m_i \rangle) = \bigcup_{i=1}^{n} V(\operatorname{Ann}(m_i)) = V\left(\bigcap_{i=1}^{n} \operatorname{Ann}(m_i) \right) = V(\operatorname{Ann}(M))$$

(e) Since localization is exact, we see

$$0 \to M'_{\mathfrak{p}} \to M_{\mathfrak{p}} \to M''_{\mathfrak{p}} \to 0$$

is an exact sequence of $R_{\mathfrak{p}}$-modules. As a result, $M'_{\mathfrak{p}} = 0$ and $M''_{\mathfrak{p}} = 0$ if and only if $M_{\mathfrak{p}} = 0$. This shows the desired statement.

□

Example 25.3. We have essentially handled the case of finitely generated modules in part (d) of Proposition 25.2. Consider the $\mathbb{Z}$ module $M = \oplus_{n \in \mathbb{N}} \mathbb{Z}/2^n\mathbb{Z}$. The annihilator of each component of the sum is precisely $\langle 2^n \rangle \subseteq \mathbb{Z}$. Therefore, if we tried to generalize the result of part (d), we would note that

$$\operatorname{Ann}(M) = \bigcap_{n \in \mathbb{N}} \operatorname{Ann}(Z/2^n\mathbb{Z}) = 0$$

and thus we might expect the support to be $V(0) = \operatorname{Spec}(\mathbb{Z})$. However, if we localize at any prime different than $\langle 2 \rangle$, we invert 2 and thus 2^n. As a result, we have that for all $a \in \mathbb{Z}/2^n\mathbb{Z}$,

$$2^n a = 0 \qquad \Longrightarrow \qquad (1, m) \sim (1, 0) = 0$$

So in fact $\operatorname{Supp}(M) = \langle 2 \rangle$.

There is a similarly startling realization when considering the module $M = \oplus_{n \in \mathbb{N}} \mathbb{Z}/n\mathbb{Z}$. Note that $\operatorname{Ann}(M) = 0$, thus $V(\operatorname{Ann}(M)) = \operatorname{Spec}(\mathbb{Z})$. However, $0 \notin \operatorname{Supp}(M)$.

One can note however that $\operatorname{Supp}(M) \subseteq V(\operatorname{Ann}(M))$ in full generality.

CLASS 26, APRIL 22ND: ASSOCIATED PRIMES

Today, we will return to the question of how to express a generic ideal in terms of prime ideals. The first step in this direction is to study the associated primes, or assassins, of an ideal, which might as well be defined for modules:

Definition 26.1. If M is an R-module, $\mathfrak{p} \in \operatorname{Spec}(R)$ is said to be **associated to** M, or an **associated prime of** M, or an **assassin of** M, if there exists an injective module homomorphism $R/\mathfrak{p} \hookrightarrow M$, i.e. $R/\mathfrak{p}$ is a submodule of M.

We (unflatteringly) call the set of Associated primes $\operatorname{Ass}(M)$.

Proposition 26.2. *Every $\mathfrak{p} \in \operatorname{Ass}(M)$ has the property that $\operatorname{Ann}(M) \subseteq \mathfrak{p}$. Additionally, $\mathfrak{p} \in \operatorname{Ass}(M)$ if and only if there exists $m \in M$ such that $\operatorname{Ann}(m) = \mathfrak{p}$.*

Proof. The second result implies the first, since $\operatorname{Ann}(M) = \bigcap_{0 \neq m \in M} \operatorname{Ann}(m)$.

$\Rightarrow$: Suppose $\mathfrak{p} \in \operatorname{Ass}(M)$. Then $R/\mathfrak{p} \hookrightarrow M$. Consider the image of $1 + \mathfrak{p}$ and call it m. Then it is immediate that $\operatorname{Ann}(m) = \mathfrak{p}$ by injectivity of the map.

$\Leftarrow$: Of course, if $\operatorname{Ann}(m) = \mathfrak{p}$, then we can construct the injective map

$$R/\mathfrak{p} \to M : 1 \mapsto m$$

□

Example 26.3. If $n = p_1^{e_1} \cdots p_l^{e_l}$, then we can easily conclude that

$$\operatorname{Ass}(Z/n\mathbb{Z}) = \{\langle p_1 \rangle, \ldots, \langle p_l \rangle\}$$

This comes by considering the elements

$$m_i = p_1^{e_1} \cdots p_i^{e_i - 1} \cdots p_l^{e_l} \in \mathbb{Z}/n\mathbb{Z}$$

for various i, which clearly has annihilator $\langle p_i \rangle$. Note that by our previous analysis we can conclude the following cool result:

$$\sqrt{\langle n \rangle} = \langle p_1 \rangle \cap \cdots \cap \langle p_l \rangle = \bigcap_{\mathfrak{p} \in \operatorname{Ass}(\mathbb{Z}/n\mathbb{Z})} \mathfrak{p}$$

We will later see how deeply this connection goes. But first, we move onto the properties of $\operatorname{Ass}(M)$.

Proposition 26.4.
(a) *If $x \in M$ has $\operatorname{Ann}(x) = \mathfrak{p} \in \operatorname{Spec}(R)$, then every non-zero R-multiple of x, say $y = rx$, has $\operatorname{Ann}(y) = \mathfrak{p}$ as well. Thus $\operatorname{Ass}(R/\mathfrak{p}) = \{\mathfrak{p}\}$*
(b) *A maximal element of $\mathcal{S} = \{\operatorname{Ann}(m) \mid 0 \neq m \in M\}$ is prime, and thus in $\operatorname{Ass}(M)$.*
(c) *If R is Noetherian, then $M \neq 0$ implies $\operatorname{Ass}(M) \neq \emptyset$.*
(d) *Given a SES $0 \to M' \to M \to M'' \to 0$, we have that*

$$\operatorname{Ass}(M') \subseteq \operatorname{Ass}(M) \subseteq \operatorname{Ass}(M') \cup \operatorname{Ass}(M'')$$

Proof.
(a) x is the image of 1 for some $R/\mathfrak{p} \hookrightarrow M$. As a result, since $R/\mathfrak{p}$ is a domain, y has image r which is a non-zero divisor. Thus $\operatorname{Ann}(y) = \mathfrak{p}$.
(b) Assume $\operatorname{Ann}(m)$ is maximal in $\mathcal{S}$. Suppose $x \cdot y \in \operatorname{Ann}(m)$, but $x, y \notin \operatorname{Ann}(m)$. Then $x \cdot m \neq 0$, and is annihilated by y. Therefore, $\operatorname{Ann}(m) \subsetneq \operatorname{Ann}(xm)$, contradicting maximality.

(c) The Noetherian property implies that any ascending chain
$$\mathrm{Ann}(m_1) \subseteq \mathrm{Ann}(m_2) \subseteq \cdots$$
must stabilize, providing an upper bound. Thus a maximal element in $\mathcal{S}$ of part (b) exists by Zorn's Lemma, and is therefore associated to M.

(d) If $\mathfrak{p} \in \mathrm{Ass}(M')$ composing yields $R/\mathfrak{p} \hookrightarrow M' \hookrightarrow M$, showing $\mathfrak{p} \in \mathrm{Ass}(M)$. Suppose $R/\mathfrak{p} \subseteq M$. Then we have that either $R/\mathfrak{p} \cap M' = 0$, in which case $R/\mathfrak{p} \hookrightarrow M''$. Alternatively, $R/\mathfrak{p} \cap M' \neq 0$. If x is in this intersection, then $\mathrm{Ann}(x) = \mathfrak{p}$ by part (a), showing $\mathfrak{p} \in \mathrm{Ass}(M')$.

