CLASS 1, MONDAY FEBRUARY 5TH: RINGS!

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 0.1. 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**.
- R is said to be a **division ring** if it is unital, $1 \neq 0$, and every element $r \in R$ has a multiplicative inverse: $\frac{1}{r}$ or r^{-1}. Note that we don't need to worry about the side in which we multiply (left/right inverses)!

Most of the time later in this course we will focus on commutative, unital, rings R.

Example 0.2.

- 0: The ring with 1 element 0 is a ring! It is unital ($1 = 0$), but is not division.
- K: A field is a commutative, unital, division ring! 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
- $M_n(K)$: $n \times n$ matrices with coefficients in a field K are a non-commutative unital ring. It is not a division ring, as something not of full rank can not be inverted. However...
- $GL_n(K)$: The **General Linear Group** of full rank $n \times n$ matrices is a subring of $M_n(K)$, which IS a unital division ring!

- $C_i(\mathbb{R})$: 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.

Proof. Exercise done in class. For the first consequence, note that

$$0 \cdot r = (0 + 0) \cdot r = 0 \cdot r + 0 \cdot r$$

so $0 \cdot r = 0$ by subtraction of the left from the right hand side. □

Some ring elements have specific properties. I now list a few of them:

Definition 0.3. 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**.

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 element is a unit. There are many nice properties of non-zero-divisors:

Proposition 0.4. *If a is a non-zero divisor, and $b, c \in R$ are such that $ab = ac$, then $b = c$.*

This was shown using distributivity. Next time we will pick up with this result:

Corollary 0.5. *Any finite integral domain R is a field.*

CLASS 2, WEDNESDAY FEBRUARY 7TH: HOMOMORPHISMS & IDEALS

Recall we left off with the following result:

Corollary 0.1. *Any finite integral domain R is a field.*

We can show existence of inverses using the previous result. The fact that R is commutative is a result of Wedderburn to be shown later.

As with every realm of math, the objects of study are very important, but often times the maps are more important even themselves encoding the information of the ring itself! This brings about the notion of a homomorphism:

Definition 0.2. 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:

$$\text{For any } r, r' \in R,\ \varphi(r + r') = \varphi(r) + \varphi(r') \text{ and } \varphi(rr') = \varphi(r)\varphi(r').$$

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.

Definition 0.3. The **kernel** of φ, denoted $\ker(\varphi)$ is the set

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

The **image** of φ, denoted $\mathrm{im}(\varphi)$, is the set

$$\mathrm{im}(\varphi) = \{s \in S \mid \exists r \in R \ s.t.\ \varphi(r) = s\} \subseteq S$$

Both are subrings of their respective rings (**proof?**). In the case where $\ker(\varphi) = 0$ and $\mathrm{im}(\varphi) = S$, we say that φ is an **isomorphism**.

As a quick exercise, check that an isomorphism has a ring homomorphism $\psi : S \to R$ which is an inverse to φ.

Example 0.4.
- What is $\mathrm{Hom}(\mathbb{Z}, \mathbb{Z})$?
- What about $\mathrm{Hom}(\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$?
- Consider $\varphi_\alpha : \mathbb{Q}[x] \to \mathbb{Q}$ defined by sending x to $\alpha \in \mathbb{Q}$.

Proposition 0.5. *Any homomorphism $\varphi : R \to S$ can be factored into a surjection $R \to R'$, followed by an injection $R' \to S$.*

This requires us to introduce the notion of **fibers**: Since $\varphi : R \to S$ is in particular a morphism of abelian groups (under addition), we can realize the kernel of this morphism as an abelian group I. We can thus form a ring of cosets

$$R/I = \{r + I \ : \ r \in R\}$$

This is most often called the **quotient ring** of R by I, and it has well defined $+$ and $\cdot$ inhereted from R itself.

The fibers of φ are $r+I$ for a choice of r, as you want to think of them as the preimage of some element of S.

$R' = R/I$ is the desired ring. One can check the existence of homomorphisms as in Proposition 0.5.

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

Definition 0.6. A subset $I \subseteq R$ is called a **left 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 $r \cdot i \in I$.

I is called a **right ideal** if the same is true, but for $\alpha \cdot r$. Finally, if I is both a left and right ideal, then I is called a **2-sided ideal**, or simply an **ideal**.

When we eventually specialize our attention to commutative rings, we will only say ideal as all of the above notions coincide.

Example 0.7.
- $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$.
- $xK[x]$ is an ideal of $K[x]$.
- 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.

Proposition 0.8. *Let R be a ring and I a (2-sided) ideal. Then R/I as defined above exists and is well defined. In fact, any subring I with this property is necessarily an ideal!*

Proof. R/I clearly makes sense with respect to addition. For multiplication, note that

$$(r + I) \cdot (s + I) = r \cdot s + r \cdot I + I \cdot s + I \cdot I = r \cdot s + I$$

since $r \cdot I, I \cdot s, I \cdot I \subseteq I$.

Now suppose I is an additive subgroup. Then

$$\begin{aligned} r + I = (r + I)(1 + I) &= r + r \cdot I + I + I^2 \\ &= (r + I)(1 + I) = r + I + I \cdot r + I^2 \end{aligned}$$

This implies $r \cdot I, I \cdot r \subseteq I$, as desired. □

As an immediate consequence, the kernel of any homomorphism is a 2-sided ideal! This leads us to our first isomorphism theorem for rings... Next Time!

CLASS 3, FRIDAY FEBRUARY 9TH: IDEALS & ISOMORPHISM THEOREMS

Last time, we developed the notion of an ideal $I \subseteq R$. Now, we exploit this idea further.

Theorem 0.1 (First Isomorphism Theorem for Rings)**.**
Let $\varphi : R \to S$ be a homomorphism of rings, and let $I = \ker(\varphi)$. Then $\varphi = \varphi' \circ q$, where $q : R \to R/I$ and $\varphi' : R/I \to S : r + I \mapsto \varphi(r)$.

In addition, any ideal is the kernel of the morphism q described above. Thus there exists a bijection

$$\{\textit{kernels of homomorphisms from } R\} \leftrightarrow \{\textit{Ideals of } R\}$$

We have essentially proved this as a remark at the end of last class.

Example 0.2. Let's try to think about ideals of $\mathbb{Z}[x]$ (there are many). Here is one example: Let $\varphi : \mathbb{Z}[x] \to \mathbb{C}$ by taking $\mathbb{Z}$ to itself and $x \mapsto i$. This is a valid ring homomorphism, defining $\varphi(x^n) = \varphi(x)^n = i^n$. What is the kernel? One can check that $x^2 + 1$ is a generator of the kernel. So there is a natural ideal $\langle x^2 + 1 \rangle$.

Another example are the projections $\mathbb{Z}[x] \to \mathbb{Z}$, $\mathbb{Z}[x] \to \mathbb{Z}/n\mathbb{Z}$, and $\mathbb{Z}[x] \to \mathbb{Z}/n\mathbb{Z}[x]$. In each case, I am either quotienting out $\mathbb{Z}$ by a number or setting x to be 0. These yield the ideals $\langle x \rangle$, $\langle n, x \rangle$, $\langle n \rangle$ respectively.

We can expand to give the complete list of isomorphism theorems for rings:

Theorem 0.3 (2nd - 4th Isomorphism Theorems for Rings)**.**

2) Let A be a subring of R, and I be an ideal of R. Then $A + I$ is a subring of R, and $A \cap I$ is an ideal of A. Furthermore,

$$(A + I)/I \cong A/(A \cap I).$$

3) Let $I \subset J$ be ideals of a ring A. Then J/I is an ideal of A/I, and

$$A/J \cong (A/I)/(J/I)$$

4) Let I be an ideal of R. Then there is a inclusion preserving bijection

$$\{\textit{Subrings } A \textit{ containing } I\} \leftrightarrow \{\textit{Subrings of } A/I\}$$

Furthermore, A is an ideal of R if and only if A/I is an ideal of R/I.

Proof. 2) $A + I$ is a subring of R, since it is closed under addition, and

$$(a + i)(a' + i') = aa' + ai' + ia' + ii'$$

$aa' \in A$, and $ai', ia', ii' \in I$.

Similarly, $I \cap A$ is an ideal of A, since $a \cdot i \subset I$ in R, and thus if $i \in A \cap I$, then $a \cdot i \in A \cap I$.

Finally, consider the composition $A \to A + I \to A + I/I$, sending a to $a + I$. This is a surjective map as any $a + i + I$ is realized as the image of a. It only goes to compute the kernel. An element $a \in A$ is sent to $0 + I$ if and only if $a \in I$. Thus $a \in A \cap I$. Therefore the kernel is exactly $A \cap I$, which implies that $A/A \cap I \cong (A + I)/I$.

3) The fact that J/I is an ideal is left as an exercise. Consider the quotient map $R/I \to R/J : r + I \mapsto r + J$. This is surjective since $J \supset I$. The kernel is $r + I \subseteq J$, which since $I \subseteq J$, implies $r \in J$ by contraposition. Therefore the kernel is exactly J/I.
4) If I is a subset of A, then $A/I \subseteq R/I$ is a subring. In the opposing direction, if B is a subring of R/I, then we can consider $q^{-1}(B) \subseteq R$. This is a subring by the same algebraic tricks of the second isomorphism, and contains I since $I = q^{-1}(0) \subseteq q^{-1}(B)$. The statement about ideals is a fun exercise.

□

Example 0.4. Consider the ring $R = \mathbb{Z}/n\mathbb{Z}$ for some positive integer $n > 1$. Let's try to find the ideals of R.

By Isomorphism Theorem 4, we know that $J/n\mathbb{Z} \subseteq \mathbb{Z}/n\mathbb{Z}$ is an ideal if and only if $J \subset \mathbb{Z}$ is an ideal containing $n\mathbb{Z}$.

What are the ideals containing $n\mathbb{Z}$ in $\mathbb{Z}$? They are simply $m\mathbb{Z}$ where $m|n$. So if n has a prime factorization of

$$n = p_1^{k_1} \cdots p_l^{k_l}$$

any m of the form $p_1^{k_1'} \cdots p_l^{k_l'}$ where at $k_j' \leq k_j$ works. This completely classifies all ideals of $\mathbb{Z}/n\mathbb{Z}$.

Finally, here are a few operations one can perform on ideals:

- (The Sum) For two ideals I, J, we can form the ideal $I + J$ to be
$$I + J = \{i + j \ : \ i \in I, \ j \in J\}$$
Note that since $0 \in I, J$, we have that $I, J \subseteq I + J$.
- (The Product) We can form the product of two ideals as follows:
$$I \cdot J = \{\sum_{k=0}^{l} i_k \cdot j_k \ : \ i \in I, \ j \in J\}$$
Note in particular that it is NOT strictly the product of two such elements, to be seen momentarily.
- (The Intersection) We can intersect two ideals set theoretically to produce an ideal $I \cap J$ contained in both (**check!**). It contains the product (sometimes properly).
- (The Power) We can iterate the product as above to produce $I^n = I^{\ n-times\ \cdots}\ I$.

Here are two quick examples to demonstrate some points for these operations:

Example 0.5 (Intersection vs Product)**.** $I \cdot J \subset I \cap J$, because any one of the elements must be in both I and J by strong closure under multiplication. However they are not always the same. For example, let $R = \mathbb{Z}$, and $I = \langle 6 \rangle$ and $J = \langle 10 \rangle$. Their intersection is seen to be $\langle 30 \rangle$, but their product is $\langle 60 \rangle$.

Example 0.6 (Fake product is NOT an ideal)**.** Suppose we defined $I \cdot J$ to be the set of elements of the form $i \cdot j$. Let $R = K[x, y, z, w]$, and consider the ideals $I = \langle x, y \rangle$ and $J = \langle z, w \rangle$. Then elements of the fake product would be xz, xw, yz, yw and any products of various elements with these elements. An ideal needs to be closed under addition, so $xz + yw \in I \cdot J$. However, this is not the case as one can check $xz + yw$ is irreducible (usually called the quadric surface), and thus not a product of elements of I and J.

CLASS 4, MONDAY FEBRUARY 12TH: NOETHERIAN PROPERTY & IDEALS

We already discussed how to generate an ideal by select elements, stating that it is the smallest two-sided ideal generated by the elements $A = \{f_1, f_2, \ldots, f_n\}$ (or potentially even an infinite set). The notation was

$$\langle A \rangle = \langle f_1, f_2 \ldots, f_n \rangle$$

We can also introduce notation for the left and right ideal; RA and AR respectively. How do we know that such a smallest ideal exists?

$$\langle A \rangle = \bigcap_{\substack{I \supseteq A \\ \text{I is an ideal}}} I$$

If there are finitely many f_i, we call the ideal **finitely generated**. If there is only a single generator, the ideal is called **principal**.

Definition 0.1. A ring R is called **Noetherian** if every ideal is finitely generated. This naturally also yields left and right Noetherian rings by putting the adjective on ideal.

This is a fantastic property, named after the great mathematician Emmy Noether. Here some equivalent ways to specify this property:

Proposition 0.2. *The following conditions are equivalent:*

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

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

  the $\exists n > 0$ such that $I_n = I_{n+1} = I_{n+2} = \ldots$.
- *Every 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. See homework. □

This condition will become extremely important later when we study **modules** and the **spectrum** of a ring, since it puts a measure on the size of a ring. Examples include $\mathbb{Z}$, $K[x_1, \ldots, x_n]$, or even $R[x_1, \ldots, x_n]$ and $R[\![x_1, \ldots, x_n]\!]$ where R is a Noetherian ring (a theorem of Hilbert that we will return to later). In fact, most rings you will study in practice are Noetherian. A simple non-example is a polynomial ring in infinitely many variables: $K[x_1, x_2, x_3, \ldots]$.

Definition 0.3. An ideal $\mathfrak{m} \neq R$ is called **maximal** if the only ideal properly containing $\mathfrak{m}$ is R itself.

An ideal $\mathfrak{p}$ is called prime if for every $r, s \in R$, if $r \cdot s \in \mathfrak{p}$, then either $r \in \mathfrak{p}$ or $s \in \mathfrak{p}$.

Proposition 0.4. *Every proper ideal ($\neq R, 0$) I in a unital ring R is contained in some maximal ideal.*

We require a Lemma from set theory; Zorn's Lemma:

Lemma 0.5 (Zorn's Lemma)**.** *Let S be a partially ordered set, with the property that every ascending chain has an upper bound. Then there exists a maximal element.*

Proof. Let $\mathcal{C}$ be the set of all proper ideals containing I. Note in particular that $\mathcal{C} \neq \emptyset$, since it contains I. If $I_1 \subseteq I_2 \subseteq \dots$ is an ascending chain of ideals in $\mathcal{C}$, then

$$J = \bigcup_{i \geq 1} I_i$$

is a proper ideal containing I which is an upper bound for the chain. Therefore, Zorn's Lemma applies, and there is a maximal element $\mathfrak{m}$ of the set $\mathcal{C}$. This is necessarily a maximal ideal since if it were contained in another proper ideal, it would contain I and therefore make $\mathfrak{m}$ non-maximal in $\mathcal{C}$. This completes the proof. □

Next up, we see an equivalent way to detect whether an ideal is maximal or prime. In addition, it demonstrates that all maximal ideals are in fact prime.

Proposition 0.6. *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.*

Since fields are in particular integral domains;

Corollary 0.7. *All maximal ideals are prime!*

Proof. of Proposition 0.6: I will prove the statements in order. Let $\mathfrak{p}$ be a prime ideal. Then there exist no elements $a, b \in R$ not in $\mathfrak{p}$ with the property that $a \cdot b \in \mathfrak{p}$. Suppose that $\bar{a}, \bar{b} \in R/\mathfrak{p}$ are such that $\bar{a} \cdot \bar{b} = 0$. Then since $R \to R/\mathfrak{p}$ is surjective, there exist a, b mapping to $\bar{a}, \bar{b}$. This implies that $a \cdot b \in \mathfrak{p}$, a contradiction.

The converse follows by an identical argument.

Now I consider the second statement. Let $\mathfrak{m}$ be a maximal ideal. Then there exists no proper ideals containing $\mathfrak{m}$. By the fourth isomorphism theorem, we know that the ideals of $R/\mathfrak{m}$ are exactly those which contain $\mathfrak{m}$, which is exactly $\mathfrak{m}$. Therefore, the only ideal of $R/\mathfrak{m}$ is the zero ideal. This is precisely the condition of a field:

Lemma 0.8. *A commutative ring is a field if and only if it's only ideal is the* 0 *ideal.*

Proof. If R is a field, then every element is a unit. Therefore, any non-zero ideal contains 1 and thus everything. Since R is commutative, it is necessarily a field.

On the other hand, if R is a commutative ring which is not a field, then R necessarily contains a non-unit r. This implies $\langle r \rangle$ is a proper, non-zero ideal. □

This completes the proof of the forward direction of the theorem. The other direction also uses the fourth isomorphism theorem naturally. □

CLASS 5, WEDNESDAY FEBRUARY 14TH: LOCALIZATION

Today, to simplify matters, we will focus exclusively on commutative rings R.

When studying the properties of the ring, sometimes having possibly uncountably many maximal ideals can be a burden. Therefore, we often can use a process called **localization** of a ring to make the ring have only a single maximal ideal. Such a ring is called **local**.

The basic idea is as follows;

1) We can make it so that any element is a unit by adjoining an inverse of it to the ring. For example, with $\mathbb{Z}$, we can make 2 into a unit by adjoining $\frac{1}{2}$: $\mathbb{Z}_2 = \mathbb{Z}[\frac{1}{2}]$.
2) The effect of this is the following: $\langle 2 \rangle$ was a prime (maximal) ideal of $\mathbb{Z}$. However, in $\mathbb{Z}_2$ we have made it so that $\mathbb{Z}$ retains all of its prime ideals except $\langle 2 \rangle$.
3) We can "continue" to adjoin inverses to remove other prime ideals.

But how can this be generalized?

Definition 0.1. A **multiplicatively closed set** $W \subseteq R$ is a subset of R such that it is closed under multiplication. We assume $1 \in W$ and $0 \notin W$ for simplicity, though the theory can be developed more broadly.

If W is a multiplicatively closed set, then we define the **localization of R at W**, denoted $W^{-1}R$ to be the following ring: As a set,

$$W^{-1}R = \{(w, r) \ : \ w \in W, \ r \in R\}/\sim$$

where $\sim$ is the equivalence relation defined by $(w, r) \sim (w', r')$ if there exists $s \in W$ such that

$$s(wr' - w'r) = 0$$

The multiplication operation is $(w, r) \cdot (w', r') = (ww', rr')$. For addition, we declare

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

Finally, we get a ring homomorphism $R \to W^{-1}R$ given by $r \mapsto (1, r)$. This is usually called the **localization map**.

It is worthwhile to check that this is a ring. Note that even though the operations in for a localized ring are complicated, they are inspired by something quite simple:

Example 0.2 (The Good)**.** Suppose that R is an integral domain, and W is a multiplicatively closed set. We will switch between the following two notations freely:

$$(w, r) = \frac{r}{w}$$

Then, as one may expect,

$$(w, r) \sim (w', r') \Leftrightarrow wr' = w'r \Leftrightarrow \frac{r'}{w'} = \frac{r}{w}$$

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

$$(w, r) + (w', r') = \frac{r}{w} + \frac{r'}{w'} = \frac{rw' + r'w}{ww'} = (ww', rw' + r'w)$$

So the motivation for localization is very simply **fractions**. However, fractions make far less sense when you are outside of an integral domain. In particular, we know division by 0 is problematic, but what about division by a zero divisor?

Example 0.3 (The Bad)**.** 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 $W^{-1}R$.

Example 0.4 (The Ugly)**.** 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 $y = z = 0$ in the new ring. So $W^{-1}R = k[x, x^{-1}]$.

Lemma 0.5 (The Beautiful)**.** *If R is a commutative ring, and $\mathfrak{p}$ is a prime ideal, then $R \setminus \mathfrak{p}$ is a multiplicatively closed set.*

Proof. See homework. □

As a result, we can make the following definition.

Definition 0.6. For a ring R and prime ideal $\mathfrak{p}$, we define the localization of R at $\mathfrak{p}$ to be the ring

$$R_{\mathfrak{p}} := (R \setminus \mathfrak{p})^{-1} R$$

We think of this ring as describing the geometry of the ring R near the prime $\mathfrak{p}$. This will be made rigorous later on. Here is the reason localization is so powerful:

Theorem 0.7. *The collection of prime ideals of $W^{-1}R$ is exactly the collection of prime ideals of R not intersecting W:*

$$\{\mathfrak{p} \subset R \text{ a prime ideal, } W \cap \mathfrak{p} = \emptyset\} \leftrightarrow \{\mathfrak{p} \in W^{-1}R \text{ a prime ideal}\}$$

Corollary 0.8. *The prime ideals of $R_{\mathfrak{p}}$ are in natural bijection with the primes of R contained in $\mathfrak{p}$. In particular, the unique maximal ideal of $R_{\mathfrak{p}}$ is $\mathfrak{p} \cdot R_{\mathfrak{p}}$.*

Proof. Prime ideals cannot contain units. Therefore, if we consider a prime ideal $\mathfrak{q}$ of $W^{-1}R$, we know that $\varphi(w) = (1,w) \notin \mathfrak{q}$, where $\varphi : R \to R_{\mathfrak{p}}$ is the localization map. Therefore, $\varphi^{-1}(\mathfrak{q})$ is a prime ideal of R by the result of the homework.

Moreover, if $\mathfrak{q}$ is a prime of R, then I claim $\mathfrak{q} \cdot R_{\mathfrak{p}}$ is a prime ideal of $R_{\mathfrak{p}}$. Indeed, if $(w,r) \cdot (w',r') \in \mathfrak{q} \cdot R_{\mathfrak{p}}$, then $r \cdot r' \in \mathfrak{q}$ by clearing denominators. Finally, we see r or r' must have been in $\mathfrak{q}$ to begin with, and therefore either (w,r) or (w',r') was in $\mathfrak{q} \cdot R_{\mathfrak{p}}$. This completes the proof. □

Example 0.9. 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 the Theorem, we have that they are in bijection with the primes primes of $\mathbb{Z}$ not intersecting W. So those primes are exactly primes not divisible 2, 3, or 5. So they are $0, \langle 7\rangle, \langle 11\rangle, \langle 13\rangle, \ldots$.

Next time we will do some homework presentations and talk about the biggest possible localization: the ring of fractions.

CLASS 6, WEDNESDAY FEBRUARY 21ST: MODULE THEORY

Assumption: From now on we will assume R is a commutative ring with unity.

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 0.1. A **module** over a commutative ring R is an abelian group $(M, +)$ with a multiplication by elements of R, that respects the additive structure of R. Let $r, s \in R$ and $m, m' \in M$:

1) R**-Distributive:** $(r + s) \cdot m = rm + sm$.
2) M**-Distributive:** $r(m + m') = rm + rm'$.
3) **Associative:** $(rs)m = r(sm)$.
4) **Unital:** If R is assumed to be a unital ring, then we assume $1 \cdot m = m$.

M is often referred to as an R-module.

Technically, this is the notion of a 2-sided module. You can guess what left/right modules are. The next few examples show the prevalence of R-modules:

Example 0.2 (**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 0.3. A module M of R is called **free** if

$$M = R^{\oplus\Lambda} = R^{\Lambda} = \{(r_\lambda)_{\lambda\in\Lambda} \mid r_\lambda \in R\}$$

Modules also generalize the notions of this class so far!

Example 0.4 (**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 0.5 (**Ring Homomorphisms).** Let $\varphi : R \to S$ be a unital ($\varphi(1_R) = 1_S$) 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) We assume unital.

We can also manipulate modules over a ring R to be more tame:

Definition 0.6. The **annihilator** of a module M is the following set:

$$Ann_R(M) = \{r \in R \mid r \cdot m = 0 \ \forall m \in M\}$$

Proposition 0.7. *$Ann_R(M)$ forms an ideal of R. If M is an R-module, then R can naturally be viewed as an $R/Ann_R(M)$ module. Therefore, if $Ann_R(M)$ is a maximal ideal, we can view M as an $R/Ann_R(M)$ vector space.*

Proof. Let $i \in Ann_R(M)$ and $r \in R$. Then $i \cdot m = 0$ implies $(ri)m = r(im) = r0 = 0$. Similarly, if $i_1, i_2 \in Ann_R(M)$, then $i_1 m = i_2 m = 0 = (i_1 + i_2)m$. So $Ann_R(M)$ is an ideal.

Consider the action of $R/Ann_R(M)$ on M given by $(r + Ann_R(M))m = rm$. This is well defined since $a \in Ann_R(M)$ implies $rm = (r + a)m$.

The final statement follows from previous observations, such as $R/Ann_R(M)$ being a field if $Ann_R(M)$ is maximal and Example 0.2. □

An additional example is in fact a major theorem (cf class 7).

Example 0.8 (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 itself: $g + g + \ldots + g$. In addition, the conditions of being a $\mathbb{Z}$-modules are precisely those required to form a group.

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 0.5.

Moreover, if for every element $x \in M$, $nx = 0$, M is naturally a $\mathbb{Z}/n\mathbb{Z}$-module by Proposition 0.7.

Example 0.9 (An alternative to linear algebra)**.** One way to study linear algebra is to consider $K[x]$-modules! In particular, given a K vector space V and a linear transformation $M : V \to V$, we can produce a $K[x]$-module structure by

$$(a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0) \cdot v = a_n M^n(v) + a_{n-1}M^{n-1}(v) + \ldots + a_1 M(v) + a_0 v$$

Moreover, we can view any modules as a K-module by considering the action of K induced by the inclusion $K \to K[x]$ under Example 0.5. This yields the desired bijection

$$\{K[x] - modules\} \leftrightarrow \{\text{V a } K\text{-Vector spaces and a linear map } T : V \to V\}$$

One can study many maps simultaneously by consideration of $K\{x_1, x_2, \ldots, x_n\}$, or even $K\{A\}$ for A a set of linear maps $V \to V$. Here the notation $\{A\}$ is to denote the fact that $x_1 \cdot x_2 \neq x_2 \cdot x_1$. In effect, we are adjoining a free group on n (or $|A|$) generators.

Example 0.10 (An alternative to calculus)**.** One can also study the ring $K[\frac{\partial}{\partial x}]$ and the module $C^\infty(K)$ of infinitely differentiable function from K to K.

As a final example of a module (for today), we can look at R-Algebras.

Definition 0.11. If R is a commutative unital ring, an **R-algebra** A is an R-module with a notion of multiplication. That is there is a ring homomorphism $R \to A$ with image in the center of A. We do not assume commutativity.

Example 0.12 (Group Rings)**.** Much like we adjoin variables to a ring, we can adjoin a (potentially non-Abelian) group G. It's objects are of the form

$$r_1 g_1 + r_2 g_2 + \ldots r_n g_n$$

for $r_i \in R$ and $g_i \in G$. We multiply $rg \cdot r'g' = rr'gg'$, noting the importance of order in gg'. This is an example of an R-algebra.

As a sub-example, $K[x_1, x_1^{-1}, \ldots, x_n, x_n^{-1}]$ can be viewed as the group ring $K[\mathbb{Z}^n]$, where $r \cdot x_1^{m_1} \cdots x_n^{m_n}$ corresponds to $r \cdot (m_1, \ldots, m_n)$. This is the degree!

CLASS 7, FRIDAY FEBRUARY 23RD: MODULE HOMOMORPHISM AND QUOTIENTS

Definition 0.1. 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 0.2. *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

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

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

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

Example 0.3. There is a natural isomorphism between $\mathrm{Hom}_R(R, M)$ and M, given by $\varphi \mapsto \varphi(1)$ and $m \mapsto (\varphi : R \to M : 1 \mapsto m)$.

Example 0.4. Consider the module $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$ is module isomorphic to $\mathbb{Z}/\gcd(m, n)\mathbb{Z}$. This can be seen as follows:

1) Every such map is determined by where $1 \in \mathbb{Z}/m\mathbb{Z}$ is sent in $\mathbb{Z}/n\mathbb{Z}$.
2) To be a well defined map, $m \cdot \varphi(1) = 0$, or equivalently, $n | m \cdot \varphi(1)$.
3) We note that there must exist $k \in \mathbb{Z}$ such that $kn = mx$, or equivalently, $x = \frac{kn}{m}$ (which must be an integer).
4) Two homomorphisms agree if $\frac{kn}{m} \equiv \frac{k'n}{m} \pmod{n}$.
5) Looking at the prime factorization, we can see that there are $\gcd(m, n)$ many possibilities.
6) Finally, we can create the map
$$\mathbb{Z}/\gcd(m, n)\mathbb{Z} \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) : a \mapsto (\varphi : 1 \mapsto an/\gcd(m, n))$$
7) This map has an inverse given by $\varphi \mapsto \frac{\varphi(1)\gcd(m,n)}{n} \pmod{\gcd(m, n)}$

As a special note, if m, n are relatively prime, then there exist NO non-zero Homs from $\mathbb{Z}/m\mathbb{Z}$ to $\mathbb{Z}/n\mathbb{Z}$.

Proposition 0.5. *There is a natural map* $\mathrm{Hom}_R(N, P) \times \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M, P)$ *given by composition.*

In addition, $\mathrm{End}_R(M) := \mathrm{Hom}_R(M, M)$ *has a natural structure as an* R*-algebra.*

Proof. See homework. □

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

Definition 0.6. 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. This is a R-module in it's own right.

Proposition 0.7. *Let $\varphi : M \to N$. Then $ker\varphi \subseteq M$ and $\mathrm{im}(\varphi) \subseteq N$ are submodules.*

As a result, every morphism $\varphi : M \to N$ factors through module homomorphisms

$$M \xrightarrow{q} M/\ker(\varphi) \xrightarrow{\varphi'} \mathrm{im}(\varphi) \xrightarrow{i} N$$

where q is a surjective map, φ' is an isomorphism, and i is an injection.

Proof. We can define q to be the quotient map $q(m) = m+\ker(\varphi)$, $\varphi'(m+\ker(\varphi)) = \varphi(m)$ (which is well defined!), and i to be the inclusion map of $\mathrm{im}(\varphi)$ into N. This is nearly identical to the case of rings just with one addition map. □

Example 0.8. We can define $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}[x]$ as $\mathbb{Z}$-modules by sending 1 to 1 in $\mathbb{Z}/p\mathbb{Z}$. This above factorization would then be

$$\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z} \hookrightarrow \mathbb{Z}/p\mathbb{Z}[x].$$

Proposition 0.9. *If $N, N' \subseteq M$ are submodules, then $N + N'$ and $N \cap N'$ are also submodules.*

Proof. Exercise. □

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 0.10. *1) The map φ' in Proposition 0.7 is an isomorphism.*

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

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

Proof. I will only prove the first of the set of isomorphism theorems. First, I will show φ' is well defined:

$$\varphi'(m + k + \ker(\varphi)) = \varphi(m + k) = \varphi(m) + \varphi(k) = \varphi(m) = \varphi'(m + \ker(\varphi))$$

φ' is surjective by design: it is the set of objects that are $\varphi(m)$ for some $m \in M$. It is also injective: if $\varphi'(m + \ker(\varphi)) = \varphi(m) = 0$, then $m \in ker(\varphi)$. □

CLASS 8, MONDAY FEBRUARY 26TH: THE STRUCTURE OF A MODULE: GENERATION AND FREE MODULES

Last time we talked about the sum of 2 submodules $N + N' \subseteq M$. This can be used to establish the idea of generation for modules in an identical way to that of ideals.

Definition 0.1.

- If $N_\lambda \subseteq M$ is a submodule for each λ in an indexing set Λ, then
$$\sum_{\lambda \in \Lambda} N_\lambda = \{n_{\lambda_1} + \ldots + n_{\lambda_m} \mid n_{\lambda_i} \in N_{\lambda_i}\}$$
That is to say the **sum of modules** consists of a finite sum of elements from each. If Λ is a finite indexing set, it is often written as $N_1 + \ldots + N_m$
- If $n \in N$, we let $\langle n \rangle_N$ be the smallest submodule of N containing n. It consists precisely of elements $r \cdot n$ for $r \in R$. We can further write
$$\langle S \rangle = \sum_{s \in S} \langle s \rangle_N$$
for any subset $S \subseteq N$.
- We say a module is **generated** by a subset $S \subseteq M$ if $M = \langle S \rangle$.
- We say M is **finitely generated** if S can be assumed to be a finite set.
- We say M is **cyclic** if S can be assumed to be 1 element.
- If M is finitely generated, we call S a **minimal generating set** if there exists no generating set of smaller cardinality.

Finitely generated modules over Noetherian rings are one of the most well studied objects in commutative algebra.

Example 0.2 (Non-finitely generated modules)**.** Consider $\mathbb{Q}$ is a $\mathbb{Z}$-module. It is fairly easy to see that this is a non-finitely generated $\mathbb{Z}$-module. In particular, if $\mathbb{Q} = \langle \frac{a_1}{b_1}, \ldots, \frac{a_n}{b_n} \rangle$, we can choose a rational number smaller than $|\frac{1}{b_1 \cdots b_n}|$. This number cannot be represented as a sum with integer coefficients.

Additionally, $K[x]$ as a K-module is an infinite dimensional vector space (with basis $1, x, x^2, \ldots$). Therefore it cannot be finitely generated, or it would be a finite dimensional vector space.

Example 0.3 (Many cyclic modules)**.** R viewed as an R-module is a cyclic module, generated by 1. The same holds for R/I for an ideal I, so these are all examples of cyclic modules.

Example 0.4 (Finitely generated modules)**.** Let $R = S = K[x]$. Consider the map $R \to S : x \mapsto x^n$ with K fixed. Then S is a non-cyclic but finitely generated R-module. It has a (minimal) generating set given by $\langle 1, x, \ldots, x^{n-1} \rangle$.

Next up, we can consider the operation of $\oplus$, called the **direct sum**.

Definition 0.5. For 2 modules M, N, we define
$$M \oplus N = \{(m, n) \mid m \in M, n \in N\}$$

where addition and multiplication are defined by $r(m,n) = (rm, rn)$ and $(m,n)+(m',n') = (m+m', n+n')$. We can perform this operation inductively to produce a finite direct sum of modules $M_1 \oplus M_2 \oplus \ldots \oplus M_n$.

There is also a notion of an infinite direct sum, where we consider infinite tuples of elements of each module, but require that all but finitely many of them are 0:

$$\oplus_{\lambda\in\Lambda} M_\lambda = \{(m_\lambda)_{\lambda\in\Lambda} \mid m_\lambda = 0 \text{ for almost all } \lambda \in \Lambda\}$$

This differs from the notion of the **Direct Product**, for which no such restriction is put on almost all m_λ. They are however identical in the case of a finite indexing set.

Definition 0.6. A module F is said to be **free** if $F \cong R^{\oplus\Lambda}$ for some indexing set Λ. If Λ is a finite set, we define the **rank** of F is $\text{rank}(F) = |\Lambda|$.

The rank of a free module is the same as the rank/dimension of a vector space.

One can view minimal generation in terms of free modules. Say M is a module generated minimally by the set $S = \{m_1, \ldots, m_n\}$. We can then consider the homomorphism

$$g : F = R^n \to M : (r_1, \ldots, r_n) \mapsto r_1 m_1 + \ldots + r_n m_n$$

This map is surjective by definition of generation! The kernel of this map can be thought of as an **obstruction** to being free. That is to say $\ker(g) = 0$ if and only if M is free, and larger kernels can be thought of as 'less free' modules.

Aside (Homology)**.** *This produces the idea of the* **Homology** *of a module. Because we can surject onto any module M by a free module F_0, we can form a* **free resolution** *of M by surjecting onto the kernel of the map by a free module F_1, and continue in this fashion:*

$$\ldots \to F_2 \to F_1 \to F_0 \to M \to 0$$

The propogation of kernels allows one to measure the complexity of the module. We may return to Homological Algebra later on.