□

Corollary 26.5. *If R is Noetherian, then for an R-module M,*
$$\{\textit{zero divisors of } M\} = \bigcup_{\mathfrak{p} \in \mathrm{Ass}(M)} \mathfrak{p}$$

Proof. This follows since zero divisors must be in some $\mathrm{Ann}(m)$ and by (b) of Proposition 26.4. For the reverse inclusion, each $\mathfrak{p}$ is the annihilator of some element by Proposition 26.2. □

Example 26.6. Let I be a radical ideal of a Noetherian domain R. Then
$$I = \sqrt{I} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_m$$
for some primes $\mathfrak{p}_i \in \mathrm{Spec}(R)$. Then we can form an exact sequence
$$0 \to I \to R \to R/I \to 0$$
by Proposition 26.4 (d), we know that
$$\mathrm{Ass}(I) \subseteq \mathrm{Ass}(R) \subseteq \mathrm{Ass}(I) \cup \mathrm{Ass}(R/I)$$
However, R being a domain implies $\mathrm{Ann}(r) = 0$ for every $r \neq 0$, so the only associated prime is 0 itself. However, since $R/I \hookrightarrow R/\mathfrak{p}_1 \times \cdots \times R/\mathfrak{p}_n$, we see $\mathrm{Ass}(R/I) \subseteq \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$. It is harder to get equality here, but in the case of the Chinese Remainder Theorem (i.e. each $\mathfrak{p}_i, \mathfrak{p}_j$ is coprime, c.f. Theorem 26.7), the above inclusion is actually an isomorphism! Thus it is easy to construct an example ($I = \mathfrak{p}_i$) where
$$\mathrm{Ass}(R) \subsetneq \mathrm{Ass}(I) \cup \mathrm{Ass}(R/I)$$

Theorem 26.7 (Chinese Remainder Theorem)**.** *If $I_1, \ldots, I_n$ are pairwise coprime ideals (i.e. $I_i + I_j = R$ for each $i \neq j$), and $I = I_1 \cap \cdots \cap I_n$, then*
$$R/I \cong R/I_1 \times \cdots \times R/I_n$$

Proof. The map $R \to R/I_1 \times \cdots \times R/I_n : r \mapsto (r + I_1, \ldots, r + I_n)$ has kernel I. It only goes to show that it is also surjective.

I proceed by induction. If $n = 2$, then we can choose $a \in I_1$ and $b \in I_2$ such that $a + b = 1$. Then considering $r_2 a + r_1 b \in R$, we have that its image is
$$(r_1, r_2) \equiv (r_1 a + r_1 b, r_2 a + r_2 b) \equiv (r_2 a + r_1 b, r_2 a + r_1 b) \equiv (r_1 b, r_2 a) \pmod{I_1 \times I_2}$$
For the induction, it only goes to note that $I_1 \cap \cdots \cap I_{n-1}$ is coprime to I_n. Taking $a_i + b_i = 1$ for $a_i \in I_i$ and $b_i \in I_n$ for $i = 1, \ldots, n-1$, we can conclude
$$1 = 1^{n-1} = \prod_i (a_i + b_i) \in a_1 \cdots a_n + I_n \subseteq I_1 \cap \cdots \cap I_{n-1} + I_n$$
as desired! □

CLASS 27, APRIL 24TH: $\mathrm{Supp}(R)$ VS $\mathrm{Ass}(R)$

Today we will discuss the relationship between associated primes and the support of a given module M. The primary result is as follows:

Theorem 27.1. *If M is an R-module, then $\bigcup_{\mathfrak{p}\in \mathrm{Ass}(M)} V(\mathfrak{p}) \subseteq \mathrm{Supp}(M)$. In particular, associated primes are in the support. Additionally, if R is Noetherian, and $\mathfrak{p} \in \mathrm{Supp}(M)$ is a minimal element, then $\mathfrak{p} \in \mathrm{Ass}(M)$.*

Proof. By Proposition 25.2 (a), it suffices to check that $\mathrm{Ass}(R) \subseteq \mathrm{Supp}(M)$. Let $\mathfrak{p} = \mathrm{Ann}(m)$ be an associated prime and consider the residue field $k(\mathfrak{p}) := (R/\mathfrak{p})_{\mathfrak{p}}$. Since $R/\mathfrak{p} \subseteq M$, we have $k(\mathfrak{p}) \subseteq M_{\mathfrak{p}}$. Therefore, $\mathfrak{p} \in \mathrm{Supp}(M)$.

Now on to the additional statement. Suppose $\mathfrak{p} \in \mathrm{Supp}(M)$ is minimal. This is to say for any $\mathfrak{q} \subsetneq \mathfrak{p}$, we have $M_{\mathfrak{q}} = 0$ but $M_{\mathfrak{p}} \neq 0$.

Step 1: (Prove the result in the local case). Consider $M_{\mathfrak{p}}$ as an $R_{\mathfrak{p}}$-module. Since $M_{\mathfrak{p}}$ is a non-zero module over a Noetherian ring, $\mathrm{Ass}_{R_{\mathfrak{p}}}(M_{\mathfrak{p}}) \neq \emptyset$. I claim that the only possibility is $\mathfrak{p}R_{\mathfrak{p}}$ itself. Suppose $\mathfrak{q} \subseteq \mathfrak{p}$. Then

$$(M_{\mathfrak{p}})_{\mathfrak{q}R_{\mathfrak{p}}} = M_{\mathfrak{q}} = 0$$

by our minimality assumption. As a result, $\mathrm{Supp}(M) = \{\mathfrak{p}R_{\mathfrak{p}}\}$. This necessarily implies $\mathrm{Ass}_{R_{\mathfrak{p}}}(M_{\mathfrak{p}}) = \{\mathfrak{p}R_{\mathfrak{p}}\}$, since $\mathrm{Ass}(R_{\mathfrak{p}}) \subseteq \mathrm{Supp}(R_{\mathfrak{p}})$.

Step 2: (Trace back to R itself). We note that step 1 yields that there exists $(s, m) \in M_{\mathfrak{p}}$ whose annihilator is precisely $\mathfrak{p}R_{\mathfrak{p}}$. If $t, u \notin \mathfrak{p}$, then t, u map to units in $R_{\mathfrak{p}}$. Therefore $u \notin \mathrm{Ann}(tm)$. This shows that $\mathrm{Ann}(tm) \subseteq \mathfrak{p}$. The assertion that remains to show is that there is a t to make this an equality.

Since $(1, p) \cdot (s, m) \sim (1, 0)$ for all $p \in \mathfrak{p}$, we have that $t \cdot pm = 0$ for some $t \notin \mathfrak{p}$ depending on p. $\mathfrak{p}$ is a finitely generated ideal by the Noetherian condition. As a result, we can choose t_i for $i = 1, \ldots, m$ for each of the generators, then notice $\mathrm{Ann}(t_1 \cdots t_n \cdot m) = \mathfrak{p}$. This completes the proof. □

This allows us to somewhat reverse the containment of Theorem 27.1:

Corollary 27.2. *If M is a finitely generated R-module, and R is Noetherian, then*

$$\mathrm{Supp}(M) = \cup_{i=1}^{n} V(\mathfrak{p}_i)$$

where $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ are the minimal primes containing $\mathrm{Ann}(M)$. Each $\mathfrak{p}_i \in \mathrm{Ass}(M)$.

Proof. We know that $\mathrm{Supp}(M) = V(\mathrm{Ann}(M))$, since M is finitely generated (by Proposition 25.2 (d)). Additionally, by Corollary 23.4, there are only finitely minimal primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ containing $\mathrm{Ann}(M)$, and $V(\mathrm{Ann}(M)) = \cup_{i=1}^{n} V(\mathfrak{p}_i)$. Since they are minimal in the support, Theorem 27.1 shows they are associated primes. □

This style of reasoning allows us to truly get at the structure of finitely generated modules over Noetherian rings:

Theorem 27.3. *If R is a Noetherian ring, and M is a finitely generated R-module, then there exists a chain of submodules*

$$0 = M_0 \subsetneq M_1 \subsetneq \ldots \subsetneq M_n = M$$

such that $M_i/M_{i-1} \cong R/\mathfrak{p}_i$ *for various* $\mathfrak{p}_i \in \operatorname{Spec}(R)$. *In addition,*

$$\operatorname{Ass}(M) \subseteq \{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}.$$

Proof. If $M \neq 0$, then there exists some associate prime $\mathfrak{p}_1 \in \operatorname{Ass}(M)$. This means precisely that $R/\mathfrak{p}_1 \subseteq M$. Call this module M_1. Then we can consider M/M_1. Either this is 0 or there exists an associated prime $\mathfrak{p}_2$. By the same procedure, we can construct $M_2' \cong R/\mathfrak{p}_2 \subseteq M/M_1$.This corresponds to modules

$$0 \subseteq M_1 \subseteq M_2 = M_2' + M_1 \subseteq M$$

Iterating this procedure yields an ascending chain

$$0 \subsetneq M_1 \subsetneq M_2 \subsetneq \ldots \subseteq M$$

But M is Noetherian, since it is finitely generated over a Noetherian ring. Therefore the chain eventually must stabilize, at M.