On the opposite end of the spectrum, we have a notion of torsion modules:

Definition 0.7. A module M is said to be **torsion** if for each $m \in M$ there exists a non-zero divisor $r \in R$ (depending on m) such that $r \cdot m = 0$.

Example 0.8 ($\mathbb{Z}$)**.** Any finite $\mathbb{Z}$-module M is a finite Abelian group (as discussed in Class 6). Therefore, if $|M| = n$, we know that $n \cdot M = 0$. Therefore, M is a torsion module!

There also exist infinite torsion groups. Let p_i be the i^{th} prime number. Then

$$M = \oplus_{i=1}^{\infty} \mathbb{Z}/p_i\mathbb{Z}$$

is an infinitely generated (thus infinite) torsion module.

This is part of a much larger theorem, that I will state without proof:

Theorem 0.9 (Finitely Generated Modules over a PID)**.** *Let R be a principal ideal domain (every ideal is principal). Then if M is a finitely generated module,*

$$M \cong F \oplus T$$

where F is a free module and T is a torsion module.

This is not the case if R is not a PID ($R = K[x,y]$, $M = \langle x^2 + y^3, x^4 - y^2\rangle$) or if M is infinitely generated ($R = \mathbb{Z}$, $M = \mathbb{Q}$).

CLASS 9, WEDNESDAY FEBRUARY 28TH: TENSOR PRODUCTS I

In Homework 2, I defined the tensor product of 2 modules M, N. This is one of the most powerful tools in the study of module theory, and today we will study some of the basic properties. Recall the definition:

Definition 0.1. The **tensor product** of two R-modules M, N is

$$M \otimes_R N = \{\sum_{i=1}^{l} m_i \otimes n_i \mid m_i \in M, n_i \in N\}/\sim$$

where $\sim$ is defined by

1) $mr \otimes n \sim m \otimes rn$
2) $m \otimes n + m' \otimes n \sim (m + m') \otimes n$
3) $m \otimes n + m \otimes n' \sim m \otimes (n + n')$

In the homework, you are asked to prove the following 2 facts: $M \otimes_R N$ has a natural R-module structure, and tensoring by a ring S which is also an R-module can upgrade M to an S-module (cf Homework 2, 5/6). These facts are invaluable. I now state some further basic properties:

Proposition 0.2. *1) If $\phi : R \to S$ is a ring homomorphism, then there is a natural R-module homomorphism $M \to M \otimes_R S$ given by $m \mapsto m \otimes 1$.*
2) There is a natural map $\otimes : M \oplus N \to M \otimes_R N$ given by $(m, n) \mapsto m \otimes n$. This is not a homomorphism!
3) If $\varphi : M \oplus N \to P$ is a bilinear map, then $\exists!\ \Phi : M \otimes_R N \to P$ such that $\varphi = \Phi \circ \otimes$.

Proof. I prove the statements in order:

1) If $r \in R$, then $r\phi(m) = r(m \otimes 1) = (rm) \otimes 1 = \varphi(rm)$. Similarly, relation 2) above implies ϕ is additive. Therefore it is a homomorphism of R-modules.
2) There is almost nothing to prove. This is what is called a **balanced product**, and is key to the definition of the tensor product. Note that this is not a homomorphism of R-modules because

$$\otimes((m, n) + (m', n')) = \otimes(m + m', n + n') = (m + m') \otimes (n + n') =$$
$$m \otimes n + m \otimes n' + m' \otimes n + m' \otimes n' \neq m \otimes n + m' \otimes n'$$

3) First note that a map is called **bilinear** if restricting to a specific $m \in M$ or $n \in N$ makes φ into a homomorphism:

$$\varphi(rm + m', n) = r\varphi(m, n) + \varphi(m', n)$$
$$\varphi(m, rn + n') = r\varphi(m, n) + \varphi(m, n')$$

Therefore, in part 2), $\otimes$ is a natural bilinear map. As a result, we define

$$\Phi : M \oplus N \to P : \sum_i m_i \otimes n_i \mapsto \sum_i \varphi(m_i, n_i)$$

This forces $\varphi = \Phi \circ \otimes$, since

$$(\Phi \circ \otimes)(m, n) = \Phi(m \otimes n) = \varphi(m, n)$$

Moreover, this is a homomorphism as a result of the conditions of the definition of $M \otimes_R N$:

$$\Phi(rm \otimes n + m' \otimes n') = \Phi(rm \otimes n) + \Phi(m' \otimes n') = r\varphi(m, n) + \varphi(m', n')$$

□

Note: This gives an important way to convert a pair of homomorphism $M \otimes P$ and $N \otimes P$ into either a bilinear map $M \oplus N \to P$ OR a single homomorphism $M \otimes_R N \to P$.

Example 0.3 (Size of the Tensor Product)**.** It is tempting to believe that the tensor product of two modules M, N is always bigger than M or N individually, much like the direct sum. However, the following nice proposition shows this is not the case:

Proposition 0.4. *Let R be a ring, and I be an ideal. Then*

$$M \otimes_R R/I \cong M/IM$$

Proof. I claim that the map is given by

$$\varphi : M \otimes_R R/I \to M/IM : m \otimes \bar{r} \mapsto \bar{r} \cdot m$$

This map is surjective, since if $m + IM \in M/IM$, we can consider $m \otimes \bar{1} \in M \otimes_R R/I$, whose image is the desired element. In addition, if $\varphi(m \otimes \bar{r}) = \bar{0}$, then $rm \in IM$. Therefore, $rm = im'$ for $i \in I$. Therefore, the following equalities show that φ is injective:

$$m \otimes \bar{r} = rm \otimes \bar{1} = m' \otimes \bar{i} = m' \otimes 0 = 0$$

□

Another typical example is as follows: Consider $R = \mathbb{Z}$;

$$\mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/\gcd(m, n)\mathbb{Z} : a \otimes b \mapsto a \cdot b$$

$$\mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q} \cong 0$$

Another natural example we will use extensively is the localization of a module:

Example 0.5 (Localization)**.** We have already described $W^{-1}R$, the localization of R at W. This can be extended to modules in the following way: There is a natural localization map $R \to W^{-1}R : r \mapsto (1, r)$. Thus we can form the localization of an R-module:

$$W^{-1}M := M \otimes_R W^{-1}R$$

This naturally has the structure of a $W^{-1}R$ module by the Homework 2 Exercise 6. It is also an R-module by virtue of the localization map.

It is useful to check that the localization of a module, $W^{-1}M$, is equivalent to that given by copying the conditions for a ring:

$$W^{-1}M = \{(w, m) \ : \ w \in W, \ m \in R\}/\sim$$

$(w, m) \sim (w', m')$ if there exists $s \in W$ such that

$$s(wm' - w'm) = 0$$

We will see soon that a module locally satisfying some properties gives us 'global' information as well!

CLASS 10, MONDAY MARCH 5TH: TENSOR PRODUCTS II

Recall last time we ended talking about the localization of a module. I will now begin with a few example of such phenomena:

Example 0.1. Consider the $\mathbb{Z}$-module $M = \mathbb{Z}/6\mathbb{Z}$. We can consider the localization at the prime ideal $\langle 2 \rangle$:

$$M_{\langle 2 \rangle} = \mathbb{Z}/6\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}_2$$

Now, 3 is a unit in $\mathbb{Z}$, as $3 \notin \langle 2 \rangle$. Therefore, we conclude

$$2 \otimes 1 = 2 \otimes 3 \cdot \frac{1}{3} = 6 \otimes \frac{1}{3} = 0 \otimes \frac{1}{3} = 0$$

By a similar measure, $n \otimes \frac{2^m}{l} = 0$ for any $n, m > 0$ and $l \notin \langle 2 \rangle$. So we are left exactly with 2 elements (up to the tensor equivalence relations): 0 and $1 \otimes 1 = 3 \otimes 1 = 5 \otimes 1$ (since they all differ by $2 \otimes 1 = 0$). Therefore, we conclude $M_{\langle 2 \rangle} = \mathbb{Z}/2\mathbb{Z}$.

There is an often used and more high level way of seeing facts such as this:

Theorem 0.2 (Universal Property of Localization)**.** *If $\varphi : M \to N$ is a homomorphism of modules, and all $w \in W \subseteq R$ act as invertible elements on N, then φ factors as*

$$M \to W^{-1}M \to N$$

where the first map is the localization map, and $(w, m) \mapsto w^{-1}m$ is the second map.

Proof. See Homework 3. □

As a result, the localization of a module can be thought of as containing all of the information of M when mapping to modules N of the type in the Theorem.

Now I will return to the tensor product. One benefit of the tensor product is that it plays particularly nicely with direct sums of modules. This can be seen as a generalization of Homework 2, number 8.

Theorem 0.3. *Suppose M, N, P are all R-modules. Then there is a natural isomorphism*

$$(M \oplus N) \otimes_R P \cong (M \otimes_R P) \oplus (N \otimes_R P)$$

In addition, $M \otimes_R N \cong N \otimes_R M$ via $m \otimes n \mapsto n \otimes m$.

Proof. Let $\Phi : (M \oplus N) \otimes_R P \to (M \otimes_R P) \oplus (N \otimes_R P)$ be defined by

$$\Phi((m, n) \otimes p) = (m \otimes p, n \otimes p)$$

and extend by linearity. This is well defined since it respects all of the equivalence relations of the tensor product. It is a ring homomorphism for the same reason. It goes to find an inverse mapping:

$$\Psi : (M \otimes_R P) \oplus (N \otimes_R P) \to (M \oplus N) \otimes_R P$$

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

Extend by linearity and note this is also well defined. Now, we can compute

$$\begin{aligned}\Psi\left(\Phi(\sum_i (m_i, n_i)\otimes p_i)\right) &= \Psi((\sum_i m_i\otimes p, \sum_i n_i \otimes p))\\ &= \sum_i (m_i,0)\otimes p_i + (n_i,0)\otimes p\\ &= \sum_i (m_i,n_i)\otimes p_i\end{aligned}$$

It is left as an exercise to prove $\Phi\circ\Psi = Id$, and that $M\otimes_R N \cong N\otimes_R M$. □

An immediate corollary is the exercise:

Corollary 0.4. *If F is a free module, $F\otimes_R M \cong R^n\otimes_R M \cong (R\otimes_R M)^n = M^n$.*

To finish off this lesson, I would like to add a note about tensor products of algebras.

Proposition 0.5. *Let R be a ring, and A, B be R-algebras. Then $A\otimes_R B$ has the structure of an R-algebra.*

Proof. We already know that $A\otimes_R B$ is an R-module. So it only goes to put a multiplicative structure on it, and check that R is in the center.

The desired multiplicative structure is

$$(a\otimes b)\cdot(a'\otimes b') := (aa')\otimes(bb')$$

and extending by linearity (thus it is naturally distributive). It also respects the equivalence relation of the tensor:

$$(ra\otimes b)\cdot(a'\otimes b') = raa'\otimes bb' = aa'\otimes rbb' = (a\otimes rb)\cdot(a'\otimes b')$$

Finally, since R is in the center of A and B (because they are themselves algebras), we see that

$$r\cdot(a\otimes b) = ra\otimes b = ar\otimes b = a\otimes rb = a\otimes br = (a\otimes b)\cdot r$$

Therefore R is in the center of $A\otimes B$. □

Example 0.6. Given two finitely generated R-algebras

$$\begin{aligned}A &= R[x_1,\dots,x_n]/I = R[x_1,\dots,x_n]/\langle f_1,\dots,f_k\rangle\\ B &= R[y_1,\dots,y_m]/J = R[y_1,\dots,y_m]/\langle g_1,\dots,g_l\rangle\end{aligned}$$

The tensor product is also an R-algebra given by

$$A\otimes_R B = R[x_1,\dots,x_n,y_1,\dots,y_m]/\langle f_1,\dots,f_k,g_1,\dots,g_l\rangle$$

This can be seen by the isomorphism

$$A\otimes_R B \to R[x_1,\dots,x_n,y_1,\dots,y_m]/\langle f_1,\dots,f_k,g_1,\dots,g_l\rangle : f\otimes g\mapsto f\cdot g$$

extended by linearity. Indeed, we can define an inverse by

$$\sum_{\alpha,\beta} r_{\alpha,\beta}\cdot x^\alpha y^\beta \mapsto \sum_{\alpha,\beta} r_{\alpha,\beta}(x^\alpha\otimes y^\beta)$$

Here $r_{\alpha,\beta}\in R$ and α,β are multi-indexes; $\alpha\in\mathbb{N}^n$ and $\beta\in\mathbb{N}^m$.

CLASS 11, WEDNESDAY MARCH 7TH: EXACTNESS

$\otimes$ and Hom_R are two of the most important operations in commutative algebra. When applied to a given module M, they can be used to measure the complexity of M through failure of **exactness**. This is a measure of how well 2 modules approximate another.

Just a quick recall and expansion of some previous definitions:

Definition 0.1. Let $\varphi : M \to N$.

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

$$\mathrm{im}(\varphi) = \{n \in N\}$$

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

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

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

Now for the definition of exactness:

Definition 0.2. 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 $\ker(\psi) = \mathrm{im}(\varphi) \subseteq M$. 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 $\ker(\varphi_i) = \mathrm{im}(\varphi_{i-1})$ for every $i \in \mathbb{Z}$.

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

Proposition 0.3 (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 $M'' = \mathrm{coker}(\varphi) = M/M'$). 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 $\ker(\varphi) = \mathrm{im}(0 \to M) = 0$ if and only if φ is injective.

2) $M \xrightarrow{\varphi} N \to 0$ is exact if and only if $N = \ker(N \to 0) = \mathrm{im}(\varphi)$ 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 0.4.
- 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
$$0 \to \ker(\psi) \to M \to \operatorname{im}(\psi) \to 0$$

Example 0.5 (Free Resolution)**.** Recall that for any R-module M, we can find a generating set m_λ for $\lambda \in \Lambda_0$ and form a surjection from a free module:
$$R^{\Lambda_0} \to M \to 0$$
We can then look at the kernel of this map, which is a submodule of R^{Λ_0}. Thus we can repeat the process finding a generating set of the kernel, and surjecting onto it via a free module:
$$R^{\Lambda_1} \to R^{\Lambda_0} \to M \to 0$$
This is an exact sequence by design. Iterating this procedure indefinitely produces a **long exact sequence**
$$\ldots \to R^{\Lambda_2} \to R^{\Lambda_1} \to R^{\Lambda_0} \to M \to 0$$
which is called a **free resolution of** M.

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

Definition 0.6. 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:

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

Proof. See homework 3. □

CLASS 12, FRIDAY MARCH 9TH: PROJECTIVE MODULES

Projective modules play an incredibly important role in commutative algebra, similar to that of vector bundles in algebraic or differential geometry. As we will see, they are closely related to free modules in a precise sense.

Definition 0.1. A module P is said to be **projective** if whenever $\varphi : M \to N$ is a surjective homomorphism, and $\psi : P \to N$ is any homomorphism, there exists $\psi' : P \to M$ such that $\psi = \varphi \circ \psi'$.

Before moving to some equivalent formulations of a projective module, I state an important notes about the Hom_R operation (functor).

Theorem 0.2. *Suppose* $0 \to M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \to 0$ *is a short exact sequence. Then for a fixed module* N*, we get exact sequences*

$$0 \to \mathrm{Hom}_R(N, M') \to \mathrm{Hom}_R(N, M) \to \mathrm{Hom}_R(N, M'')$$

$$0 \to \mathrm{Hom}_R(M'', N) \to \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M', N)$$

Proof. First, note that if $\varphi : A \to B$ is a map of R-modules, then we get the following homomorphisms for free via composition:

$$\varphi_* : Hom(N, A) \to \mathrm{Hom}(N, B) : \psi \mapsto \varphi \circ \psi$$

$$\varphi^* : \mathrm{Hom}(B, N) \to \mathrm{Hom}(A, N) : \psi \mapsto \psi \circ \varphi$$

So in each case, we take these R-module homomorphisms to be our maps in the asserted SESs. It goes to show exactness.

Suppose $\psi \in \mathrm{Hom}_R(N, M')$ maps to to $0 \in \mathrm{Hom}_R(N, M)$. Then $\varphi(\psi(n)) = 0$ for every $n \in N$. But φ was assumed injective, so $\psi(n) = 0$ which is to say $\psi = 0$. Therefore, the first map is injective.

The only things left to show for the first SES is that it is exact at $\mathrm{Hom}_R(N, M)$, or

$$\mathrm{im}(\mathrm{Hom}_R(N, M') \to \mathrm{Hom}_R(N, M)) = \ker(\mathrm{Hom}_R(N, M) \to \mathrm{Hom}_R(N, M''))$$

I denote these submodules im and ker for sake of brevity. Note im $\subseteq$ ker, since

$$\psi(\varphi(\xi(m)) = (\psi \circ \varphi)(\xi(m)) = 0(\xi(m)) = 0.$$

In addition, suppose $\xi \in \ker$. Then $\psi(\xi(n)) = 0$ for all $n \in N$. For each n, we know that $\xi(n) \in \ker(\psi) = \mathrm{im}(\varphi)$. Therefore, we can see that $\xi(n) = \varphi(m')$ for some $m' \in M'$. Define $\xi' : N \to M' : n \mapsto m'$. This is well defined by the previous argument, and a homomorphism because ξ, φ are. Therefore, $\xi' \mapsto \xi \in \ker$, which completes the proof.

The case of the second SES is left as an exercise. □

What I have just proved is that $\mathrm{Hom}_R(N, -)$ and $\mathrm{Hom}_R(-, N)$ are **left exact**, e.g. they take short exact sequences to left exact sequences. We note that the Hom-map on the right is not surjective in general. Here is an example:

Example 0.3. There is a natural SES of $\mathbb{Z}$-modules

$$0 \to \mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \to 0$$

If we apply $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, -)$ to this sequence, we get

$$0 \to 0 \to 0 \to \mathbb{Z}/n\mathbb{Z} \to 0$$

Of course, there is no way $\mathbb{Z}/n\mathbb{Z}$ can be surjected on by 0.

However, for projective modules P, this is an exact sequence. This can be seen in the following characterization:

Proposition 0.4. *The following conditions are equivalent:*

1) P is a projective R-module.

2) $\mathrm{Hom}_R(P, -)$ is **exact***: Applying it maintains exactness of a SES.*

3) Every exact sequence

$$0 \to A \to B \to P \to 0$$

is a split exact sequence.

4) P is a direct summand of a free module: $F = R^{\Lambda} \cong P \oplus M$.

Proof. 1) $\Leftrightarrow$ 2): It goes to show exactness given left exactness, which equates to showing $\mathrm{Hom}_R(P, M) \to \mathrm{Hom}_R(P, M'')$ is surjective. P being projective states that every $\xi : P \to M''$ factors as $\psi \circ \xi' : P \to M \to M''$. Therefore, $\xi' \mapsto \xi$ and surjectivity ensues.

Similarly, if $\mathrm{Hom}_R(P, M) \to \mathrm{Hom}_R(P, M'')$ is surjective, we can simply take $\xi' \mapsto \xi$ to show projectivity.

1) $\Rightarrow$ 3): By Homework 3, or Class 11 Definition 0.6, the sequence is split exact if there exists $P \to B$ composing with the given map to the identity on P. Take the identity map on P. By projectivity of P, this map lifts to the desired splitting map $P \to B$.

3) $\Rightarrow$ 4): As we have talked about, any module has a surjection from a free module $F = R^{\Lambda}$. This fits into a SES

$$0 \to \ker(\psi) \to F \xrightarrow{\psi} P \to 0$$

Being split exact, again by Homework 3, a split exact sequence implies that $F = R^{\Lambda} \cong P \oplus \ker(\psi)$.

4) $\Rightarrow$ 1): If $R^{\Lambda} = P \oplus M$, and $M \to M''$ is a surjection, then R^{Λ} is certainly projective. Therefore, given a map $P \to M''$, we can precompose with $F \to P$ to get a map $F \to M$. This yields

$$P \to R^{\Lambda} \to M$$

which maps to the original map $P \to M''$. □

Notice the following fact about Hom_R:

Lemma 0.5. *For modules M_λ, N, $\lambda \in \Lambda$, we have isomorphisms*

$$\mathrm{Hom}_R(\bigoplus_{\lambda \in \Lambda} M_\lambda, N) \cong \prod_{\lambda} \mathrm{Hom}_R(M_\lambda, N)$$

$$\mathrm{Hom}_R(N, \bigoplus_{\lambda \in \Lambda} M_\lambda) \cong \bigoplus_{\lambda \in \Lambda} \mathrm{Hom}_R(N, M_\lambda)$$

As a corollary, we get the following nice statement:

Corollary 0.6. *If P_λ are projective modules, so is $\oplus P_\lambda$.*

CLASS 13, MONDAY MARCH 12TH: INJECTIVE MODULES

Now that we have studied projective modules, we will also study their dual notion: **injective modules**. These play a very important role in homological algebra, since many (left-exact) functors behave well with an injective resolution.

Definition 0.1. A module I is said to be **injective** if whenever $\varphi : M \to N$ is an injective homomorphism, and $\psi : M \to I$ is any homomorphism, there exists $\psi' : N \to I$ such that $\psi = \psi' \circ \varphi$.

Note the similarity to projectives, except the arrows are facing the opposing way. Similar to how a module P is projective if and only if $\mathrm{Hom}_R(P, -)$ is an exact functor, a module I is injective if and only if $\mathrm{Hom}_R(-, I)$ is an exact functor (note that arrows are flipped by this functor. This notion is called **contravariance**).

Checking something is injective seems like quite a chore; you need to check that every injection of R-modules satisfies a given property. However, a theorem of Baer allows this condition to be relaxed:

Theorem 0.2 (Baer's Criterion)**.** *A module I is injective if and only if for every ideal J of R, and every $\psi : J \to I$, there is a $\psi' : R \to I$ such that $\psi = \psi' \circ \iota$ where $\iota : J \hookrightarrow R$ is the inclusion.*

Proof. The $\Rightarrow$ direction of this theorem is obvious (if it holds for all module inclusions, it certainly holds for a subset of them!)

So it goes to prove the $\Leftarrow$ direction. Suppose $\varphi : M \hookrightarrow N$ and $\psi : M \to I$. Let $\mathcal{S}$ be the set of submodules N' of N together with $\psi' : N' \to I$ such that $\psi = \psi' \circ \varphi$. This is a non-empty set, since it certainly contains $\varphi(M) \subseteq N$. We can put a partial ordering on this set by taking $(N', \psi') \leq (N'', \psi'')$ if $N' \subseteq N''$ and $\psi' = \psi''|_{N'}$. We can take the union of an ascending chain to produce a module and map in $\mathcal{S}$, so Zorn's Lemma applies and therefore there is a maximal element of $\mathcal{S}$, call it (N_0, ψ_0). If $N_0 = N$, we are done. If not, take $x \in N \setminus N_0$. Let

$$J = \{r \in R \ : \ rx \in N_0\} \subseteq R$$

J is an ideal of R, and we can make $g : J \to I : r \to \psi_0(rx)$. So we can apply the assumption: there is a map $g' : R \to I$ factoring ψ_0. But this produces a map

$$\psi_1 : N_0 + xR \to I : n + rx \to \psi_0(n) + g'(r)$$

from a strictly larger module of $\mathcal{S}$, contradicting maximality and proving the result. $\square$

For a general ring, the proof of this theorem shows that if I is an injective R-module, then I is **divisible**: $r \cdot I = I$ for every $r \in R$ a NZD. A nice converse can be realized in the case of principal ideal domains:

Corollary 0.3. *If R is a PID, then I is an injective module if and only if I is divisible.*

Proof. We only need to prove the $\Leftarrow$ direction. Using Baer's criterion, we know I is injective if and only if the condition holds for ideals $J \subseteq R$. But R is a PID, so we know

$J = \langle x \rangle$, and $\psi : J \to I$ is completely determined by where it sends x. But I is divisible, so if $\psi(x) = \alpha$, then there is α' such that $x\alpha' = \alpha$. Therefore, we can define

$$\psi' : R \to I : 1 \mapsto \alpha'$$

This satisfies the desired condition and proves the corollary. □

This gives us a way to generate a lot of examples quickly:

Example 0.4.

1) R is an injective module over itself implies that R is divisible as an R-module. Therefore most rings do not satisfy this property.
2) As a special case of the previous item, $\mathbb{Z}$ is not an injective $\mathbb{Z}$-module. This is because $1 \notin 2\mathbb{Z}$.
3) $\mathbb{Q}$ is an injective $\mathbb{Z}$-module. In particular, every integer is invertible in $\mathbb{Q}$, so **??** applies.
4) $\mathbb{Q}/\mathbb{Z}$ is also injective. Not that we can still divide by n as a valid isomorphism.
5) A field is a PID, and every module is a vector space over a field which is divisible. Therefore, every modules over a field is injective (and projective if fg)!

The final portion of this class is devoted to the following claim: every module M is a subset of an injective module I.

Lemma 0.5. *Every $\mathbb{Z}$-module M is a subset of an injective module I.*

Proof. We have already shown that there exists a surjection $\mathbb{Z}^\Lambda \to M$. Let K be the kernel of this map, so that $M \cong \mathbb{Z}^\Lambda/K$. We see that $\mathbb{Q}^\Lambda$ is an injective $\mathbb{Z}$-module, since it is a direct sum of injectives, containing $\mathbb{Z}^\Lambda$ and thus K. We therefore conclude that $\mathbb{Q}^\Lambda/K$ is an injective module identically to the case of $\mathbb{Q}/\mathbb{Z}$. Finally, we see that $M = \mathbb{Z}^\Lambda/K \hookrightarrow \mathbb{Q}^\Lambda/K$. This completes the proof. □

This can be upgraded to any ring using the following adjointness theorem (as well as some information from next time):

Theorem 0.6 (Hom_R-$\otimes_R$ adjointness)**.** *If L, M, N are R-modules, then there is a natural isomorphism of R-modules*

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

Proof. The strategy will be to construct mutually inverse homomorphisms. Given $\psi \in \mathrm{Hom}_R(M \otimes_R N, L)$, we construct $F(\psi) \in \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, L))$ as follows:

$$(F(\psi)(m))(n) = \psi(m \otimes n)$$

Note the notation $(F(\psi)(m))(n)$ is because we want to construct an element of $\mathrm{Hom}_R(N, L)$ given an element of M. This is easily checked to be a well-defined homomorphism. Finally, it goes to construct its inverse.

Given $\varphi \in \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, L))$, define

$$G(\varphi)(m \otimes n) = (\varphi(m))(n)$$

This is well defined, since

$$(\varphi(rm))(n) = (r\varphi(m))(n) = (\varphi(m))(rn)$$

Finally, $G \circ F = Id$ and $F \circ G = Id$. This completes the proof. □

CLASS 14, WEDNESDAY MARCH 14TH: FLAT MODULES

The motivation for studying flat modules is to give $M \otimes_R -$ the same treatment as $\mathrm{Hom}_R(M, -)$ and $\mathrm{Hom}_R(-, M)$. Basically, projectives and injectives transform the Hom_R functors from merely left exact to exact functors. A flat module will do the same thing for the tensor product.

Proposition 0.1. *Let N be an R-module. If*

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

is a SES of R-modules, then the following sequence is also exact:

$$M' \otimes_R N \xrightarrow{\varphi \otimes Id_N} M \otimes_R N \xrightarrow{\psi \otimes Id_N} M'' \otimes_R N \to 0$$

Proof. First, I will show surjectivity of $M \otimes_R N \xrightarrow{\psi \otimes Id_N} M'' \otimes_R N$. Given $m'' \otimes n$, there is $m \in M$ such that $\psi(m) = m''$. Therefore, surjectivity is achieved:

$$(\psi \otimes Id_N)(m \otimes n) = \psi(m) \otimes n = m'' \otimes n$$

Now, it goes to show the sequence is exact in the middle.

$$(\psi \otimes Id_N) \circ (\varphi \otimes Id_N) = (\psi \circ \varphi) \otimes Id_N = 0 \otimes Id_N$$

So $\ker \supseteq \mathrm{im}$. This implies that there is a natural map

$$M \otimes_R N / \mathrm{im}(\varphi \otimes Id_N) \to M'' \otimes_R N$$

and it suffices to prove that this is an isomorphism by construction of an inverse. Given $m'' \otimes n$, we know $\exists m \in M$ such that $\psi(m) = m''$. Thus, we define

$$M'' \times N \to M \otimes_R N / \mathrm{im}(\varphi \otimes Id_N) : (m'', n) \mapsto m \otimes n$$

It goes to show this is well defined. If $m_1, m_2 \mapsto m''$, then $m_1 - m_2 \in \ker(\psi) = \mathrm{im}(\varphi)$. Therefore, $\exists m' \mapsto m_1 - m_2$. Therefore

$$m_1 \otimes n = (m_2 + \varphi(m')) \otimes n = m_2 \otimes n + \varphi(m') \otimes n = m_2 \otimes n$$

This is also seen to be the inverse of the map above, completing the proof. □

As an alternative, one can use the adjointness of Hom and $\otimes$ proven last class. Note that this is not exact on the left:

Example 0.2. Consider the injection $\mathbb{Z} \hookrightarrow \mathbb{Z} : 1 \mapsto n$ of $\mathbb{Z}$-modules. Tensoring by $\mathbb{Z}/n\mathbb{Z}$, we get the map

$$\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} : 1 \otimes 1 \mapsto n \otimes 1 = 1 \otimes n = 0$$

The zero map between $\mathbb{Z}/n\mathbb{Z}$ and itself clearly isn't injective.

This brings about the definition of a flat R-module:

Definition 0.3. A module F is said to be **flat** if and only if for every injection of R-modules $M \hookrightarrow N$, we get that $M \otimes_R F \hookrightarrow N \otimes_R F$ is injective. Equivalently, $- \otimes_R F$ is an exact functor (taking exact sequences to exact sequences).

Proposition 0.4. *If P is a projective module, then P is also flat.*

Proof. Let $0 \to M' \to M \to M'' \to 0$ be an exact sequence. Since P is a projective module, we know that $F = R^n \cong P \oplus P'$. Tensoring by F, we get

$$0 \to (M')^n \to M^n \to (M'')^n \to 0$$

Which is still exact, since the maps are direct sums of exact sequences. On the other hand, this induces

$$0 \to (M' \otimes_R P) \oplus (M' \otimes_R P') \to (M \otimes_R P) \oplus (M \otimes_R P') \to (M'' \otimes_R P) \oplus (M'' \otimes_R P') \to 0$$

Therefore, injectivity holds on the left, and thus $M' \otimes_R P \hookrightarrow M \otimes_R P$ □

Just to keep up the list of definitions we can associate to modules: Free implies Projective, and Projective implies Flat. The following two examples show that the notions are inequivalent.

Example 0.5 (Projective but not free)**.** Let $R = \mathbb{Z}/6\mathbb{Z}$, and $M = \mathbb{Z}/2\mathbb{Z}$ with the quotient module action. Then $R \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ by the Chinese remainder theorem. Therefore,

$$\mathrm{Hom}_R(R, -) \cong \mathrm{Hom}_R(\mathbb{Z}/3\mathbb{Z}, -) \oplus \mathrm{Hom}_R(M, -)$$

Thus we can conclude that M is projective, since the left hand side is clearly exact. However, M cannot be free, since a free R-module has either 6^n elements, or ∞-many elements.

Example 0.6 (Flat but not projective)**.** Consider $\mathbb{Q}$ as a $\mathbb{Z}$-module. $\mathbb{Q}$ is flat, since if $\varphi : M \to N$ is injective, and $\frac{1}{d} \otimes m \mapsto \frac{1}{d} \otimes \varphi(m) = 0$, then $c\varphi(m) = 0$. But this implies $cm = 0$, since φ was injective to begin with. Therefore, $\frac{1}{d} \otimes m = \frac{1}{cd} \otimes cm = 0$. However, $\mathbb{Q}$ is not projective: Suppose $F = \mathbb{Z}^\Lambda = \mathbb{Q} \oplus P$. However, $\mathrm{Hom}_\mathbb{Z}(\mathbb{Q}, \mathbb{Z}) = 0$ (since if $\alpha \mapsto n$, $\frac{\alpha}{2n} \mapsto \frac{1}{2} \notin \mathbb{Z}$). Therefore, $\mathbb{Q}$ is not a projective $\mathbb{Z}$-module.

I conclude by showing that every module injects into a injective module:

Lemma 0.7. *Let A be an R-algebra, F a flat A-module, and I an injective R-module. Then $\mathrm{Hom}_R(F, I)$ is also injective as an A-module.*

Proof. Note that $\mathrm{Hom}_A(-, \mathrm{Hom}_R(F, I)) \cong \mathrm{Hom}_R(- \otimes_A F, I)$ is a composition of two exact functors $- \otimes_R F$ and $\mathrm{Hom}_R(-, I)$. Therefore, it is exact itself. □

Theorem 0.8. *Every R-module M injects into an injective module.*

Proof. Any commutative unital ring R can be viewed as a $\mathbb{Z}$-algebra via the canonical map $\mathbb{Z} \to R : 1 \mapsto 1$. Let $I = \mathbb{Q}/\mathbb{Z}$ be the injective $\mathbb{Z}$-module discussed last class, and consider the R-module $\mathrm{Hom}_\mathbb{Z}(M, I)$. We can take a free module $F = R^\Lambda$ surjecting onto it. Applying $\mathrm{Hom}_R(-, \mathbb{Q}/\mathbb{Z})$ to this surjection, we have

$$\mathrm{Hom}_R(\mathrm{Hom}_R(M, \mathbb{Q}/\mathbb{Z}), \mathbb{Q}/\mathbb{Z}) = M^{\vee\vee} \hookrightarrow \mathrm{Hom}_R(F, \mathbb{Q}/\mathbb{Z})$$

Lastly, $M \hookrightarrow M^{\vee\vee} : m \mapsto (\psi \mapsto \psi(m))$. This completes the proof. □

Definition 0.9. The smallest such injective module (ordered by inclusions) containing a given module M is called the injective hull of M. It is usually denoted by $E_R(M)$.

There is a very nice summary of many of these results on page 402 of Dummit-Foote.

After spring break, we will talk about Nakayama's Lemma and regular rings, and then move on to positive characteristic commutative algebra.

CLASS 15, MONDAY APRIL 2ND: NAKAYAMA'S LEMMA & APPLICATIONS

Nakayama's lemma is one of the most useful tools in commutative algebra. It gives a strong passage of local properties and global properties of a ring. Today, I will state the result, and use it to prove several slight extensions of it as well as some applications. We will prove the result (starting) next time.

Theorem 0.1 (Nakayama's Lemma)**.** *If R is a local ring with unique maximal ideal $\mathfrak{m}$, and M is a finitely generated R-module, then $M = \mathfrak{m}M$ implies $M = 0$.*

Some equivalent formulations are as follows:

Theorem 0.2 (Nakayama's Lemma+)**.** *If R is a local ring with unique maximal ideal $\mathfrak{m}$, $N \subseteq N$ are finitely generated R-modules, then $M = \mathfrak{m}M + N$ implies $M = N$.*

Proof. Given the setup, we know that $M = \mathfrak{m}M + N$. If we mod out by N, we see that

$$M/N = (\mathfrak{m}M + N)/N = \mathfrak{m}M/(N \cap \mathfrak{m}M) = \mathfrak{m}M/N$$

The second equality is by the 3rd module isomorphism theorem. By Nakayama, we have $M/N = 0$, or equivalently, $M = N$.

□

Theorem 0.3 (Nakayama's Lemma++)**.** *If R is a local ring with unique maximal ideal $\mathfrak{m}$ 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 $\langle m_1, \ldots, m_n \rangle = M$.*

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

There is another formulation which gives a little more than Nakayama's Lemma.

Theorem 0.4 (Nakayama's Lemma+++)**.** *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 $rM = 0$.*

Note that there is no local assumption here. If we take $I = \mathfrak{m}$, then $r = 1 + m$ for $m \in \mathfrak{m}$. So $r \cdot M/\mathfrak{m}M = 1 \cdot M/\mathfrak{m}M = 0$ which implies $M = \mathfrak{m}M$. We will prove this variant on Wednesday.