For the latter statement, we can consider $0 \to M_i \to M_{i+1} \to M_{i+1}/M_i \cong R/\mathfrak{p}_{i+1} \to 0$. Induction shows $\operatorname{Ass}(M_{i+1}) \subseteq \operatorname{Ass}(M_i) \cup \operatorname{Ass}(R/\mathfrak{p}_{i+1}) = \{\mathfrak{p}_1, \dots, \mathfrak{p}_{i+1}\}$. □

Definition 27.4. A series associated to M as in Theorem 27.3 is called a **prime filtration** for M.

Prime filtrations are non-unique, this is easily detectable for things such as direct sums: $R/\mathfrak{p} \oplus R/\mathfrak{q}$. Here is another few examples:

Example 27.5. The $\mathbb{Z}$-module $\mathbb{Z}/n\mathbb{Z}$ has a filtration of length $e_1 + \ldots + e_m$, where $n = p_1^{e_1} \cdots p_n^{e_n}$;

$$0 \subseteq Z/p_1\mathbb{Z} \subseteq \mathbb{Z}/p_1^2\mathbb{Z} \subseteq \mathbb{Z}/p_1^n\mathbb{Z} \subseteq \mathbb{Z}/p_1^n p_2\mathbb{Z} \subseteq \ldots \subseteq \mathbb{Z}/n\mathbb{Z}$$

Of course, there are many distinct possibilities for a series. Up to isomorphism, there are (at least)

$$\binom{e_1 + \ldots + e_n}{e_1, \ldots, e_n} = \binom{e_1 + \ldots + e_n}{e_1}\binom{e_2 + \ldots + e_n}{e_2} \cdots \binom{e_{n-1} + e_n}{e_{n-1}}\text{-many}$$

It should be noted that in this case the associated primes are exactly those which appear in the composition series.

Example 27.6. Consider the ring $R = K[x^4, x^3y, xy^3, y^4]$ and the ideal $I = \langle x^4 \rangle$. It can be checked that

$$\operatorname{Ass}(R/I) = \{\langle x^4, x^3y, xy^3 \rangle, \mathfrak{m} = \langle x^4, x^3y, xy^3, y^4 \rangle\}$$

The first is the annihilator of $(xy^3)^3 = x^3y^9$. Notice

$$x^3y \cdot x^3y^9 = x^4y^{10} = x^6y^{10} = x^4 \cdot (xy^3)^2 \cdot y^4 = 0$$

$$xy^3 \cdot x^3y^9 = x^4y^{12} = x^4(y^4)^3 = 0$$

Of $xy^3 \cdot y^{4i} \neq 0$ in R/I. I leave it to you to check $\operatorname{Ann}((x^3y)^2) = \mathfrak{m}$. This is already weird, as we have a non-minimal element in the associated primes. Such a thing is sometimes called an embedded component. Modding out by the first ideal, we get

$$0 \subseteq M_1 = R/\langle x^4, x^3y, xy^3 \rangle \cong K[y^4] \subseteq R/I$$

The cokernel of this inclusion is nothing but a K-vector space generated by $(x^3y)^i$ and $(xy^3)^i$. For $i = 1, 2, 3$. This accounted for with 6 iterations of $R/\mathfrak{m}$ (from the highest degree to lowest).

CLASS 28, APRIL 26TH: PRIMARY IDEALS

Today we will approach the idea of decomposing any ideal in a Noetherian ring. So far, we've shown that radical ideals are exactly intersections of finitely many primes. Here we will attempt to broaden that horizon. Recall (from homework 1!) the definition of a primary ideal.

Definition 28.1. $q \subseteq R$ an ideal is said to be **primary** if when $x \cdot y \in \mathfrak{q}$, then either $x \in \mathfrak{q}$ or $y^m \in \mathfrak{q}$ for some $m \in \mathbb{N}$.

This is a slight weakening of the notion of prime. Slight is clarified here:

Proposition 28.2. *If $\mathfrak{q}$ is a primary ideal, then $\sqrt{q}$ is a prime ideal.*

Proof. Suppose $x \cdot y \in \sqrt{q}$. This is to say that $x^n \cdot y^n \in \mathfrak{q}$ for some n. As a result, either $x^n \in \mathfrak{q}$ or $y^{nm} \in \mathfrak{q}$. But naturally this implies either $x \in \sqrt{q}$ or $y \in \sqrt{q}$. □

Thus it is also common to call a primary ideal **$\mathfrak{p}$-primary** to indicate directly the corresponding prime ideal $\mathfrak{p} = \sqrt{q}$.

Example 28.3. As checked in the first homework, $\langle p^n \rangle \subseteq \mathbb{Z}$ is a $\langle p \rangle$-primary ideal. Indeed, if $m \cdot l \in \langle p^n \rangle$, then either p^n divides m or it doesn't. If it doesn't, then p divides l which implies p^n divides l^n.

In fact you showed $\langle p^n \rangle$ is the only type of primary ideal in $\mathbb{Z}$.

It should be noted that if $\mathfrak{p}$ is a finitely generated ideal (e.g. R Noetherian), then since $\sqrt{\mathfrak{q}} = \mathfrak{p}$, we have that for some $N \gg 0$, we have that

$$\mathfrak{p}^N \subseteq \mathfrak{q} \subseteq \mathfrak{p}$$

Indeed, if $f_i^{n_i} \in \mathfrak{q}$ for the generators f_i, then $N = \sum_i (n_i - 1) + 1$ will suffice. One should however note that this is not enough to ensure that $\mathfrak{q}$ is a primary ideal.

Example 28.4. If $I = \langle x^2, xy \rangle$, then $\sqrt{I} = \langle x \rangle$. However, I is not primary, since $x \notin I$ and $y^n \notin I$ for any n.

This example shows that it is also not enough to ask either $x^n \in I$ or $y^n \in I$ for some I. This is a strictly weaker condition than 'primary'. There is however one example where this is not the case:

Proposition 28.5. *If $\sqrt{\mathfrak{q}} = \mathfrak{m}$ is a maximal ideal, then $\mathfrak{q}$ is $\mathfrak{m}$-primary.*

Proof. Let $f \notin \mathfrak{q}$. Then we can consider the ideal

$$I = \mathfrak{q} : f = \{g \in R \mid fg \in \mathfrak{q}\}$$

Note I is proper since $1 \notin I$. As a result, $I \subseteq \mathfrak{m}'$ for some maximal ideal $\mathfrak{m}'$. However, $\mathfrak{q} \subseteq \mathfrak{q} : f$, and $\mathfrak{m}$ is the only prime ideal containing $\mathfrak{q}$. As a result, $\mathfrak{m}' = \mathfrak{m}$. This shows that if $fg \in \mathfrak{q}$, and $f \notin \mathfrak{q}$, then $g \in \mathfrak{m}$ which implies $g^n \in \mathfrak{q}$. □

$\mathfrak{m}$-primary ideals play a very important part in the study of Artinian rings. Recall that you proved the following result:

Proposition 1. $\mathfrak{q}$ *is a primary ideal if and only if* $R/\mathfrak{q}$ *contains only zero divisors which are non-reduced.*

By the analysis of Proposition 28.5, we can conclude that such a ring $R/\mathfrak{q}$ where $\mathfrak{q}$ is $\mathfrak{m}$-primary, is also local with a unique prime ideal $\mathfrak{m}$. If R was also Noetherian, we conclude by the above discussion that $\mathfrak{m}^n = 0$ in this ring. This yields a big class of Artinian rings.

Next, we will get into a slightly different classification of primary ideals;

Theorem 28.6. *If* R *is Noetherian, then*

$$\mathfrak{q} \text{ is } \mathfrak{p}\text{-primary} \iff \mathrm{Ass}(R/\mathfrak{q}) = \{\mathfrak{p}\}$$

Example 28.7. If R and I are as in Example 28.4, then we have that I is not $\langle x\rangle$-primary. Indeed, one can note that $\mathrm{Ass}(R/I) = \{\langle x\rangle, \langle x, y\rangle\}$, since $\mathrm{Ann}(y) = \langle x\rangle$ and $\mathrm{Ann}(x) = \langle x, y\rangle$. Therefore, we can conclude in a different way that I is not $\langle x\rangle$-primary.

The Noetherian assumption is absolutely paramount here.