We can get around the local assumptions by replacing $\mathfrak{m}$ by the following object

Definition 0.5. The **Jacobson radical** of a ring R is

$$Jac(R) = \bigcap_{\mathfrak{m}\ max'l} \mathfrak{m}$$

We note that we can pass from a non-local ring to a local one via localization at $\mathfrak{p}$, sending M to $M_{\mathfrak{p}}$. Moreover, we can provide a partial inverse to this procedure as follows:

Proposition 0.6 (Locally zero modules are zero)**.** *Let R be any ring, and M be any module. $M_{\mathfrak{m}} = 0$ for each maximal ideal $\mathfrak{m}$ if and only if $M = 0$.*

Proof. The localization of the zero module is certainly 0, since $M \otimes W^{-1}R = 0 \otimes W^{-1}R \cong 0$. Therefore it only goes to prove the $\Rightarrow$ direction. I will prove this statements contrapositive.

Suppose $M \neq 0$. Consider the set $Ann_R(m) = \{r \in R \mid rm = 0\}$. This is an ideal of R, and if we assume $m \neq 0$, this is a proper ideal since in particular it doesn't contain 1 (M is unital). Therefore, there exists a maximal ideal $\mathfrak{m}$ containing $Ann_R(m)$. I claim $(1, m) \neq 0$ in $M_\mathfrak{m}$. Indeed, otherwise

$$i(m - 1 \cdot 0) = i \cdot m = 0$$

for some $i \in R \setminus \mathfrak{m}$. This is impossible, since $i \notin Ann_R(m)$ by assumption. So $M_\mathfrak{m} \neq 0$. □

Therefore, if we are faced with a situation where $M = Jac(R)M$, we can localize at each maximal ideal and see

$$M_\mathfrak{m} \supseteq \mathfrak{m}M_\mathfrak{m} \supseteq Jac(R)M_\mathfrak{m} \supseteq M_\mathfrak{m}$$

Therefore $M_\mathfrak{m} = \mathfrak{m}M_\mathfrak{m}$, which implies $M_\mathfrak{m} = 0$ by Nakayama's lemma, and therefore $M = 0$ by Proposition 0.6.

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

Proposition 0.7. *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 $M = IM$. Nakayama+++ now implies that $\exists p(x) \in R[x]$ such that $1 - p(x) = x \cdot q(x)$. Since $p(x) \cdot m = 0$ for every $m \in M$, we note that $x \cdot q(x)m = m$. Therefore, $x \cdot m = \varphi(m) \neq 0$ for every $m \in M$. (MAGIC!) □

As a final remark, I want to add a nice note about Projective modules:

Theorem 0.8. *Let R be Noetherian and P be a finitely generated R-module. Then P is a projective module if and only if $P_\mathfrak{m}$ is a free $R_\mathfrak{m}$-module for every maximal ideal $\mathfrak{m}$. In this case, P is called* **locally free**.

Proof. P is projective if and only if $P \oplus P' \cong R^n$. Localizing at $\mathfrak{m}$, we can then quotient by $\mathfrak{m}$:

$$P_\mathfrak{m}/\mathfrak{m}P_\mathfrak{m} \oplus P'_\mathfrak{m}/\mathfrak{m}P'_\mathfrak{m} \cong (R_\mathfrak{m}/\mathfrak{m}R_\mathfrak{m})^n \cong (R/\mathfrak{m})^n$$

Therefore, the RHS is a vector space, and we can produce a basis with $n - m$ elements $\bar{p}_1, \ldots, \bar{p}_{n-m}$ of $P_\mathfrak{m}/\mathfrak{m}P_\mathfrak{m}$ and m elements of $P'_\mathfrak{m}/\mathfrak{m}P'_\mathfrak{m}$. As a result of Nakayama++, we see lifts $p_1, \ldots, p_{n-m}$ generate $P_\mathfrak{m}$ (similarly for $P'_\mathfrak{m}$). This shows $P'_\mathfrak{m} \cong R_\mathfrak{m}^{n-m}$.

On the other hand, let P be locally free. If $M \to N$ is a surjection, consider

$$\mathrm{Hom}_R(P, M) \xrightarrow{\psi} \mathrm{Hom}_R(P, N) \to \mathrm{coker}(\psi)$$

Localizing at each maximal ideal $\mathfrak{m}$, we see

$$\mathrm{Hom}_{R_\mathfrak{m}}(R_\mathfrak{m}^n, M_\mathfrak{m}) \xrightarrow{\psi} \mathrm{Hom}_R(R_\mathfrak{m}^n, N_\mathfrak{m}) \to \mathrm{coker}(\psi)_\mathfrak{m} = 0$$

Since $R_\mathfrak{m}^n$ is free (projective) as an $R_\mathfrak{m}$-module. By Proposition 0.6, we see $\mathrm{coker}(\psi) = 0$, and thus the desired surjectivity holds! □

CLASS 16, WEDNESDAY APRIL 4TH: NAKAYAMA'S LEMMA PROOFS

Recall the version of Nakayama we will prove is the following:

Theorem 0.1 (Nakayama's Lemma+++)**.** *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 $rM = 0$.*

We will prove this using the following generalization of the Cayley-Hamilton theorem for vector spaces.

Lemma 0.2 (Atiyah-Macdonald)**.** *Suppose M is an n-generated R-module, and $\varphi : M \to M$ is an R-linear map. If there is 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.

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 M 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 0.3. The adjugate of an $n \times n$ matrix M has its (i,j)-entry as $(-1)^{ij}$ times the determinant of the matrix M with the j^{th} row and i^{th} column omitted.

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

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

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. □

We now apply this result to the case Nakayama's lemma:

Nakayama: The assumption of Nakayama's lemma ensures that there is $Id(M) \subseteq IM$, 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. □

I now continue to add a few extra corollaries:

Theorem 0.4. *If $F \cong R^n$ is a free module, any n-generators form a* **basis** *of F. That is to say, they span (generate) F and are linearly independent:*

$$a_1 f_1 + \ldots + a_n f_n = 0 \Leftrightarrow a_i = 0 \ \forall i = 1, \ldots, n$$

Proof. This follows from our previous claim about surjective endomorphisms. The generators $f_1, \ldots, f_n$ give a surjection $R^n \to F$. However, $F \cong R^n$, so we can form the surjection $F \to R^n \to F$. By the previous corollary, this is an isomorphism, so we have that $R^n \to F$ was also injective. Therefore, $f_1, \ldots, f_n$ form a basis. □

This combined with the final result of Homework 2 demonstrates that rank is a well defined notion:

Definition 0.5. A free module $F \cong R^n$ has **rank** n, which is equivalently the minimum number of generators of F as an R-module.

More generally, we define the rank of a module M over an integral domain R to be $\text{rank}(M \otimes K(R))$, where $K(R)$ is the localization of R at the 0 ideal (thus a field).

Another application is to what are called **integral extensions**:

Definition 0.6. An inclusion of rings $R \subseteq S$ is called a **ring extension**. It is furthermore called an **integral extension** if for every $s \in S$, the module $R[s] \subseteq S$ is finite as an R-module ('s in **integral** over R'). Equivalently, s satisfies

$$s^n + r_{n-1} s^{n-1} + \ldots + r_0$$

for $r_i \in R$.

Example 0.7. Some typical examples of integral extensions are quotient rings: $R \subseteq R[x]/\langle x^2 + 1 \rangle = S$. x naturally satisfies $t^2 + 1$, and every element of S is expressible as $r_0 + r_1 x$ due to the relation. Therefore,

$$p(t) = t^2 - 2r_0 t + r_1^2 + r_0^2$$

is a monic polynomial with $p(r_0 + r_1 x)$ given by

$$\begin{aligned} &(r_0 + r_1 x)^2 - 2r_0(r_0 + r_1 x) + r_1^2 + r_0^2 \\ = r_0^2 + 2r_0 r_1 x + r_1^2 x^2 - 2r_0^2 - 2r_0 r_1 x + r_1^2 + r_0^2 \\ &= r_1^2(x^2 + 1) = 0 \end{aligned}$$

By Nakayama's lemma, we achieve the following (maybe unexpected) result:

Theorem 0.8 (Lying-over/Going-Up)**.** *Let $R \subseteq S$ be an integral extension of rings. If $\mathfrak{p}$ is a prime ideal of R, there exists $\mathfrak{q}$ a prime ideal of S such that $\mathfrak{q} \cap R = \mathfrak{p}$. Moreover, $\mathfrak{q}$ can be chosen to contain any given ideal $\mathfrak{q}'$ such that $\mathfrak{q}' \cap R \subseteq \mathfrak{p}$.*

Proof. Quotienting out by $\mathfrak{q}'$ and $\mathfrak{q}' \cap R$, we may assume $\mathfrak{q}' = 0$. Furthermore, localizing at the multiplicative set $R \setminus \mathfrak{p}$ in R and S, we may assume R is local.

With this setup, if $\mathfrak{q}$ is a maximal ideal of S containing $\mathfrak{p}\,S$, then $\mathfrak{q}$ satisfies the theorem. So it is enough to show that $\mathfrak{p}\,S \neq S$. Assume the contrary: $1 = s_1 p_1 + \ldots + s_n p_n \in S$ for $p \in \mathfrak{p}$. If we consider $S' = R[s_1, \ldots, s_n]$, then $\mathfrak{p}\,S' = S'$ as well. But this implies S' is a finitely generated R-module. By Nakayama's Lemma, $S' = 0$. This is a contradiction. □

By induction, this implies any chain of primes of R lifts to one for S.

CLASS 17, FRIDAY APRIL 6TH: REGULAR LOCAL RINGS

Next up, we will study the most idealized version of a ring from the perspective of Algebraic Geometry and commutative algebra. It corresponds closely with the idea of a manifold being smooth, or without nodes, cusps, or similar phenomena.

Definition 0.1. The dimension of a ring R is the longest length n of a chain of prime ideals of R

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_n$$

Therefore, the dimension of a field K is 0, the dimension of $\mathbb{Z}$ and $K[x]$ is 1 (because they are PIDs), and the dimension of $K[x_1, \ldots, x_n]$ can be shown to be n. This is one of the most important invariants of a ring. We will restrict our focus to finite dimensional rings for the remainder of today (and possibly the course).

Definition 0.2. A local ring $(R, \mathfrak{m})$ is **regular** (or a **regular local ring**, or **RLR**) if $\mathfrak{m}$ is generated minimally by exactly $\dim(R)$ many elements.

We note that in general, we can compute the number of generators in this setting quite naturally:

Proposition 0.3. *If $(R, \mathfrak{m})$ is a local ring,*

$$\beta(\mathfrak{m}) = min\{n \mid \mathfrak{m} = \langle f_1, \ldots, f_n \rangle\} = \dim_{R/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2)$$

Proof. By Nakayama's Lemma++, we know that generators of $\mathfrak{m}$ correspond directly with those of $\mathfrak{m}/\mathfrak{m}\cdot\mathfrak{m} = \mathfrak{m}/\mathfrak{m}^2$. Therefore, the minimal number of generators of one corresponds precisely to those of the other. □

We think of $\mathfrak{m}/\mathfrak{m}^2$ as the cotangent space of R at $\mathfrak{m}$. Another very important thing to note is that $dim(R) \leq \beta(\mathfrak{m})$, so being regular is stating a minimality of the generating set of $\mathfrak{m}$. This follows from the following theorem:

Theorem 0.4 (Principal Ideal Theorem)**.** *If $x_1, \ldots, x_c$ are elements of a ring R, then if $I = \langle x_1, \ldots, x_c \rangle$, the* **codimension** *or* **height** *of I is*

$$\operatorname{codim}(I) = ht(I) := \min\{\dim(R_\mathfrak{p}) \mid I \subseteq \mathfrak{p} \text{ is prime}\} \leq c$$

I will black box this proof for now, as it takes some work and machinery. However, we note that for a local ring $(R, \mathfrak{m})$, $\operatorname{codim}(\mathfrak{m}) = \dim(R)$. So this equality gives us directly that $dim(R) \leq \beta(\mathfrak{m})$. Even moreso, it gives that $R/\langle x_1, \ldots, x_i \rangle$ has dimension $\dim(R) - i$. We will now explore some nice properties of regular local rings, by use of Krull's Intersection Theorem.

Theorem 0.5 (Krull's Intersection Theorem)**.** *Let R be a Noetherian ring and let $I \subsetneq R$ be an ideal. If M is a finitely generated R-module, then $\cap_{n \geq 0} I^n M = 0$*

I will prove this momentarily, but first some nice semi-corollaries.

Proposition 0.6. *If $(R, \mathfrak{m})$ is a regular local ring of dimension d, then considering the* **graded Algebra** *of $\mathfrak{m}$, we have*

$$gr_\mathfrak{m}(R) := R/\mathfrak{m} \oplus \mathfrak{m}/\mathfrak{m}^2 \oplus \mathfrak{m}^2/\mathfrak{m}^3 \oplus \ldots \cong (R/\mathfrak{m})[X_1, \ldots, X_d]$$

Proof. Given $\mathfrak{m} = \langle x_1, \ldots, x_d \rangle$, we know that $\mathfrak{m}^n$ is generated by elements of the form $x_1^{n_1} \cdots x_n^{n_d}$ where $n = n_1 + \ldots + n_d$. Therefore, there is a natural surjection

$$(R/\mathfrak{m})[X_1, \ldots, X_d] \to gr_{\mathfrak{m}}(R)$$

Moreover, this map is injective by Krull's Intersection Theorem. This completes the proof. □

Proposition 0.7. *Every regular local ring R is an integral domain.*

Proof. We will use crucially that $\cap_{n \geq 0} \mathfrak{m}^n = 0$, which holds as a result of the Krull Intersection Theorem, to be seen momentarily. Suppose that $f \cdot g = 0$. Then there exists $a, b \geq 0$, we have $f \in \mathfrak{m}^a, g \in \mathfrak{m}^b$, but not in any larger power. Proposition 0.6 then implies that since $0 = f \cdot g \in \mathfrak{m}^{a+b+1}$, that $f \in \mathfrak{a}^{a+1}$ or $g \in \mathfrak{m}^{b+1}$. This contradicts our assumptions. □

I will now prove Krull's Intersection Theorem.

Lemma 0.8 (Artin-Rees Lemma)**.** *Suppose R is a Noetherian ring, and $I \subseteq R$ is an ideal. Let $N \subseteq M$ be two finitely generated R-modules. Then there exists $c > 0$ such that*

$$I^n M \cap N = I^{n-c}(I^c M \cap N)$$

for every $n \geq c$.

Proof. Consider the **blowup algebra** of I:

$$bl_I(R) = R \oplus I \oplus I^2 \oplus I^3 \oplus \ldots = \oplus_{n \geq 0} I^n$$

where we multiply elements of I^n and I^m into I^{n+m}. If $I = \langle f_1, \ldots, f_t \rangle$, then $bl_I(R)$ is Noetherian, since it is a quotient of the Noetherian ring $R[X_1, \ldots, X_t]$ by $X_i \mapsto f_i$. Similarly, we may consider

$$bl_I(M) = M \oplus IM \oplus I^2 M \oplus I^3 M \oplus \ldots = \oplus_{n \geq 0} I^n M$$

This is certainly a finitely generated $bl_I(R)$-module. This yields the following submodule:

$$\oplus_{n \geq 0} I^n M \cap N$$

This is a finitely generated S-module as well. Take $\alpha_i = \alpha_i^0 + \ldots + \alpha_i^{n_i}$ generators (decomposed into their direct sums). Set $c = \max_i\{n_i\}$. Then for $n \geq c$. Then for every $n \geq c$, every element has the form

$$\sum_{i,j} h_j \alpha_i^j \text{ where } h_j \in I^{n-j} \subseteq I^{n-c}$$

This implies that $I^n M \cap N \subseteq I^{n-c}(I^c M \cap N)$. The other direction is left as an exercise. □

Finally, we conclude Krull:

Proof. Let $N = \cap_{n \geq 0} I^n M$. Then $N = I^n M \cap N$ for all $n \geq 0$. By Artin-Rees, we get

$$N = I^n M \cap N \subseteq IN$$

for some suitably large power of n. But Nakayama's Lemma then implies $N = 0$. □

Next time we will talk briefly about global dimension and it's relation to regularity.

CLASS 18, MONDAY APRIL 9TH: REGULAR RINGS AND GLOBAL DIMENSION

We have already seen some nice properties of regular local rings. Today I will extend several notions of the previous lecture to more arbitrary rings. In the process, some hands will be waived for the sake of time. Resources are available for those interested.

Definition 0.1. A Noetherian ring R is said to be **regular** if for every prime ideal $\mathfrak{p} \subseteq R$, $R_{\mathfrak{p}}$ is a regular local ring (as defined last class).

This is a nice definition, since it makes regularity a local property. However, there is one problem that remains unanswered: Is a regular local ring a regular ring? This is true, yet unclear as of now; how can you ensure every localization at $\mathfrak{p} \subseteq \mathfrak{m}$ is regular?

We will assume throughout all rings are Noetherian. We need a few extra definitions to resolve this question (in the affirmative):

Definition 0.2.

1) A sequence $x_1, x_2, \ldots, x_n$ is called a R-**regular sequence** if each x_i is a NZD for $R/\langle x_1, \ldots, x_{i-1}\rangle$, and $R/\langle x_1, \ldots, x_n\rangle \neq 0$. We can do the analogous thing for a module M.

2) The **depth** of a module M is exactly the length of the longest M-regular sequence.

3) A ring R is called **Cohen-Macaulay** or **CM** if $\operatorname{depth}(R) = \dim(R)$. Note that we always have $\operatorname{depth}(R) \leq \dim(R)$.

4) If R is a ring, and M is an R-module, the **projective dimension** of M is

$$\operatorname{pdim}_R(M) = \inf\{n \mid \exists 0 \to P_n \to \ldots \to P_0 \to M \to 0 \text{ a projective resolution}\}.$$

We can analogously define the **injective dimension**.

5) The **global dimension** of a ring R is

$$\text{gl-dim}(R) = \sup\{\operatorname{pdim}_R(M) \mid M \text{ is an } R\text{-module}\}.$$

Example 0.3.

- Given an RLR $(R, \mathfrak{m})$ with $\mathfrak{m} = \langle x_1, \ldots, x_n\rangle$, then $x_1, \ldots, x_n$ form a regular sequence on R. Thus an RLR is Cohen-Macaulay.
- $R = K[x^2, x^3] \cong K[X, Y]/\langle X^3 - Y^2\rangle$ is Cohen-Macaulay, but not regular. It is not regular because $R_{\langle x^2, x^3\rangle}$ has maximal ideal $\langle x^2, x^3\rangle$, and this can't be generated by 1 element (exercise). But $R \subseteq K[x]$ is an integral extension, so $\dim(R) = 1$.
  On the other hand, $\operatorname{depth}(R) = 1$, since x^2 is a length 1 regular sequence.
- The following ring is not CM:

$$R = K[x, y, u, v]/\langle x, y\rangle \cap \langle u, v\rangle = K[x, y, u, v]/\langle xu, yu, xv, yv\rangle$$

It is left as a homework exercise to check that $\dim(R) = 2$ and $\operatorname{depth}(R) = 1$.

- If P is projective, $\text{pdim}_R(P) = 0$ since $0 \to P \to P \to 0$ is exact. So it is natural to think lower projective dimension implies more projective.
- Consider the ring $R = K[x,y]/\langle xy \rangle$ and $M = K[x] = R/\langle y \rangle$. We have a projective resolution
$$\ldots \xrightarrow{\cdot x} R \xrightarrow{\cdot y} R \xrightarrow{\cdot x} R \xrightarrow{\cdot y} R \to M \to 0$$
via localization at $\langle x, y \rangle$, we can furthermore see that there is no finite projective resolution of M. Therefore, $\text{pdim}_R(M) = \text{gl-dim}(R) = \infty$.

This last fact is part of an important characterization of RLRs.

Theorem 0.4. *A local ring $(R, \mathfrak{m})$ is regular if and only if R has finite global dimension. In this case,* $\text{gl-dim}(R) = \dim(R)$.

Caution: This does NOT hold without the local hypothesis. This is usually shown with the following two lemmas:

Lemma 0.5. *Let $(R, \mathfrak{m})$ be a local ring. Then the following inequality holds:*
$$\text{pdim}_R(R/\mathfrak{m}) \geq \dim_{R/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2) \geq \dim(R)$$

Lemma 0.6. *Let $(R, \mathfrak{m})$ be a local ring. If $R/\mathfrak{m}$ has finite* $\text{pdim} = n$, *then* $\dim(R) \geq n$. *Thus if $(R, \mathfrak{m})$ is regular,* $\dim(R) = \text{pdim}_R(R/\mathfrak{m})$. *Otherwise,* $\text{gl-dim}(R) = \infty$.

Finally, coupled with Nakayama's lemma, one can show that $\text{pdim}(M) \leq \text{pdim}(R/\mathfrak{m})$ for any M. These elements completes the proof of Theorem 0.4.

Given these results, one can resolve the question issued above:

Theorem 0.7. *A regular local ring satisfies Definition 0.1, and therefore is itself regular.*

Proof. Let $(R, \mathfrak{m})$ be a local ring, and let $\mathfrak{p}$ be a prime ideal. Let M be an $R_\mathfrak{p}$-module. This gives it the structure of an R-module via the localization map $R \to R_\mathfrak{p}$. Therefore, we can construct a projective resolution of M as an R-module. We know that R has finite projective dimension, so
$$0 \to R^{m_n} \to R^{m_{n-1}} \to \ldots \to R^{m_0} \to M \to 0$$
where $n = \dim(R)$.[1] But we can localize this sequence at $\mathfrak{p}$:
$$0 \to R_\mathfrak{p}^{m_n} \to R_\mathfrak{p}^{m_{n-1}} \to \ldots \to R_\mathfrak{p}^{m_0} \to M_\mathfrak{p} \to 0$$
But from the universal property of localization (Class 10, Theorem 0.2), we have $M_\mathfrak{p}$ is the unique smallest R-module with a homomorphism from M for which elements of $R \setminus \mathfrak{p}$ are inverted. However, note that if $r \in R \setminus \mathfrak{p}$,
$$r \cdot M = (1, r)M = (1, r)(r, 1)M = M$$
So r acts as a unit on M. This shows that $M \cong M_\mathfrak{p}$. Therefore, the above resolution looks like
$$0 \to R_\mathfrak{p}^{m_n} \to R_\mathfrak{p}^{m_{n-1}} \to \ldots \to R_\mathfrak{p}^{m_0} \to M \to 0$$
So M has finite projective dimension, bounded above by $n = \dim(R)$, and M was arbitrary implies $\text{gl-dim}(R_\mathfrak{p}) \leq n$, and thus $R_\mathfrak{p}$ is a RLR as desired. □

We now have most of the desired resources to proceed to some positive characteristic commutative algebra, which we will start Friday.

[1] Every projective is free since R is local!

CLASS 19, FRIDAY APRIL 13TH: CHARACTERISTIC AND THE FROBENIUS

We now have a lot of the prerequisite material required to begin studying some of the most important properties of rings in positive characteristic. To begin, I will start by reviewing (from the Day 1 introduction) the notion of characteristic, and then issuing some of the various notations surrounding the Frobenius.

Rings come in many flavors. As mentioned on the first day, one of the most basic invariants is whether it is equal characteristic or mixed characteristic.

Definition 0.1. We define the **characteristic** of a ring R to be the smallest $n > 0$ such that $1+ \overset{n-times}{\cdots\cdots} +1 = 0$. If there is no such positive n, the characteristic is set to 0. Generally, we write $\mathrm{char}(R) = n$ to represent this quantity.

A ring R is called **equal characteristic** n if there exists a field K such that $K \hookrightarrow R$ and such that $\mathrm{char}(K) = n$. Otherwise, we say the ring is **mixed characteristic**.

Sometimes the **equal** is dropped. All rings fall into one of these categories:

Proposition 0.2. *A ring R is equal characteristic 0 if and only if $\mathbb{Q} \subseteq R$. A ring is characteristic $p > 0$, where p is a prime number, if and only if $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \subseteq R$. All other rings are mixed characteristic, which holds if and only if $\mathrm{char}(R) \neq \mathrm{char}(R/\mathfrak{m})$ for some maximal ideal $\mathfrak{m}$.*

Proof. See homework 5. □

Example 0.3.

- $\mathbb{Z}$ is a ring of mixed characteristic. Indeed, it does not contain a field. Moreover, we note that $R/\mathfrak{m}$ can be a field of any possible characteristic.
- $R = \mathbb{Z}_{\langle p \rangle}$ is a local ring of mixed characteristic. R itself is characteristic 0, where as $R/\mathfrak{m} \cong \mathbb{Z}/p\mathbb{Z}$ has characteristic p.
- $R[x_1, x_2, \ldots, x_n]$ and R are either both mixed characteristic or equal characteristic. In the second case, we can also consider $R[x_1, x_2, \ldots, x_n]/I$ where I is any proper ideal.
- As a corollary of the previous statement, $\mathbb{C}[x_1, x_2, \ldots, x_n]$ is equal characteristic 0 and $\mathbb{F}_p[x_1, x_2, \ldots, x_n]$ is equal characteristic p.
- $\mathbb{Z}/n\mathbb{Z}$ with n composite is mixed characteristic. Indeed, it does not contain a field and has characteristic n vs. characteristic p_i for all quotients by $\mathfrak{m}$, where $n = p_1^{e_1} \cdots p_m^{e_m}$.

Here is a theorem that is commonly proven in an abstract algebra or Galois theory course:

Theorem 0.4. *Any finite field has cardinality $q = p^e$, where p is a prime number. Moreover, there is a unique field of such cardinality, which can be thought of as formally adjoining the roots of the (splitting) polynomial $x^q - x$ over $\mathbb{F}_p$ to $\mathbb{F}_p$. Finally, the algebraic closure is the union of all such fields:*

$$\overline{\mathbb{F}_p} = \cup_{n \geq 0} \mathbb{F}_{p^e}$$

Proof. Given Proposition 0.2, and $\mathbb{Q}$ is infinite, we know finite field K has characteristic $p > 0$ prime. Therefore, $\mathbb{F}_p \subseteq K$. This makes K into an $\mathbb{F}_p$-module, or vector space, so $K \cong \mathbb{F}_p^e$ for some $e > 0$. Therefore, $|K| = p^e$.

If K, L are two such fields, we know that they are isomorphic as $\mathbb{F}_p$-modules (in many ways). Furthermore, we can consider $K^\times$ and $L^\times$, the group of non-zero elements under multiplication. Every element satisfies $x^{p^e-1} = 1$ because that is the order of the groups. If we put 0 back in, we see that the roots are necessarily those satisfying $x^{p^e} - x$. This shows $K \cong L$.

Finally, the algebraic closure of a field is always the union of all the algebraic extensions of the field, which are precisely those represented above. □

Caution: $\mathbb{F}_{p^e} \subseteq \mathbb{F}_{p^{e'}}$ if and only if $e|e'$ (not if $e \leq e'$). Also as noted, not all positive characteristic fields are finite. We have $\overline{\mathbb{F}_p}$ as an example already, and others include $\mathbb{F}_p(x)$, the rational functions with coefficients in $\mathbb{F}_p$.

We can now begin talking of the Frobenius morphism:

Definition 0.5. If R is a ring of characteristic $p > 0$, then the ring homomorphism

$$F : R \to R : r \mapsto r^p$$

is called the **Frobenius**.

This can be iterated, to produce $F^e = F \circ \overset{e-times}{\cdots\cdots} \circ F$. As noted (on day 1), this is a homomorphism of rings:

$$(r+s)^p = r^p + pr^{p-1}s + \ldots + \binom{p}{i} r^{p-i}s^i + \ldots + prs^{p-1} + s^p \equiv r^p + s^p$$

$$(rs)^p = r^p s^p$$

However, this quite obviously is not a R-module homomorphism:

$$(rs)^p = r^p s^p \neq r(s)^p = rs^p$$

There are a few ways to get around this:

1) We can think about R^p as a ring, containing only p^{th} powers of elements of R. In this case, the Frobenius can be viewed as the inclusion $R^p \subseteq R$.
2) We can similarly think of $R^{\frac{1}{p}}$ of formal p^{th} roots of elements of R. The Frobenius is then the inclusion $R \subseteq R^{\frac{1}{p}}$.
3) We can write F_*R for the range of the Frobenius: $F : R \to F_*R$. F_*R is an R-module which is R as an additive abelian group, but with multiplicative structure $r \cdot s = r^p s$. If confusion can arise, sometimes we write F_*s for s, and $rF_*s = F_*r^p s$.

I end today's lecture by demonstrating that the Frobenius gives some small information about the ring (also mentioned day 1):

Proposition 0.6. *If R is a ring of characteristic $p > 0$, then $F : R \to R$ is injective if and only if R is reduced (e.g. the nilradical $\mathcal{N} = 0$).*

Proof. See homework 5. □

CLASS 20, MONDAY APRIL 16TH: FUN WITH FROBENIUS

Today we will play around with F_* and see what can be drawn out. Some things fall out quite naturally from the definition.

Proposition 0.1. *The map $F : R \to F_*R$ induces a bijection of prime ideals.*

Proof. I claim that the bijection is given by $F^{-1}(\mathfrak{p}) \leftarrow\!\shortmid F_*\mathfrak{p}$ and $\mathfrak{p} \mapsto \sqrt{\mathfrak{p} \cdot F_*R}$.

Let $\mathfrak{p} \subseteq R$ be a prime ideal. Then if $F_*a \cdot F_*b \in \sqrt{\mathfrak{p} \cdot F_*R}$, this implies that $F_*a \cdot F_*b = F_*c^n$ for some $c \in \mathfrak{p}$. But this implies that

$$F_*a^p \cdot F_*b^p = a \cdot b = c^{np} \in \mathfrak{p}$$

Therefore, either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$, which implies $F_*a \in \sqrt{\mathfrak{p} \cdot F_*R}$ or $F_*b \in \sqrt{\mathfrak{p} \cdot F_*R}$, as desired.

Finally, it goes to show that they are mutually inverse to one another. It is clear that $F^{-1}(\sqrt{\mathfrak{p} \cdot F_*R}) = \mathfrak{p}$. On the other hand, if $\mathfrak{p} \subseteq F_*R$ is prime, $F^{-1}(\mathfrak{p}) = \{a \in R \mid a^p \in \mathfrak{p}\} = \mathfrak{p}$. So this is in fact a bijection. □

This brings about a nice idea: studying how F_* behaves on modules. As a lemma, we can see how it behaves on ideals.

Lemma 0.2. *If I is an ideal of R, then $F(I) = I \cdot F_*R \cong F_*I^{[p]}$, where $I^{[p]}$ is the ideal consisting of p^{th} powers of elements of I. We can also characterize it in terms of generators: if $I = \langle a_1, \ldots, a_n \rangle$, then $I^{[p]} = \langle a_1^p, \ldots, a_n^p \rangle$.*

Proof. The first claim is completely definitional. For the second part, if $a \in I$, then

$$a = r_1a_1 + \ldots + r_na_n$$

$$a^p = r_1^pa_1^p + \ldots + r_n^pa_n^p$$

Therefore, $F_*a^p = r_1F_*a_1^p + \ldots + r_nF_*a_n^p \in \langle a_1^p, \ldots, a_n^p \rangle$. So $I^{[p]} \subseteq \langle a_1^p, \ldots, a_n^p \rangle$. On the other hand, $I^{[p]}$ certainly contains a_i^p, so equality is achieved. □

Now, I make a very natural observation: If M is an R-module, we can form F_*M as the module M as an Abelian group, but having $r \cdot m = r^pm$. This makes F_* into a functor from R-modules to R-modules: $F_*\varphi : F_*m \mapsto F_*\varphi(m)$.

Proposition 0.3. *Let $0 \to M' \to M \to M'' \to 0$ be a SES. Then so is*

$$0 \to F_*M' \to F_*M \to F_*M'' \to 0$$

That is to say, F_* is an exact functor.

Next up, I would like to get a handle on how complicated F_*R is as an R-module. On the surface, it seems quite docile, being isomorphic to R as Abelian groups. However, things can get quite complication. As an issue, sometimes F_*R is not even finitely generated as an R-module, even when R is Noetherian or even a field (cf Homework 5). Therefore, we make the following definition:

Definition 0.4. A Noetherian ring R of positive characteristic is called **F-finite** if F_*R is a finitely generated R-module.

Notation 0.5. For the rest of the course, R will be a Noetherian F-finite ring of positive characteristic $p > 0$. If $(R, \mathfrak{m})$ is written, we add the local condition. If $(R, \mathfrak{m}, k)$ is written, $(R, \mathfrak{m})$ is local and $k = R/\mathfrak{m}$.

Because they make things somewhat *perfect* for our study, I introduce the following notion:

Definition 0.6. A field K is called **perfect** if (it is characteristic 0 or) the map $F : K \to F_*K$ is surjective (it is always injective, thus an isomorphism). Otherwise, K is called **imperfect**.

This notion naturally extends to the notion of a **perfect ring**. We can also always take the perfection of a field (or ring), which is usually denoted $k^{\frac{1}{p^\infty}}$ or k_∞. This exists as it can be identified with the union of $F_*^e K$ for all $e \geq 0$.

Proposition 0.7. *Any $\mathbb{F}_q$ is a perfect field for $q = p^e$.*

Proof. We need to show that F is surjective. Take $0 \neq x \in \mathbb{F}_q$ ($0 \mapsto 0$ of course). Since $x \in \mathbb{F}_q^\times$, we know that the order of x, say d, divides $p^e - 1$. But p and $p^e - 1$ are relatively prime, so $\gcd(p, d) = 1$. Therefore, there is an integer equation $mp + nd = 1$. Therefore

$$x = x^1 = x^{mp+nd} = x^{pm}x^{nd} = x^{pm} = (x^m)^p$$

So $x = F(x^m) \in \mathrm{im}(F)$. But x was arbitrary, so we are done. □

Example 0.8. Consider the ring $R = K[x]$ where K is a perfect field. If we consider the module F_*R, we can see that

$$F_*a = \sum_{n \geq 0} F_* a_i x^i$$

for $a_i \in K$. Doing a small bit of combinatorics, we note that by the division algorithm, there exists a unique m and $r = 0, 1, \ldots, p-1$ such that $n = mp + r$ (say $m = \lfloor \frac{n}{p} \rfloor$ and r their difference, where $\lfloor - \rfloor$ is the floor function, or the integer part). Therefore, we can rewrite

$$F_*a = \sum_{m \geq 0} \sum_{r=0}^{p-1} F_* a_{mp+r} x^{mp+r} = \sum_{m \geq 0} \sum_{r=0}^{p-1} a_{mp+r}^{\frac{1}{p}} x^m F_* x^r$$

where $a_{mp+r}^{\frac{1}{p}}$ is the standard notation for the unique element b such that $b^p = a_{mp+r}$. This demonstrates F_*x^r for $r = 0, \ldots, p-1$ is a basis for F_*R as an R-module. Therefore F_*R is free:

$$F_*R \cong R^{\oplus p}$$

Example 0.9. Let $R = K[x^2, x^3]$ be the CM ring which is not regular (from class 18), and K perfect. Let's examine F_*R. I specialize to the case of $\mathrm{char}(K) = 3$ and leave the general case to the ambitious student.

In this case, we see that a generating set of F_*R over R is

$$F_*1, F_*x^2, F_*x^3, F_*x^4, F_*x^5, F_*x^7$$

This can be demonstrated explicitly. Thus R is F-finite. Moreover, localizing at the origin, we can show that all of these generators are necessary by degree arguments. So if F_*R was projective, $F_*R_{\langle x^2, x^3 \rangle} \cong R^6_{\langle x^2, x^3 \rangle}$. However, we can further localize at 0 to conclude $F_*K(x) \cong K(x)^6$, which is certainly not true by Example 0.8.

We will explore this relationship via Kunz Theorem next time.