Example 28.8. Consider the ring $R = K[x_1, x_2, \ldots]$ and $I = \langle x_1^2, x_2^2, \ldots\rangle$. By virtue of Proposition 28.5, we have that I is $\mathfrak{m}$-primary. However, if we consider R/I, then $\mathfrak{m}$ is NOT the annihilator of any single element. Indeed, to be annihilated by every variable, you need to be divisible by every variable. This can never happen. Since $\mathrm{Ann}(x) \supseteq I$ for every $x \in R/I$, we actually have $\mathrm{Ass}(R/I) = \emptyset$!

Proof. $\Rightarrow$: Suppose $\sqrt{q} = \mathfrak{p}$ is a $\mathfrak{p}$-primary ideal. By Proposition 1, we know that the zero divisors of $R/\mathfrak{q}$ are those elements that are non-reduced: $x^n = 0$. As a result, we have $x \in \mathfrak{p}$ and $\mathfrak{p} \supseteq \mathrm{Ann}(x) \supseteq \mathfrak{q}$. But every associated prime is $\mathrm{Ann}(x)$ for some x, so the only possibility for a prime is $\mathfrak{p}$.

$\Leftarrow$: The main claim is as follows: if $\mathrm{Ass}(R/\mathfrak{q}) = \{\mathfrak{p}\}$, and M is a non-zero submodule of $R/\mathfrak{q}$, then $\sqrt{\mathrm{Ann}(M)} = \mathfrak{p}$. This follows since $\sqrt{\mathrm{Ann}(M)}$ is the intersection of all prime ideals containing $\mathrm{Ann}(M)$. But this can be realized as the intersection of all minimal primes containing $\mathrm{Ann}(M)$, which are the minimal elements of $\mathrm{Supp}(M)$. Therefore we can conclude by Theorem 27.1 that these minimal elements are in fact associated primes. But $\mathrm{Ass}(R/\mathfrak{q}) = \{\mathfrak{p}\}$, and therefore $\mathrm{Ass}(M) = \{\mathfrak{p}\}$. This proves the assertion.

As a result we have that $\mathfrak{q} = \mathrm{Ann}(R/\mathfrak{q})$ has radical $\mathfrak{p}$. Suppose $fg \in \mathfrak{q}$ and $f \notin \mathfrak{q}$. Consider $\bar{f} \in R/\mathfrak{q}$, we have $g \in \mathrm{Ann}(f) \subseteq \sqrt{\mathrm{Ann}(f)} = \mathfrak{p}$. So $g^n \in \mathfrak{q}$, which implies $\mathfrak{q}$ is $\mathfrak{p}$-primary. $\square$

Finally, we get to the most important reason to concern yourself with primary ideals; the primary decomposition.

Definition 28.9. If I is an ideal in a ring R, then I has a **primary decomposition** if

$$I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$$

where $\mathfrak{q}_i$ is a primary ideal. It is **shortest** if $\mathfrak{q}_i \not\subseteq \mathfrak{q}_1 \cap \cdots \cap \hat{\mathfrak{q}_i} \cap \cdots \cap \mathfrak{q}_n$ and $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$ has the property that $\mathfrak{p}_i \neq \mathfrak{p}_j$ for any $i \neq j$.

Given any primary decomposition, you can easily make it shortest by using the following lemma:

Lemma 28.10. *If* $\mathfrak{q}_1, \mathfrak{q}_2$ *are* $\mathfrak{p}$*-primary ideals, so is* $\mathfrak{q}_1 \cap \mathfrak{q}_2$.

As a result we can combine away all primary ideals with the same prime. In addition, this also implies no $\mathfrak{q}_i$ is redundant since we could simply omit it.

CLASS 29, APRIL 29TH: PRIMARY DECOMPOSITIONS EXIST!

Today we ask the question of when a primary decomposition exists for all ideals of a given ring. The first result in this direction is for Noetherian rings.

Theorem 29.1. *If R is a Noetherian ring, and $I \subsetneq R$ is a proper ideal, then I has a primary decomposition*

$$I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_m$$

To prove this result, we will use an idea similar to irreducibility but for ideals:

Definition 29.2. An ideal I is called **indecomposable** if there exists no strictly larger ideals J, K such that $I = J \cap K$.

Prime ideals are examples of indecomposable ideals, and the following shows a direct comparison with irreducible decompositions of varieties. The proof in fact has many similarities.

Lemma 29.3. *If R is a Noetherian ring, then every ideal is an intersection of a finite number of indecomposable ideals.*

Proof. Let $\mathcal{S}$ be the set of ideals that can't be written as a finite intersection of indecomposables. If $\mathcal{S} \neq \emptyset$, then $\mathcal{S}$ contains a maximal element I by the Noetherian property and Zorn's Lemma. Clearly I cannot be indecomposable, so $I = J \cap K$ for two larger ideals. But these each can be expressed as a finite intersection of indecomposables by maximality of I in $\mathcal{S}$. As a result, we contradict the fact that $I \in \mathcal{S}$. □

Lemma 29.4. *If R is a Noetherian ring, every indecomposable ideal is primary.*

Proof. Note that $\mathfrak{q} \subseteq R$ is indecomposable if and only if $0 \subseteq R/\mathfrak{q}$ is indecomposable (by the ideal correspondence). Therefore we reduce to the case $\mathfrak{q} = 0$. Suppose $xy = 0$, i.e. $y \in \mathrm{Ann}(x)$. We can consider the chain of ideals

$$\mathrm{Ann}(x) \subseteq \mathrm{Ann}(x^2) \subseteq \ldots \subseteq \mathrm{Ann}(x^n) = \mathrm{Ann}(x^{n+1}) = \ldots$$

I claim $\langle x^n \rangle \cap \langle y \rangle = 0$. Suppose $a \in \langle x^n \rangle \cap \langle y \rangle$. Then $ax = 0$ since $y|a$. This implies $ax = (bx^n) \cdot x = 0$. This is to say $b \in \mathrm{Ann}(x^{n+1}) = \mathrm{Ann}(x^n)$. This is only possible if $a = bx^n = 0$, proving the result.

Therefore, if 0 is indecomposable, we have that $xy = 0$ implies either $x^n = 0$ or $y = 0$, which demonstrates 0 is primary. □

This yields Theorem 29.1 immediately, because a decomposition into indecomposables is already an intersection of primary ideal! Now we move onto the question of uniqueness of a decomposition.

Theorem 29.5. *If R is Noetherian, and $I \subsetneq R$ is an ideal with shortest primary decomposition*

$$I = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_n$$

then $\mathrm{Ass}(R/I) = \{\sqrt{\mathfrak{q}_1}, \ldots, \sqrt{q_n}\}$.

Proof. Given $I = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_n$, we can use our standard inclusion

$$R/I \hookrightarrow \oplus_{i=1}^n R/\mathfrak{q}_i$$

As a result, $\text{Ass}(R/I) \subseteq \cup \text{Ass}(R/\mathfrak{q}_i) = \{\sqrt{\mathfrak{q}_1}, \ldots, \sqrt{\mathfrak{q}_n}\}$. Since we chose our decomposition to be shortest possible, we have that $M = \left(\cap_{i \neq j} \mathfrak{q}_i\right)/I \neq 0$. Therefore M has an associated prime. But $M \hookrightarrow R/\mathfrak{q}_j \subseteq \oplus_{i=1}^n R/\mathfrak{q}_i$, since all other factors map to 0. As a result, $\text{Ass}(M) \subseteq \text{Ass}(R/\mathfrak{q}_j) = \{\sqrt{\mathfrak{q}_j}\}$, which shows every ideal in the list is necessary. □

As a small note, this does NOT show that the choices of $\mathfrak{q}_i$ are uniquely determined in a shortest decomposition.

Example 29.6. Consider again our famous example of $I = \langle x^2, xy \rangle \subseteq K[x, y]$. We found that the associated primes of I are $\langle x \rangle$ and $\langle x, y \rangle$. Now, note that $I = \langle x^2, xy, y^n \rangle$ is $\langle x, y \rangle$-primary for any choice of n. Indeed, the radical is clearly $\langle x, y \rangle$. Furthermore, if we consider $K[x, y]/\langle x^2, xy, y^n \rangle$, then we should note that the zero divisors of this ring are any element of $\langle x, y \rangle$. Considering

$$f = ax + b_1 y + \ldots + b_{n-1} y^{n-1}$$

where $a, b \in K$, we see that $f^n = 0$. Indeed, every xy term is 0, $x^n = 0$, and $y^m = 0$ for $m \geq n$. This shows $\langle x^2, xy, y^n \rangle$ is primary. Finally,

$$\langle x^2, xy \rangle = \langle x \rangle \cap \langle x^2, xy, y^n \rangle \qquad \forall n \geq 1.$$

To finish up with primary decompositions, I would like to mention how they behave under localization. Note that if $\mathfrak{q}$ is a $\mathfrak{p}$-primary ideal, and $\mathfrak{p} \cap W = \emptyset$, then $\cdot W^{-1}\mathfrak{q}$ is a $\cdot W^{-1}\mathfrak{p}$-primary ideal in the localization, and even $\varphi^{\#}(\cdot W^{-1}\mathfrak{q}) = \mathfrak{q}$, where $\varphi : R \to W^{-1}R$ is the localization map.