CLASS 21, WEDNESDAY APRIL 18TH: Tor_i^R

We have already noted the importance of flat modules; they allow us to conclude all modules inject into an injective R-module. Today we will study how close a module is to being flat. We will use some homological methods.

Definition 0.1. If M is an R-module, we have already talked about how we can take a free resolution of M producing an exact sequence

$$\cdots \xrightarrow{\psi_3} R^{\lambda_2} \xrightarrow{\psi_2} R^{\lambda_1} \xrightarrow{\psi_1} R^{\lambda_0} \longrightarrow M \to 0$$

We can tensor this sequence with N and produce

$$\cdots \xrightarrow{\psi_3 \otimes 1_N} R^{\lambda_2} \otimes_R N \xrightarrow{\psi_2 \otimes 1_N} R^{\lambda_1} \otimes_R N \xrightarrow{\psi_1 \otimes 1_N} R^{\lambda_0} \otimes_R N \xrightarrow{\psi_0 \otimes 1_N} 0$$

This sequence is no longer exact (unless N was flat to begin with). However, we do maintain the inclusion $\ker(\psi_i \otimes 1_N) \supseteq \mathrm{im}(\psi_{i+1} \otimes 1_N)$. Therefore, we measure

$$\mathrm{Tor}_i^R(M, N) = \ker(\psi_i \otimes 1) / \mathrm{im}(\psi_{i+1} \otimes 1)$$

An important note is that this is independent of the chosen free resolution. The primary advantage of Tor is that it defines a LES for the tensor product:

Theorem 0.2. *If $0 \to M' \to M \to M'' \to 0$ is a SES, then the following is exact:*

$$\begin{array}{rrrr} \cdots \longrightarrow & \mathrm{Tor}_2^R(M, N) \longrightarrow & \mathrm{Tor}_2^R(M'', N) \longrightarrow & \\ \mathrm{Tor}_1(M', N) \longrightarrow & \mathrm{Tor}_1^R(M, N) \longrightarrow & \mathrm{Tor}_1^R(M'', N) \longrightarrow & \\ M' \otimes_R N \longrightarrow & M \otimes_R N \longrightarrow & M'' \otimes_R N \longrightarrow & 0 \end{array}$$

This theorem allows us complete the SES corresponding to a tensor, since it is only in general right exact. The proof of this theorem requires us to use the snake lemma and complete a free resolution of M' and M'' to one for M. I recommend reading about this proof independently.

To make this more succinct, I make the following note:

Proposition 0.3. *Consider R-modules M, N. Then*

$$M \otimes_R N \cong \mathrm{Tor}_0^R(M, N)$$

Proof. Note that we have a right exact sequence

$$R^{\lambda_1} \xrightarrow{\psi_1} R^{\lambda_0} \longrightarrow M \to 0$$

Therefore, tensoring with N maintains this:

$$R^{\lambda_1} \otimes_R N \xrightarrow{\psi_1 \otimes 1_N} R^{\lambda_0} \otimes_R N \to M \otimes N \to 0$$

This implies

$$M \otimes N \cong R^{\lambda_0} / \mathrm{im}(\psi_1 \otimes 1_N) \cong \ker(\psi_0 \otimes 1_N) / \mathrm{im}(\psi_1 \otimes 1_N) = \mathrm{Tor}_0^R(M, N)$$

□

Here is the theorem that represents the importance of Tor explicitly.

Theorem 0.4. *The following are equivalent:*

1) N is a flat R-module.
2) $\mathrm{Tor}_1^R(M,N)=0$ for all R-modules M.
3) $\mathrm{Tor}_i^R(M,N)=0$ for all R-modules M and $i\geq 1$.

Proof. 1) $\Leftrightarrow$ 2): Given Theorem 0.2, we have an exact sequence

$$\mathrm{Tor}_1(M'',N)\to M'\otimes_R N\to M\otimes_R N\to M''\otimes_R N\to 0$$

Therefore, the desired SES holds if and only if $\mathrm{Tor}_1(M'',N)=0$. Additionally, every M'' can be surjected onto by a free module, so M'' can always appear in such a SES sequence.

3) $\Rightarrow$ 2) Obvious.

1) $\Rightarrow$ 3) Given M is flat, we see that

$$\cdots \xrightarrow{\psi_3\otimes 1_N} R^{\lambda_2}\otimes_R N \xrightarrow{\psi_2\otimes 1_N} R^{\lambda_1}\otimes_R N \xrightarrow{\psi_1\otimes 1_N} R^{\lambda_0}\otimes_R N\to M\otimes N\to 0$$

is an exact sequence. Therefore, $\ker(\psi_i\otimes 1_N)=\mathrm{im}(\psi_{i+1}\otimes 1_N)$ for all $i\geq 1$, or equivalently, $\mathrm{Tor}_i^R(M,N)=\ker(\psi_i\otimes 1_N)/\mathrm{im}(\psi_{i+1}\otimes 1_N)=0$. □

Another important remark is that Tor_i is symmetric:

Proposition 0.5.

$$\mathrm{Tor}_i^R(M,N)\cong \mathrm{Tor}_i^R(N,M)$$

This requires tensoring together a free resolution of M with one for N, then taking the total complex. This shares homology with both complexes simultaneously, and therefore allows one to conclude the desired isomorphism. Now onto some examples:

Example 0.6. $\mathbb{Q}$ is a flat $\mathbb{Z}$-module which is not projective (not locally-free). However, $\mathbb{Q}$ is a flat $\mathbb{Z}$-module since it is torsion-free over a PID. So we can look at the short exact sequence

$$0\to\mathbb{Z}\to\mathbb{Q}\to\mathbb{Q}/\mathbb{Z}\to 0$$

which induces an exact sequence

$$0=\mathrm{Tor}_1^R(\mathbb{Q},D)\to\mathrm{Tor}_1(\mathbb{Q}/\mathbb{Z},D)\to\mathbb{Z}\otimes D\to\mathbb{Q}\otimes D\to\mathbb{Q}/\mathbb{Z}\otimes D\to 0$$

for a given module D. Therefore, $\mathrm{Tor}_1(\mathbb{Q}/\mathbb{Z},D)=\ker(\mathbb{Z}\otimes D\to\mathbb{Q}\otimes D)$. This is precisely the torsion subgroup of D.

CLASS 22, FRIDAY APRIL 20TH: KUNZ THEOREM I

We have already spoken about how nice regular rings are in commutative algebra, with every module having finite projective dimension. In fact, they are the commutative algebraic analog of smooth manifolds from differential geometry. Today, we give a classical yet extremely powerful way to detect regularity in positive characteristic.

Theorem 0.1 (Kunz's Theorem)**.** *Let R be an F-finite ring. Then R is regular if and only if F_*R is a flat module.*

We can use some of the previous results to apply the following characterization:

Theorem 0.2 (Local Kunz's Theorem)**.** *If R is a local F-finite ring, then R is an RLR if and only if F_*R is a free R-module.*

We have already indicated the following implications for R-modules:

$$\text{Free} \Rightarrow \text{Projective} \Rightarrow \text{Flat} \Rightarrow \text{Torsion-free}$$

We additionally have the following under additional conditions (R Noetherian):

$$\text{Free} \overset{R \text{ local}}{\Longleftarrow} \text{Projective} \overset{\text{f.g.}}{\Longleftarrow} \text{Flat} \overset{\text{Dedekind}}{\Longleftarrow} \text{Torsion-free}$$

To make Local Kunz sufficient for Kunz, we need to prove Projective $\overset{\text{f.g.}}{\Longleftarrow}$ Flat. Suppose M is flat. We may assume $(R, \mathfrak{m})$ is a local ring. Choose $\langle m_1, \ldots, m_n \rangle$ a minimal generating set for M. Then we get a surjection $R^n \to M$. We can expand to a SES and tensor with $R/\mathfrak{m}$ to yield a SES

$$0 \to K \otimes_R R/\mathfrak{m} \to R^n \otimes_R R/\mathfrak{m} \to M \otimes_R R/\mathfrak{m} \to 0$$

The zero on the left comes from the fact that M is flat (which implies $\operatorname{Tor}_1^R(M, R/\mathfrak{m}) = 0$). Since the generating set was chosen minimal, we see that $R^n \otimes R/\mathfrak{m} \to M \otimes R/\mathfrak{m}$ is an isomorphism of vector spaces, implying $K \otimes_R R/\mathfrak{m} = K/\mathfrak{m}K = 0$. By Nakayama's lemma, we see that $K = 0$. Therefore, M is free.

Therefore, it suffices to prove Theorem 0.2. First, we need some information about the completion of a ring.

Definition 0.3. Let $(R, \mathfrak{m})$ be a local ring. We denote $\hat{R}$, called the **completion** of the ring R at $\mathfrak{m}$, to be the inverse limit of the sequence

$$\hat{R} \to \ldots R/\mathfrak{m}^n \to \ldots \to R/\mathfrak{m}^2 \to R/\mathfrak{m} \to 0$$

Alternatively, it is the completion of the metric space R with the $\mathfrak{m}$-adic metric:

$$d(x, y) = 2^{-\max\{n \mid x - y \in \mathfrak{m}^n\}}$$

This is a metric by Krull's intersection theorem.

This can be thought of as an even more local version of localization. $\hat{R}$ is always a faithfully (taking non-zero modules to non-zero modules under tensor) flat R-module. The reason this is important is because regular rings themselves can be quite strange looking:

Example 0.4. The ring $R = K[x,y]/\langle y^2 - x(x-1)(x+1)\rangle$ with $\mathrm{char}(K) > 2$ is a regular ring. This can be seen via the Jacobian criterion.

However, by the following theorem of Cohen, we get a much nicer characterization for complete rings:

Theorem 0.5 (Cohen's Structure Theorem: Regular case)**.** *Suppose that R is a ring containing a field K. Then $\hat{R} = K[\![x_1,\ldots,x_n]\!]/I$. Furthermore, if R is regular, then $\hat{R}$ is a power series ring:*

$$\hat{R} \cong K[\![x_1,\ldots,x_{\dim(R)}]\!]$$

This is a very nice result, and will be used to simplify the proof of Kunz dramatically.

Easy direction. Let R be a regular F-finite ring. As a result of Cohen's structure theorem, we note that $\hat{R} \cong K[\![x_1,\ldots,x_d]\!]$. Now, we can apply F_* to get the following commutative diagram:

$$\begin{array}{ccc} \hat{R} & \xrightarrow{F} & F_*\hat{R} \\ \uparrow & & \uparrow \\ R & \xrightarrow{F} & F_*R \end{array}$$

As mentioned, the extension $R \subseteq \hat{R}$ is flat, and given $F_*\hat{R} \cong \hat{F_*R}$, we see the the right arrow is flat as well. I now demonstrate that $F_*\hat{R}$ is flat as a $\hat{R}$-module. Notice that

$$\hat{R} = K[\![x_1,\ldots,x_n]\!] \subseteq (F_*K)[\![x_1,\ldots,x_n]\!] \subseteq F_*K[\![x_1,\ldots,x_n]\!] = F_*\hat{R}$$

The first extension is free: given R is F-finite, we see K is as well. Therefore, there is a basis of F_*K over K consisting of $F_*k_1 = F_*1,\ldots,F_*k_m$. This implies directly that

$$(F_*K)[\![x_1,\ldots,x_n]\!] = \bigoplus_{i=1}^{m} F_*k_i \cdot \hat{R} \cong \hat{R}^n$$

Now, if we apply the same analysis of Homework 5, problem 7, we see that $F_*\hat{R} = F_*K[\![x_1,\ldots,x_n]\!]$ is a free $(F_*K)[\![x_1,\ldots,x_n]\!]$-module of rank N. Combining these 2 pieces of data, we see that

$$F_*\hat{R} \cong ((F_*K)[\![x_1,\ldots,x_n]\!])^N \cong (\hat{R}^m)^N \cong \hat{R}^{mN}$$

In particular, we note that $F_*\hat{R}$ is a flat $\hat{R}$-module. Now, consider an injection $M \subseteq N$ of R-modules. Suppose that $F_*R \otimes_R M \not\subseteq F_*R \otimes_R N$. Let K be its kernel. We can now apply the exact functor $- \otimes_{F_*R} F_*\hat{R}$:

$$\begin{array}{ccccccc} 0 & \longrightarrow & K \otimes_{F_*R} F_*\hat{R} & \longrightarrow & M' \otimes_R F_*R \otimes_{F_*R} F_*\hat{R} & \longrightarrow & M' \otimes_R F_*R \otimes_{F_*R} F_*\hat{R} \\ & & \updownarrow\cong & & \updownarrow\cong & & \updownarrow\cong \\ 0 & \longrightarrow & K \otimes_{F_*R} F_*\hat{R} & \longrightarrow & M' \otimes_R F_*\hat{R} & \longrightarrow & M' \otimes_R F_*\hat{R} \end{array}$$

Since $K \neq 0$, $K \otimes_{F_*R} F_*\hat{R} \neq 0$ by faithful flatness. However, $M' \otimes_R F_*\hat{R} \hookrightarrow M' \otimes_R F_*\hat{R}$ since $F_*\hat{R}$ is $\hat{R}$-flat, and $\hat{R}$ is R-flat. Thus, a contradiction is reached. $\square$

CLASS 23, WEDNESDAY APRIL 25: KUNZ THEOREM II

It remains to show that the other direction of Kunz Theorem holds (aka the hard direction). Just to recall:

Theorem 0.1 (Kunz's Theorem)**.** *Let R be an F-finite ring. Then R is regular if and only if F_*R is a flat module.*

We have proved the only if direction of this Theorem already. What remains to prove is if F_*R is a flat module, then R is regular. The original proof due to Kunz was lengthy and chased elements around. The proof I will exhibit here uses more advanced techniques with the result of a shortened proof.

Definition 0.2. If R is a ring of characteristic $p > 0$, then we can consider the sequence

$$R \to F_*R \to F_*^2R \to \dots$$

The **perfection** of a ring, denoted R^∞ or $F_*^\infty R$, is the direct limit of this sequence. A ring is called **perfect** if $R = R^\infty$.

If R is reduced, we have that each map above is injective and $F_*^\infty R = \cup_{e\geq 0} F_*^\infty R$. Otherwise, non-reduced elements are set to zero in R^∞, and therefore if $R^\infty = (R/\mathcal{N})^\infty$ satisfies the previous statement. Note that perfections are often Non-Noetherian.

Example 0.3. If $R = K[x]$ with K perfect, then $R^\infty = K[x, x^{\frac{1}{p}}, x^{\frac{1}{p^2}}, x^{\frac{1}{p^3}}, \dots]$. We have the naturally ascending chain of ideals which never stabilizes:

$$0 \subseteq \langle x \rangle \subseteq \langle x^{\frac{1}{p}} \rangle \subseteq \langle x^{\frac{1}{p^2}} \rangle \subseteq \dots$$

A very similar statement holds for $R = K[x_1, \dots, x_n]$.

We can use the following (recent) theorem of Bhatt-Scholze to prove the desired theorem:

Lemma 0.4. *If $S \to R$ and $S \to R'$ are surjections of rings of characteristic $p > 0$, then there are induced surjections $S^\infty \to R^\infty$ and $S \to R'^\infty$. For all $i > 0$, $\operatorname{Tor}_i^{S^\infty}(R^\infty, R'^\infty) = 0$. As a result, $\operatorname{Hom}_{R^\infty}(M, N) \cong \operatorname{Hom}_{S^\infty}(M, N)$.*

They actually prove this result for arbitrary perfect rings, not perfections of rings. This Lemma allows us to prove the desired result. For a proof, consult the professor privately.

Proposition 0.5. *If R is a complete Noetherian local ring, and R^∞ is its perfection, then R^∞ has finite global dimension.*

Proof. Given the assumptions, $R \cong K[\![x_1, \dots, x_n]\!]/I$. Let M be an R^∞-module. Then the proposition implies

$$M \cong M \otimes_{R^\infty} R^\infty \cong M \otimes_{R^\infty} (R^\infty \otimes_{S^\infty} R^\infty) \cong (M \otimes_{R^\infty} R^\infty) \otimes_{S^\infty} R^\infty \cong M \otimes_{S^\infty} R^\infty$$

Now, M is an S^∞-module. Furthermore, we may consider M as an $F_*^e S$-module, since $F_*^e S \to S^\infty$. Furthermore, if we let $M_e = M \otimes_{S^{\frac{1}{p^e}}} S^\infty$, we have maps given by increasing the amount of linearity:

$$M \otimes_S S^\infty \to \dots \to M \otimes_{S^{\frac{1}{p^e}}} S^\infty \to M \otimes_{S^{\frac{1}{p^{e+1}}}} S^\infty \to \dots \to M$$

and that M is the direct limit of M_e. This is because every element of S^∞ is in some $F_*^e S$.

Now, since M is an $S^{\frac{1}{p^e}}$-module, and $S^{\frac{1}{p^e}}$ is a regular ring of dimension n (thus has global dimension n), we have $\operatorname{pdim}_{S^{\frac{1}{p^e}}}(M) \leq n$. However, tensoring the sequence with S^∞ implies that $\operatorname{pdim}_{S^\infty} M_e \leq n$.

Finally, consider the module $M_+ = \oplus_{e \geq 0} M_e$. We can create an endomorphism φ of M_+ by sending $a_e \in M_e$ to $(a_e, -a_e) \in M_e \oplus M_{e+1}$ extended by linearity. The cokernel of φ is isomorphic to M. Therefore, the projective dimension of M is bounded by $n+1$. But M was arbitrary, so $\text{gl-dim}(S^\infty) \leq n+1$. This completes the proof. □

Given the technique of the previous lecture, the assumption of Kunz Theorem is that F_*R is a flat R-module. But this naturally implies $F_*(F_*R) = F_*^2 R$ is a flat F_*R-module, and thus a flat R-module. Therefore, $F_*^e R$ is a flat R-module for any $e \geq 0$. Now, the direct limit is an exact functor, so we can conclude that since $F_*^e R$ is a flat R-module for all e, so too is R^∞. This allows us to conclude the proof of Kunz.