Corollary 29.7. *If I is an ideal with shortest primary decomposition*

$$I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$$

and let $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$. Reorder $\mathfrak{q}_i$ so that $\mathfrak{p}_i \cap W = \emptyset$ for $i \leq m$ and $\mathfrak{p}_i \cap W \neq \emptyset$ for $i > m$. Then

$$W^{-1}I = W^{-1}\mathfrak{q}_1 \cap \cdots \cap W^{-1}\mathfrak{q}_m$$
$$\varphi^{-1}(W^{-1}I) = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_m$$

In particular, one should note that this yields an example of extension and contraction not being inverse to one another:

$$I \subseteq \varphi^{-1}(W^{-1}I)$$

Proof. Recall that localization and intersections commute (can be interchanged). Therefore we get

$$W^{-1}I = W^{-1}\mathfrak{q}_1 \cap \cdots \cap W^{-1}\mathfrak{q}_m \cap W^{-1}\mathfrak{q}_{m+1} \cap \cdots \cap W^{-1}\mathfrak{q}_n$$

but $W \cap \mathfrak{q}_i \neq \emptyset$ implies $W^{-1}\mathfrak{q}_i = W^{-1}R$. This completes the proof. □

Corollary 29.8. *If I is as in Corollary 29.7, and $\mathfrak{p}_i$ is minimal among $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$, then localizing at $W = R \setminus \mathfrak{p}_i$ yields*

$$\mathfrak{q}_i = \varphi^{-1}(W^{-1}I)$$

Therefore, such a $\mathfrak{q}_i$ primary to a minimal prime is unique!

Corollary 29.8 demonstrates that $\langle x \rangle$ cannot be modified in Example 29.6.

CLASS 30, MAY 1ST: DISCRETE VALUATIONS

We will now move into the final chapter of Reid, which talks about valuation rings and normal domains. These are important classes of rings in commutative algebra, algebraic geometry, and number theory.

We have seen many examples of discrete valuation rings previously. I now recall some of them to motivate the definition that will follow.

Example 30.1 (Localizations of PIDs)**.** The rings $\mathbb{Z}_{\langle p \rangle}$ and $K[x]_{\langle x \rangle}$ are both local domains. A further thing to note is the following: the maximal ideal is principal, generated by $t = p$ in the first case and $t = x$ in the latter. This gives us a very interesting interpretation for what elements of these rings look like; $f = u \cdot t^n$ for some $n \geq 0$ and u a unit.

Example 30.2 (Power Series in 1 Variable)**.** The same story applies to $K[\![x]\!]$, or the subring of convergent power series. We showed in Homework 3, #4, that every element of a power series ring in any number of variables is a unit if and only if it has non-zero constant coefficient. Here this means that every element can be expressed as $f = u \cdot x^n$ for some n and u a unit.

The enjoyment of rings with such properties brings us to the following definition;

Definition 30.3. Let K be a field. A **discrete valuation** is a surjective map $v : K^\times \to \mathbb{Z}$ such that the following properties hold $\forall x, y \in K$:

(a) $v(x \cdot y) = v(x) + v(y)$.
(b) $v(x \pm y) \geq \min\{v(x), v(y)\}$.

As a convention, we let $v(0) = \infty$ to extend the valuation to all of K, and to further ensure that the above properties are satisfied.

Example 30.4. Consider the field $L = K((x))$ of formal Laurent series with coefficients in K. It's elements look like

$$f = \sum_{i=m}^{\infty} a_i x^i$$

where $m \in \mathbb{Z}$. L is a field. This allows us to consider the valuation

$$v : L \to \mathbb{Z} : f \mapsto \inf\{m \mid a_m \neq 0\}$$

This is a valuation; the smallest non-zero coefficient of a product $f \cdot g$ is $a_m b_n x^{m+n}$, where $f = \sum_{i=m}^{\infty} a_i x^i$ and $g = \sum_{i=n}^{\infty} b_i x^i$. For addition, the smallest coefficient of $f + g$ is either a_m, b_n, or $a_m + b_m$ if $m = n$ and $a_m \neq b_m$ (otherwise it is larger degree than m).

Definition 30.5. The **valuation ring** associated to a valuation $v : K^\times \to \mathbb{Z}$ is

$$R = R_v = \{a \in K \mid v(a) \geq 0\}$$

Proposition 30.6. *R_v is a local ring with maximal ideal*

$$\mathfrak{m}_v = \{a \in K \mid v(a) > 0\}$$

Proof. First note that R is a ring. $0 \in R$ by our convention, and $1 \in R$ since

$$v(1) = v(1 \cdot 1) = v(1) + v(1) \qquad \Longrightarrow \qquad v(1) = 0$$

It is also closed under addition and multiplication by the axioms for a valuation, and distribute since it is a subset of a field.

Finally, it goes to show $\mathfrak{m}_v$ is the unique maximal ideal. Every unit in R_v is a unit in K (duh!). But we have that

$$v(x) + v(x)^{-1} = v(x \cdot x^{-1}) = v(1) = 0$$

which is to say that $v(x^{-1}) = -v(x)$. So $x, x^{-1} \in R_v$ if and only if $v(x) = 0$. This shows everything outside of $\mathfrak{m}_v$ in R_v is a unit. □

Example 30.7. Continuing with Example 30.4, we see that $R_v = K[\![x]\!]$ and $\mathfrak{m}_v = \langle x \rangle$. This is the unique maximal ideal of R_v by the previous discussion.

Example 30.8. We can consider

$$v : \mathbb{Q}^\times \to \mathbb{Z} : \frac{a}{b} = p^m \frac{a'}{b'} \mapsto m \qquad \text{where } p \nmid a', b'$$

This is also a valuation, typically called the p-adic valuation on $\mathbb{Q}$. One can verify that $R_v = \mathbb{Z}_{\langle p \rangle}$ and $\mathfrak{m}_v = \langle p \rangle$. One can also extend v to $\mathbb{Q}_p$, the p-adic rationals, to yield R_v the p-adic integers and $\mathfrak{m}_v = \langle p \rangle$.

Proposition 30.9. *For a discrete valuation $v : K^\times \to \mathbb{Z}$, $\mathfrak{m}_v = \langle t \rangle$ is a principal ideal. In fact every non-zero ideal is of the form $I = \langle t^n \rangle$ for some $n \in \mathbb{N}$. In particular, DVRs are Noetherian.*

Proof. Pick any element $t \in R_v$ such that $v(t) = 1$. If $s \in \mathfrak{m}_v$ is another, then in $K^\times$ we have that there exists u such that $t = us$. But then

$$1 = v(t) = v(us) = v(u) + v(s) \leq v(u) + 1$$

which is to say that $v(u) \geq 0$, i.e. $u \in R_v$. Therefore $s \in \langle t \rangle$.

The statement for I is identical, taking t^n to be your element with valuation n the smallest among elements of I. □

This is actually very strong. It says that the proper ideals of R_v are in bijection with positive integers $n \in \mathbb{N}$.

Definition 30.10. t as in Proposition 30.9 is called a (sometimes **uniformizing**)**parameter** for v.

As we can see, there are some natural choices of a uniformizing parameter in the above examples, such as p and x. However, such a choice is clearly non-unique, as we can multiply it by any unit that exists within our ring (not the field).

Next time, we will study some equivalent formulations of being a DVR. For the interested student, I encourage you to check out the opening of the wiki page:

`https://en.wikipedia.org/wiki/Discrete_valuation_ring`

CLASS 31, MAY 3RD: EQUIVALENT CONDITIONS FOR DVRS

Today we will approach DVRs from a different angle (or two). This gives some equivalent characterizations and produces an easy way to see when a ring is a DVR. I will first note a specific case of the much broader Krull Intersection Theorem.

Lemma 31.1. *If R is a Noetherian integral domain, and $0 \neq t \in R$ is a non-unit, then $\cap_{n=1}^{\infty}\langle t^n\rangle = 0$.*

Proof. Note that

$$\langle t\rangle \supsetneq \langle t^2\rangle \supsetneq \cdots \supsetneq \langle t^n\rangle \supsetneq \langle t^{n+1}\rangle \supsetneq \cdots$$

Each inclusion is strict: If $t^{n+1}g = t^n$. This implies that $t^n(tg-1) = 0$. Therefore, $tg-1 = 0$, since $t \neq 0$ in a domain. But t is not a unit! So no such g exists.

Suppose $x \in \langle t\rangle$. Then $x = tx_1$. Continue in this process with x_1 to produce

$$\langle x\rangle \subseteq \langle x_1\rangle \subseteq \langle x_2\rangle \subseteq \ldots \subseteq \langle x_n\rangle$$

This process must stop by the Noetherian property. But this means $x_n \notin \langle t\rangle$, which is to say $x \notin \langle t^{n+1}\rangle$. □

Theorem 31.2. *Let R be a local domain with $\mathfrak{m} = \langle t\rangle$, $t \neq 0$. Assume $\bigcap_{i=1}^{\infty}\langle t^n\rangle = 0$. Then*

(a) *Every $0 \neq x \in R$ has the form $x = ut^n$ for u a unit and some n.*
(b) *Define $v(x) = n$, with x as in (a). For $\frac{a}{b} \in \mathrm{Frac}(R)$, define $v(\frac{a}{b}) = v(a) - v(b)$. Then v is a discrete valuation on $\mathrm{Frac}(R)$.*
(c) *Every non-zero ideal $I = \langle t^n\rangle$ for some n.*

Proof. (a) Since $\mathfrak{m} = \langle t\rangle$ is maximal, everything indivisble by t is a unit. Thus x is either a unit ($x = u$) or $x = tx_1$. Continuing inductively with x_1 to produce $x = t^n x_n$ whenever possible. Since $\bigcap_{i=1}^{\infty}\langle t^n\rangle = 0$, we have that at some point x_n is not divisible by t, and is thus a unit. Therefore, $x = u \cdot t^n$, with $u = x_n$.

(b) v is well defined by the previous step. $v(xx') = v(ut^n u' t^{n'}) = v(uu' t^{n+n'}) = n + n'$. Similarly, WLOG assuming $n \geq n'$

$$v(x + x') = v(ut^n + u't^{n'}) = v(t^{n'}(ut^{n-n'} + u'))) = n' + v(ut^{n-n'} + u') \geq n' = \min\{n, n'\}$$

(c) Choose $n = \min\{n' \mid x = ut^{n'} \in I\}$. Then clearly $I = \langle x^n\rangle$.

□

This shows that ALL Noetherian local integral domains with principal maximal ideal are DVRs. In fact, even non-Noetherian rings with the above description satisfy many of the desirable properties of a DVR.

Now I move to the so-called *Main Theorem on DVRs*. It says that DVRs are exactly Noetherian normal domains with exactly 2 pointed spectra.

Theorem 31.3. *The following sets are in natural bijection:*

$$\{R \text{ a DVR}\} \longleftrightarrow \{R \text{ a Noetherian normal ring with } \mathrm{Spec}(R) = \{0, \mathfrak{m}\}\}$$

This can be said concisely by DVRs are precisely 1-dimension local normal domains. We will use this slight abstraction of what a DVR to great effect later on, when we consider localizations of normal domains. This will reduce many local questions in Commutative Algebra, Number Theory, and Algebraic geometry to rather simple questions regarding DVRs.

Proof. ($\Longrightarrow$): Since every ideal of a DVR R has the form $I = \langle t^n \rangle$, it is clearly finitely generated. Thus R is Noetherian. It is a domain, since it is a subring of a field (domain). Lastly, $\mathfrak{m} = \langle t \rangle$ is the only non-zero prime ideal, thus it is maximal.

To check that R is normal, we use the fact that R is a PID, thus a UFD. All UFD are themselves normal (c.f. Exam 1).

($\Longleftarrow$): Choose $x \in \mathfrak{m} \setminus \mathfrak{m}^2$. Note that this is possible because of Nakayma's Lemma! I claim that $\mathfrak{m} = \langle x \rangle$. Consider the R-module $M = \mathfrak{m}/\langle x \rangle$. If $M \neq 0$, then M has an associated prime $\mathfrak{p} = \mathrm{Ann}(y)$! Note that since $\langle x \rangle \subseteq \mathfrak{p}$, we have that $\mathfrak{p} = \mathfrak{m}$. Therefore, there exists $y \in \mathfrak{m} \setminus \langle x \rangle$ such that $y \cdot \mathfrak{m} \subseteq \langle x \rangle$.

We now move to $K = \mathrm{Frac}(R)$. Then $\frac{y}{x} \in K$, but $\frac{y}{x} \notin R$ since $y \notin \langle x \rangle$. However, $\frac{y}{x}\mathfrak{m} \subseteq R$, and is an ideal of R.

Case 1: $\frac{y}{x}\mathfrak{m} = R$. This implies the existence of $y' \in \mathfrak{m}$ such that $\frac{yy'}{x} = 1$, or equivalently $x = yy'$. But $y, y' \in \mathfrak{m}$ imply that $yy' = x \in \mathfrak{m}^2$, contradicting our choice of x.

Case 2: $\frac{y}{x}\mathfrak{m} \subseteq \mathfrak{m}$. In this case, I claim that $\frac{y}{x}$ is integral over R. Indeed, we can view $\varphi : \mathfrak{m} \to \mathfrak{m} : m \mapsto \frac{y}{x}m$ as an endomorphism of finitely generated (Noetherian!) R-modules. Therefore, the determinant trick implies that φ satisfies a monic polynomial relation $\varphi^n + r_1\varphi^{n-1} + \ldots + r_n = 0$ with $r_i \in R$. Applying this relation to $r \neq 0$ in $\mathfrak{m}$ yields the desired result since R is a domain.

Finally, since we assumed R was normal, we have that $\frac{y}{x} \in R$, which implies $y \in \langle x \rangle$. This is a contradiction to our choice of y.

Therefore $\mathfrak{m} = \langle x \rangle$, which implies by Lemma 31.1 and Theorem 31.2 that R is a DVR. □

Example 31.4. We have shown that $K[x,y]/\langle y^2 - x^3 \rangle$ and $K[x,y]/\langle y^2 - x^3 - x^2 \rangle$ are non-normal, even upon localization at $\langle x, y \rangle$. In each case it can be shown that $\frac{y}{x}$ is integral over these rings. Therefore, they are non-normal and thus immediately not DVRs.

Example 31.5. The ring $R = K[x,y]/\langle y^2 - x^3 - x \rangle$ is normal (for a field K not of characteristic 2). As a result, we have that for any (a,b) satisfying $b^2 - a^3 - a$ in K, the ring $R_{\langle x-a, y-b \rangle}$ is a DVR. $\mathrm{Spec}(R)$ is an example of an elliptic curve (missing one 'projective' point at infinity).

Next time, we will discuss what to do if our valuation is not discrete, i.e. doesn't take values in $\mathbb{Z}$. This will lead us to a similar notion to discrete valuation rings, but will allow us to consider rings such as germs of functions on an algebraic variety:

$$K[x,y]_{\mathfrak{m}}/\sqrt{J}$$

CLASS 32, MAY 6TH: VALUATION RINGS

Today we drop the assumption that our value group is discrete, i.e. $\mathbb{Z}$. This allows us to upgrade our list of rings that have several *valuable* properties.

Definition 32.1. Let R be an integral domain with fraction field $L = \mathrm{Frac}(R)$. Then R is said to be a **valuation ring** if for every $0 \neq x \in L$, we have either $x \in R$ or $x^{-1}R$.

This may seem out of the blue compared with our old definition. However, we will give a more favorable definition later on.

Example 32.2. Lets return again to our perfect ring

$$R = \mathbb{F}_p[x]_{perf} = \mathbb{F}_p[x^{\frac{1}{p^\infty}}] = \mathbb{F}_p[x, x^{\frac{1}{p}}, x^{\frac{1}{p^2}}, \ldots]$$

This is an integral domain with fraction field

$$K = \mathbb{F}_p(x^{\frac{1}{p^\infty}}) = \mathbb{F}_p(x, x^{\frac{1}{p}}, x^{\frac{1}{p^2}}, \ldots)$$

R is not a valuation ring, as neither $\frac{x-1}{x-2}$ nor $\frac{x-2}{x-1}$ are in R. We can localize R at $\mathfrak{m} = \langle x, x^{\frac{1}{p}}, x^{\frac{1}{p^2}}, \ldots \rangle$ to fix this problem. Now, given a non-zero fraction $\frac{f}{g}$, we can extract all copies of x:

$$\frac{f}{g} = x^i \frac{f'}{g'}$$

where $f', g' \notin \mathfrak{m}$. Noting that $\frac{f}{g} \in R$ if and only if $i \geq 0$, we immediately yield that either $\frac{f}{g} \in R$ or $\frac{g}{f} \in R$. It should be noted however that i is taking values in $\mathbb{Z}[\frac{1}{p}]$, and in particular is NOT a DVR.

To get to a nice equivalent formulation, I define a total ordering:

Definition 32.3. A set Λ together with a transitive binary operation $<$ with the property that exactly one of $x < y$, $x = y$, or $x > y$ is true is called a **totally ordered set**.

If G is an Abelian group, we call it an **ordered group** if it is totally ordered compatibly with addition: $a \geq b$ and $a' > b'$, then $a + a' > b + b'$.

Given R a domain, we can form $G = K^\times / R^\times$. Note that this is well defined since $R^\times$ is (an automatically normal) subgroup of $K^\times$. It is typical to write G additively, even though the operation is multiplication: $[a \cdot b] = [a] + [b]$.

We can endow G with the **partial order** defined by $[\alpha] > 0$ if and only if $\alpha \in R$. This yields $[\alpha] \geq [\beta]$ if and only if $\frac{\alpha}{\beta} \in R$.

This method brings us to the following equivalent characterization of valuation rings:

Proposition 32.4. *R is a valuation ring if and only if $>$ is a total order on G. In this case, the quotient map $v : K^\times \to G = K^\times / R^\times$ satisfies the following properties:*

(a) $v(xy) = v(x) + v(y)$
(b) $v(x \pm y) \geq \min\{v(x), v(y)\}$

Moreover, if G is any ordered group, and $v : K^\times \to G$ is a surjective map satisfying properties (a) & (b), then the subset

$$R = \{\alpha \in K \mid v(\alpha) \geq 0\} \cup \{0\}$$

is a valuation ring, and $G = K^\times/R^\times$.

Definition 32.5. In the setup of Proposition 32.4, v is called a **valuation** and G is called the **value group** of v.

Example 32.6. In our previous example, Example 32.2, one can verify that

$$v : K^\times \to K^\times/R_{\mathfrak{m}}^\times \cong \mathbb{Z}[\frac{1}{p}] : \frac{f}{g} = x^i \frac{f'}{g'} \mapsto i$$

is a valuation. The stated isomorphism is essentially the given one, since $\frac{f'}{g'} \mapsto 0$ and is exactly representative of the kernel.

Proof. R is a valuation ring if and only if $0 \neq \frac{a}{b} \in K$ implies $\frac{a}{b} \in R$ but not $\frac{b}{a}$, or $\frac{b}{a} \in R$ but not $\frac{a}{b}$, or $\frac{a}{b} \in R^\times$. These are exactly the conditions $v(a) > v(b)$, $v(b) > v(a)$, or $v(b) = v(a)$.

Given R a valuation ring, property (a) is direct from the fact that v is a homomorphism of groups, with multiplication in $K^\times$ and 'addition' in G.

(b) follows, since if $v(x) \geq v(y)$, then $v(xy^{-1}) \geq 0$, implying $xy^{-1} \in R$. Thus

$$v(y^{-1}(x+y)) = v(xy^{-1}+1) \geq 0$$

or equivalently $v(x+y) \geq v(y)$.

The final sentence (Moreover, ...) is left for the eager reader. □

A cool aftereffect of Proposition 32.4 is the following: If you can come up with a surjective group homomorphism $v : K^\times \to G$, where G is an ordered group, then you have produced a valuation ring.

Definition 32.7. Consider the group $G = \mathbb{Z}^2$ with the lexicographical/dictionary order; $(a,b) > (a',b')$ if and only if $a > a'$ or $a = a'$ and $b > b'$. This yields a natural map

$$v : K(x,y)^\times \to \mathbb{Z}^2 : \frac{f}{g} = x^i y^j \frac{f'}{g'} \mapsto (i,j)$$

where we use the standard that $f', g' \notin \langle x, y\rangle$ to make the map well-defined. Doing this, we can verify that the associated valuation ring is

$$R = K[x,y]_{\langle x,y\rangle}\left[\frac{x}{y}, \frac{x}{y^2}, \frac{x}{y^3}, \ldots\right]$$

and in particular contains $\frac{x^i}{y^j}$ with $i > 0$ and any $j \in \mathbb{Z}$.

This assists with the next realization:

Theorem 32.8. *If R is a valuation ring, then R is Noetherian if and only if R is a DVR.*

Proof. We know DVRs are Noetherian, so it only suffices to check $\Rightarrow$. Assume R is Noetherian. Then all ideals I are finitely generated. If $I = \langle x_1, \ldots, x_n\rangle$, then I claim I is in fact principal! Let x_1 WLOG be the generator with smallest valuation. Then we have $\frac{x_i}{x_1} \in R$ for all i, since

$$v(\frac{x_i}{x_1}) = v(x_i) - v(x_1) \geq 0$$

As a result, $x_1 \frac{x_i}{x_1} = x_i \in \langle x_1\rangle$, meaning every other generator is redundant. □

CLASS 33, MAY 8TH: NORMAL IN CODIMENSION 1

Today we will study what normal tells you about the singular locus of a given algebraic variety. This is one of the essential results that make normal rings/varieties a nice class of objects to study. First, one last example of a valuation ring in general.

Example 33.1. If R is a DVR with parameter t, we can construct a new valuation ring by adjoining all the roots of t. Let $A = R[t^{\frac{1}{2}}, t^{\frac{1}{3}}, \ldots]_{\mathfrak{m}}$. It is easy to check that

$$L = \mathrm{Frac}(A) = \mathrm{Frac}(R)(t^{\frac{1}{2}}, t^{\frac{1}{3}}, \ldots)$$

Therefore, we can define a valuation $v : L \to \mathbb{Q} : t^\alpha \mapsto \alpha$, which extends the valuation for R. Then A is exactly the set of elements for which $v(a) \geq 0$.

We can do a similar thing with $\mathbb{R}$ to produce a valuation ring with value group $\mathbb{R}$.

Now we turn to the condition of being normal. Recall the definition:

Definition 33.2. An integral domain R is **normal** if R is integrally closed in $K = \mathrm{Frac}(R)$.

First, we will start with a local characterization:

Lemma 33.3. *If R is an integral domain, then $R_{\mathfrak{p}} \subseteq K$ for all $\mathfrak{p} \in \mathrm{Spec}(R)$. Furthermore,*

$$R = \bigcap_{\mathfrak{p} \in \mathrm{Spec}(R)} R_{\mathfrak{p}} = \bigcap_{\mathfrak{m} \in m\text{-}\mathrm{Spec}(R)} R_{\mathfrak{m}}$$

Note these intersections are all happening in K by the first part.

Proof. For $x \in K$, define the **ideal of denominators** of x to be

$$D(x) = \{r \in R \mid rx \in R\} = \{0\} \cup \{s \in R \mid x = \frac{r}{s} \text{ for some } r \in R\}$$

This is an ideal. For $x \in K$, we have $x \in R$ iff $D(x) \neq R$. If $D(x)$ is proper, it is contained within some maximal ideal $\mathfrak{m}$, and therefore $x \notin R_{\mathfrak{m}}$. $x \notin \bigcap_{\mathfrak{m} \in m\text{-}\mathrm{Spec}(R)} R_{\mathfrak{m}}$ as desired. □

Now we can prove that being normal is a local condition, much like being 0 as a module.

Proposition 33.4. *TFAE:*

(a) *R is normal*
(b) *$R_{\mathfrak{p}}$ is normal for all $\mathfrak{p} \in \mathrm{Spec}(R)$.*
(c) *$R_{\mathfrak{m}}$ is normal for all $\mathfrak{m} \in m\text{-}\mathrm{Spec}(R)$.*

Proof. For (a)⇒(c)⇒(b), I prove instead that $W^{-1}R$ is normal if R is normal for any multiplicative set W. If $\alpha \in K$ satisfies some monic polynomial with coefficients in $W^{-1}R$, then

$$\alpha^n + \frac{a_1}{b_1}\alpha^{n-1} + \ldots + \frac{a_n}{b_n} = 0$$

Therefore, we can multiply the whole equation by $(b_1 \cdots b_n)^n$ to produce a non-monic relation in R:

$$(b_1 \cdots b_n\alpha)^n + a_1 b_2 \cdots b_n (b_1 \cdots b_n\alpha)^{n-1} + \ldots + b_{n-1}^{-1}(b_1 \cdots b_{n-1})^n a_n = 0$$

Therefore, since R is normal, we note $b_1 \cdots b_n\alpha \in R$. As a result, we can conclude that $\alpha \in S^{-1}R$, as desired.

Since (b)⇒(c) is a triviality, it suffices to check (c) implies (a). If x is integral over R, then x is clearly integral over $R_{\mathfrak{m}}$ for each $\mathfrak{m}$. As a result, $x \in R_{\mathfrak{m}}$ by normality. But then $x \in \cap_{\mathfrak{m}} R_{\mathfrak{m}} = R$ by Lemma 33.3. □

This brings us to the central theorem about Normal domains:

Theorem 33.5. *Let R be a normal Noetherian domain. If $\mathfrak{p} \neq 0$ is minimal among non-zero primes, then $R_{\mathfrak{p}}$ is a DVR. Furthermore, if $I \neq 0$ is principal, $\mathfrak{p} \in Ass(R/I)$ are among the minimal non-zero prime ideals of R.*

Proof. By Lemma 33.3, $R_{\mathfrak{p}}$ is a normal Noetherian domain. Moreover, $\mathrm{Spec}(R_{\mathfrak{p}})$ contains only $\mathfrak{p}$ and 0 by assumption of minimality of $\mathfrak{p}$. Therefore, by Theorem 31.3, we have $R_{\mathfrak{p}}$ is a DVR.

For the second statement, we first reduce to the local case. Given $\mathfrak{p} \in \mathrm{Ass}(R/I)$, consider the local ring $(R_{\mathfrak{p}}, \mathfrak{p}R_{\mathfrak{p}})$. Let $I' = xR_{\mathfrak{p}}$ be the extension of I. Since $R_{\mathfrak{p}}/I' = (R/I)_{\mathfrak{p}}$, we have by Corollary 29.7 that $\mathfrak{p}R_{\mathfrak{p}} \in \mathrm{Ass}(R_{\mathfrak{p}}/I')$. If we can show $\mathfrak{p}R_{\mathfrak{p}}$ is a minimal non-zero prime ideal of $R_{\mathfrak{p}}$, then $\mathfrak{p}$ is minimal non-zero in R by our relationships of ideals through localization.

Let $\mathfrak{m} = \mathfrak{p}R_{\mathfrak{p}}$. Since $\mathfrak{m} \in \mathrm{Ass}(R_{\mathfrak{p}}/I')$, there exists $y \notin I'$ such that $y \cdot \mathfrak{m} \subseteq I'$. As a result, there exists $x \in I'$ such that $\frac{y}{x} \in \mathrm{Frac}(R)$ satisfies $\frac{y}{x} \cdot \mathfrak{m} \subseteq R_{\mathfrak{p}}$. Therefore, we can mirror the proof of Theorem 31.3:

Case 1: $\frac{y}{x}\mathfrak{m} \subseteq \mathfrak{m}$. In this case, $\frac{y}{x}$ is integral over $R_{\mathfrak{p}}$. But $R_{\mathfrak{p}}$ is normal, so $\frac{y}{x} \in R_{\mathfrak{p}}$. But this would contradict that $y \notin I'$.

Case 2: $\frac{y}{x}\mathfrak{m} = R_{\mathfrak{p}}$. This implies the existence of $y' \in \mathfrak{m}$ such that $\frac{yy'}{x} = 1$, or equivalently $x = yy'$. But then we would have for all $z \in \mathfrak{m}$, $z\frac{y}{x} = \frac{z}{y'} \in R_{\mathfrak{p}}$, or $z \in \langle y' \rangle$.

In this case, we know $\mathfrak{m} = \langle y' \rangle$. As a result, $R_{\mathfrak{p}}$ is a DVR and $\mathfrak{m}$ is a minimal non-zero prime ideal. □

Geometrically, what we have just ascertained is that the singular points of a normal variety must exist in codimension ≥ 2. This is a major result, as it gives us the following information:

(a) Normal curves are non-singular.
(b) Normal surfaces have isolated point singularities.
(c) Normal 3-folds have at worst singularities lying on a curve.
(d) Normal n-folds have at worst singularities lying on a $(n-2)$-fold.

Example 33.6. We have already shown that the cusp $R = K[x,y]/\langle y^2 - x^3 \rangle$ is non-normal; $\tilde{R}$ contains $\frac{y}{x}$ as a root of $t^2 - x$.

Additionally, on the Midterm it was demonstrated that $R = K[x,y]/\langle y^2 - x^3 - x \rangle$ is non-normal for the same reason. These 2 facts are special cases of (a) in this classification.

The Whitney umbrella is an example of a surface with a singular curve $C = V(x,y)$ (or worse if $char(K) = 2$); $R = K[x,y,z]/\langle x^2 z - y^2 \rangle$. Thus we immediately know R cannot be normal. This is further verified by noting

$$\left(\frac{y}{x}\right)^2 = \frac{x^2 z}{x^2} = z \qquad \text{or} \qquad \left(\frac{xz}{y}\right)^2 = \frac{y^2 z}{y^2} = z$$

This condition of being regular in codimension 1 is insufficient to verify normalcy. You also need a condition known as S_2, Serre's second condition. This is beyond our scope!

CLASS 34, MAY 10TH: NORMALS ARE INTERSECTIONS OF DVRS

For the final day, I want to give an example of a non-normal surface with isolated singularities, and then prove all normal Noetherian domains are intersections of DVRs.

Example 34.1. Consider the subring of $K[x, y]$ defined by

$$R = \{f \in K[x, y] \mid f(0, 0) = f(0, 1)\}$$

This can be thought of as taking the affine plane $\mathbb{A}^2_K$ and gluing 2 points together. Note that if we take $\text{Frac}(R)$, it is equal to $\text{Frac}(K[x, y]) = K(x, y)$; note that $x, xy \in R$. As a result, we have $\frac{xy}{x} = y \in \text{Frac}(R)$.

Now, I claim that $y \in \tilde{R}$, meaning $\tilde{R} = K[x, y] \neq R$, implying R is not normal. y satisfies

$$t^2 - t + y(y - 1) = 0$$

Notice that $y(y - 1) \in R$!

R is an example of a non-Normal domain with localizations at minimal non-zero primes DVRs. Therefore it lacks the S_2-condition mentioned last class.

To conclude the course, we prove the following theorem:

Theorem 34.2. *If R is a normal Noetherian integral domain, then*

$$R = \bigcap_{0 \neq \mathfrak{p} \text{ minimal}} R_{\mathfrak{p}}$$

In particular, R is an intersection of DVRs.

Proof. We already know that

$$R = \bigcap_{\mathfrak{p} \in Spec(R)} R_{\mathfrak{p}} \subseteq \bigcap_{0 \neq \mathfrak{p} \text{ minimal}} R_{\mathfrak{p}}$$

So it suffices to check $\supseteq$. Let $x = \frac{r}{s} \in K = \text{Frac}(R)$. Again, let

$$D(x) = \{d \in R \mid dx \in R\}$$

We can note that $D(x) = \{d \in R \mid dr \in \langle s \rangle\} = \langle s \rangle : r = \text{Ann}(\bar{r})$, where we view $\bar{r} \in A/\langle s \rangle$. Suppose $x \notin R$, which is to say $\bar{r} \neq 0$.

I claim $D(x) \subseteq \mathfrak{p} \in \text{Ass}(R/\langle s \rangle)$. $D(x) = \text{Ann}(\bar{r})$, so since R is Noetherian we have $D(x)$ is contained in some maximal element of this form, which is thus associated. By Theorem 33.5, we have any $\mathfrak{p} \in \text{Ass}(R/\langle s \rangle)$ is a minimal non-zero prime. Therefore, $x \notin R_{\mathfrak{p}}$. This completes the proof of $\supseteq$. □