Theorem 0.6. *If R is a complete Noetherian local ring of characteristic $p > 0$ and R^∞ is a flat R-module, then R is a regular ring.*

Note that this is enough to conclude the proof by Cohen's Structure Theorem.

Proof. Note that by Proposition 0.5, we have that every R^∞-module has finite projective dimension. Our assumption implies that $R \to R^\infty$ is faithfully flat, which implies $M \otimes_R R^\infty \neq 0$ if $M \neq 0$.

Let d be the global dimension of R^∞. Suppose that M is a module with projective resolution

$$\ldots \to P_{n+1} \to P_n \to \ldots \to P_0 \to M \to 0$$

Applying $\operatorname{Hom}_R(-, N)$,

$$\ldots \overset{\psi_{n+1}}{\leftarrow} \operatorname{Hom}_R(P_{n+1}, N) \overset{\psi_n}{\leftarrow} \operatorname{Hom}_R(P_n, N) \overset{\psi_{n-1}}{\leftarrow} \ldots \overset{\psi_0}{\leftarrow} \operatorname{Hom}_R(P_0, N) \leftarrow 0$$

Then $\text{gl-dim}(R)$ is the largest (or ∞ if no finite one works) i such that $\ker(\psi_i)/\operatorname{im}(\psi_{i-1}) \neq 0$. This is most commonly called $\operatorname{Ext}_R^i(M, N)$. So assume the desired statement is false, and there is $i > d$ such that $\operatorname{Ext}_R^i(M, N) \neq 0$. Then by flatness,

$$\operatorname{Ext}_R^i(M, N) \otimes_R R^\infty = \operatorname{Ext}_{R^\infty}^i(M \otimes_R R^\infty, N \otimes_R R^\infty)$$

But the extension is faithful, so this is no zero, contradicting the global dimension of R^∞. This completes the proof. □

CLASS 24, FRIDAY APRIL 27: FROBENIUS SPLITTINGS

Last time we finished the proof of the fact that a local ring R is regular in characteristic $p > 0$ if and only if F_*R (and thus $F_*^e R$) is a flat R-module. The Frobenius being able to detect local properties of a ring is extremely valuable in general in characteristic $p > 0$, and has no (or only using very modern methods) analog in characteristic 0 or mixed characteristic. Throughout I assume all rings are F-finite.

Writing this equationally, we have that R is regular local if and only if

$$F_*R \cong R^n \quad \text{for some } n \geq 1$$

So the quickly question becomes how can we allow ourselves some singularities (irregularities) without letting in massively bad ones? An immediate and profitable conclusion would be to weaken the free hypothesis. Maybe F_*R is not entirely composed of Rs, but simply contains one copy of R:

$$F_*R \cong R \oplus M$$

This gives us the following definition:

Definition 0.1. An F-finite ring R of positive characteristic is called **F-split** if and only if there exists an R-module M such that

$$F_*R \cong R \oplus M$$

As we will see a little later, a ring is F-split implies some very nice geometric statements about the ring. First, as with projective and injective modules, I would like to give some equivalent characterizations.

Proposition 0.2. *Let R be a ring of positive characteristic. Then TFAE:*

(1) R is F-split.
(2) $F_*^e R \cong R \oplus M_e$ for **all** *$e > 0$.*
(3) $F_*^e R \cong R \oplus M_e$ for **some** *$e > 0$.*
(4) There exists $\phi : F_*^e R \to R : F_*1 \mapsto 1$ for some (all) $e > 0$.
(5) There exists a surjective R-homomorphism $F_*^e R \to R$ for some (or all) $e > 0$.

Proof. (1) implies (2): Suppose that R is F split. Then note that we can proceed by induction on e. The base case, $e = 1$, is exactly given by (1). For the induction step:

$$F_*^{e+1}R \cong F_*(F_*^e R) \cong F_*(R \oplus M_e) \cong F_*R \oplus F_*M_e \cong R \oplus M \oplus F_*M_e$$

(2) implies (3): Obvious.

(3) implies (4): For the some portion, this is exactly the equivalent definitions of split exact sequences. To convince yourself of the **all** given **some** assumption, if it holds for $F_*^e R \to R$, then for $e' < e$, we have $F_*^{e'} R \to F_*^e R$ induced by the Frobenius, for which clearly $1 \mapsto 1$, and then we can compose with the given map. If $e' > e$, then there exists $m > 1$ such that $me > e'$, then we can use $F_*^{me}\phi : F_*^{me} R \to F_*^{(m-1)e} R$ and induction to conclude that there exists a splitting for $F_*^{e'} R \to R$.

(4) implies (5): Use ϕ.

(5) implies (1): Suppose that there is a surjective map $\phi : F_*R \to R$. I claim we can modify this map to send 1 to 1. Indeed, suppose $\phi(F_*r) = 1$. Then We can consider $\varphi(F_*s) = \phi(F_*(sr))$, obtained by premultiplying by F_*r. This map clearly has the desired property. □

Next up, like regularity, we can show that F-split is a local property:

Proposition 0.3. *R is an F-split ring if and only if $R_{\mathfrak{m}}$ is F-split for all maximal ideals $\mathfrak{m}$.*

Proof. See homework 6. □

As a corollary of this fact, we can say that regular rings are in fact F-split, because we can check the condition locally and use the above observation.

Proposition 0.4. *A ring R that is F-split is also reduced.*

Proof. If $r^n = 0$, then $r^{p^e} = 0$ for some $e > 0$ (for example, $e = n$). But by characterization (4) of Proposition 0.2, we have that there is a a map $\phi : F_*R \to R$ sending 1 to 1. But this implies

$$R \to F_*R \to R : r \mapsto rF_*^e 1 = F_* r^{p^e} \mapsto r$$

But the middle term is 0, so $r = 0$. Thus R is reduced. □

Example 0.5. Consider the ring $R = K[x_1, \ldots, x_n]/\langle x_1 \cdots x_n \rangle$ where K is a perfect field. According to our analysis so far, this has a chance to be F-split (since it is reduced). Let's see if we can prove this is the case.

It is natural to check that a generating set for F_*R as an R-module is

$$\langle F_* x_1^{i_1} \cdots \hat{x_j} \cdots x_n^{i_n} \mid 0 \leq i_k < p \rangle_R$$

where the 'hat' indicates remove this variable from the product (to avoid producing 0). This is not a basis, since R is not regular: $\dim(R) = n-1$, but $\langle x_1, \ldots, x_n \rangle$ is a minimal generating set for the maximal ideal. In particular, some generators have torsion (e.g. $x_1 F_* x_2 \cdots x_n = 0$). However, there is a way to represent elements of F_*R uniquely in this basis (dividing everything into it's $x_1, \ldots, x_n$ degrees). Therefore, we can create a map $\phi : F_*R \to R : F_*1 \mapsto 1$ and all the other generators to 0. This is well defined, surjective, and thus represents an F-splitting of R.

This seemed involved to conclude F-splittings exist. Next time we will simplify this via Fedder's Criterion. Here is one other classical result which yields further examples:

Proposition 0.6. *If $R \subseteq S$ are rings, and there exists $\psi \in \mathrm{Hom}_R(S, R)$ a surjection, then if S is F-split, so is R.*

Proof. $F_*R \hookrightarrow F_*S \xrightarrow{s} S \xrightarrow{\psi} R$ is surjective. □

Example 0.7. We can consider the ring $R = K[x^2, xy, y^2] \subseteq K[x, y] = S$. We can decompose elements of S into even and odd components, and surject the even components onto R (sending odd to 0 for example). S is a regular ring, so it is F-split. Therefore, Proposition 0.6 implies R is F-split.

This generalizes naturally to any number of variables and R a polynomial ring in the degree n monomials; the so-called **Veronese subrings**.

CLASS 25, MONDAY APRIL 30: FEDDER'S CRITERION

A key point from Friday's lecture is that F-split, though a very nice criterion, is slightly tricky to check by hand. So the question becomes how can we simiplify this procedure? This led Fedder to prove a beautiful theorem.

To state the theorem, we need some machinery. We note that by criteria 4 for being F-split, R is F-split if and only if

$$ev_1 : \mathrm{Hom}_R(F_*R, R) \to R : \psi \mapsto \psi(1)$$

is surjective. This naturally motivates studying $\mathrm{Hom}(F_*R, R)$ as an object.

Theorem 0.1. *Let $S = K[x_1, \ldots, x_n]$ be a polynomial ring over an R-finite field K of characteristic $p > 0$. Then there exists $\Phi_S \in \mathrm{Hom}_S(F_*S, S)$ such that Φ is a F_*S-module generator.*

Proof. We can begin by localizing at the origin $\langle x_1, \ldots, x_n \rangle$ without loss of generality. First, note that $\mathrm{Hom}_S(F_*S, S)$ has the natural structure of an S-module and F_*S-module:

$$(s \cdot \Psi)(F_*m) := s\Psi(F_*m) = \Psi(F_*s^p m)$$

$$(F_*s \cdot \Psi)(F_*m) := \Psi(F_*sm)$$

Now, by Kunz Theorem, we know that $F_*S \cong S^l$ for some $l = m \cdot p^n$, where m is the dimension of F_*K over K. We may assume one copy of S is generated by $F_*(x_1^{p-1} \cdots x_n^{p-1})$. I claim that projecting from this copy of S is the desired generator. Call it Φ_S. Indeed, suppose that $\Psi : F_*S \to S$. Ψ is determined uniquely by where it sends the basis:

$$\{F_* k_i x_1^{\alpha_1} \cdots x_n^{\alpha_n} \mid 1 \leq i \leq m,\ 0 \leq \alpha_j < p\rangle$$

Now, note that

$$F_* x_1^{p-1} \cdots x_n^{p-1} = F_*\left(x_1^{p-1-\alpha_1} \cdots x_n^{p-1-\alpha_n}\right) \cdot F_*\left(k_i x_1^{\alpha_1} \cdots x_n^{\alpha_n}\right)$$

So if $\Psi(F_*\left(k_i x_1^{\alpha_1} \cdots x_n^{\alpha_n}\right)) = s_{\alpha,i}$, we see

$$\Psi(-) = \sum_{i,\alpha} s_{\alpha,i} \Phi_S(F_*\left(k_i x_1^{p-1-\alpha_1} \cdots x_n^{p-1-\alpha_n}\right) \cdot -) = \Phi_S(F_*\left(\sum_{i,\alpha} s_{\alpha,i}^p k_i x_1^{\alpha_1} \cdots x_n^{\alpha_n}\right) \cdot -)$$

This completes the proof. □

Note that this theorem extends naturally to the case of $\mathrm{Hom}_S(F_*^e S, S)$. So there in particular is a homomorphism generating the others as a F_*S-module.

Definition 0.2. Let I, J be ideals of a ring R. Then we define the **colon ideal**

$$I :_R J := \{r \in R \mid r \cdot J \subseteq I\}$$

sometimes the R is omitted. This is also sometimes called the **ideal quotient**.

This allows us to setup Fedder's Criterion:

Theorem 0.3 (Fedder's criterion)**.** *If $R = S/I$, where $S = K[x_1, \ldots, x_n]$ and K is F-finite,*

$$\mathrm{Hom}_R(F_*R, R) \cong \left(F_*(I^{[p]} : I)/F_*(I^{[p]})\right) \cdot \mathrm{Hom}_S(F_*S, S)$$

Proof. I divide this proof into several parts.

(1) There is a map $\Lambda : F_*(I^{[p]} : I) \cdot \mathrm{Hom}_S(F_*S, S) \to \mathrm{Hom}_R(F_*R, R)$.
(2) Λ is a surjective map.
(3) $\ker(\Lambda)$ is exactly $IF_*R = F_*I^{[p^e]}$.

---

(1) Suppose that $x \in I^{[p]} : I$. Then for a given map $\varphi : F_*S \to S$, I define
$$\Lambda_x(\varphi)(F_*r) = \overline{\varphi(F_*xr)} \in R = S/I$$
It goes to show that this is a well defined homomorphism. Suppose that $r - r' \in I$. Then the problem is equivalent to showing that $\Lambda_x(\varphi)(F_*r) = \Lambda_x(\varphi)(F_*r')$:
$$\Lambda_x(\varphi)(F_*r) - \Lambda_x(\varphi)(F_*r') = \overline{\varphi(F_*xr)} - \overline{\varphi(F_*xr')} = \overline{\varphi(F_*x(r-r'))}$$
But by definition of the colon ideal, we see $x \cdot (r - r') = a^p \cdot y \in I^{[p]}$. Therefore,
$$\overline{\varphi(F_*x(r-r'))} = \overline{\varphi(aF_*y)} = \overline{a\varphi(F_*y)} = 0$$
as desired.

(2) Next, it goes to show that for any map $\psi \in \mathrm{Hom}_R(F_*R, R)$, we can find $\varphi \in F_*(I^{[p]} : I) \cdot \mathrm{Hom}_S(F_*S, S)$ corresponding to it. Since S is assumed regular, we know that F_*S is a projective (free) S-module. Therefore, given the map $F_*S \overset{F_*q}{\to} F_*R \overset{\psi}{\to} R$, and the surjection $q : S \to R$, we get that there exists a map $\varphi : F_*S \to S$ such that $q \circ \varphi = \psi \circ F_*q$.
It only goes to show that $\varphi \in F_*(I^{[p]} : I) \cdot \mathrm{Hom}_S(F_*S, S)$. Suppose not. Then $\varphi(-) = \Phi(F_*r \cdot -)$ with $r \notin I^{[p]} : I$. Then $ri \notin I^{[p^e]}$ for some $i \in I$, and therefore $\Phi(F_*ri) \notin I$. On the other hand,
$$(\varphi \circ q)(ri) = \psi(F_*q(ri)) = \psi(0) = 0$$
Therefore φ is not well defined, a contraction.

(3) It is clear that $IF_*R \subseteq \ker(\Lambda)$, by R-linearity. On the other hand, if $\varphi \in \ker(\Lambda)$, then $\varphi(-) = \Phi(F_*r \cdot -)$. But then φ applied to the basis is 0 necessarily. This implies precisely that $F_*r \in IF_*R$. This completes the proof.

□

Example 0.4. Last time we showed that $R = K[x_1, \ldots, x_n]/\langle x_1 \cdots x_n \rangle$ is an F-split ring. Here is a quick proof. Applying Fedder's criterion, and the fact that $I^{[p]} : I = \langle x_1^{p-1} \cdots x_n^{p-1} \rangle$, we see that
$$\varphi(-) = \Phi_S(F_*x_1^{p-1} \cdots x_n^{p-1} \cdot -) \in \mathrm{Hom}_R(F_*R, R)$$
But this implies $\varphi(F_*1) = 1$. Therefore, we are done!

As a Corollary of Theorem 0.3, we have the following.

Corollary 0.5. *If R is a local ring, then R is F-split if and only if $I^{[p]} : I \not\subseteq \mathfrak{m}^{[p]}$*

Example 0.6. If $R = K[x, y]/\langle f = x^2 + y^2 \rangle$. This is also a non-regular ring. However, $I^{[p]} : I = \langle f^{p-1} \rangle$. Notice
$$f^{p-1} = \sum_{i+j=p-1} c_{ij} x^{2i} y^{2j}$$
If we consider the corollary, we have that this is F-split if and only if $\exists i, j$ satisfying $2i, 2j < p$ and $i + j = p - 1$. If p is odd, then $\frac{p-1}{2}$ is an integer, and i, j can be set to it making R F-split. If $p = 2$, then $f \in \mathfrak{m}^{[2]}$, so R is NOT F-split.

CLASS 26, WEDNESDAY, MAY 2: F-REGULARITY

So F-splitting is a wonderful property that is relatively easy to check by Fedder. However, being weakly normal and reduced are often unsatisfactory for a 'nice' ring. Therefore, we introduce a property between being regular and being F-split.

We can think of being F-split as having the inclusion (because of F-split) $R \to F_*R$ being a split inclusion. The next notion perturbs this by an ϵ.

Definition 0.1. A ring R is called F-regular if for every non-zero divisor $c \in R$, we have that the following inclusion splits for some $e \gg 0$:

$$R \xrightarrow{F} F_*^e R \xrightarrow{\cdot F_*^e c} F_*^e R$$

I think of this as an ϵ perturbation since thinking of $F_*^e c$ as $c^{\frac{1}{p^e}}$ makes c quite small. On homework 6, you are asked to show that this property is also a local property. I will first show that regular rings (such as polynomial rings) are F-regular.

Proposition 0.2. *If R is a regular, then R is F-regular. If R is F-regular, then it is F-split.*

Proof. The case of units is handled by being F-split. Otherwise, by Krull's intersection theorem, we can take $n > 0$ such that $c \notin \mathfrak{m}^n$. Choose $e > 0$ such that $p^e > n$. If $\mathfrak{m} = \langle x_1, \dots, x_n \rangle$, then

$$c = \sum_{\substack{\beta \\ \alpha_i < p^e}} c_\alpha F_*^e k_\beta x_1^{\alpha_1} \cdots x_n^{\alpha_n}$$

where $c_\alpha, k_\alpha \in K$ and $F_*^e k_\beta$ is a basis for $F_*^e K$ over K. Choose a $c_\alpha \neq 0$, and take $\varphi \in \mathrm{Hom}_R(F_*R, R)$ to be the projection from the $F_*^e k_\alpha x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ free summand. This map will be nonzero, and map c to c_α. Post-composing by $\cdot c_\alpha^{-1}$ completes the proof.

The second statement follows by taking $c = 1$. □

Example 0.3. We have shown that $R = K[x_1, \dots, x_n]/\langle x_1 \cdots x_n \rangle$ is F-split. It is not F-regular, since if we take $c = x_1$, then

$$\Phi_S^e(F_* x_1^{p^e-1} \cdots x_n^{p^e-1} \cdot r \cdot x_1) = x_1 \Phi_S(F_* x_2^{p^e-1} \cdots x_n^{p^e-1} \cdot r) \in \langle x_1 \rangle$$

In fact, $\phi(\mathfrak{m}) \subseteq \mathfrak{m}$ for any $\phi \in \mathrm{Hom}_R(F_*^e R, R)$.

Example 0.4. If $R = K[x, y]/\langle f = x^2 + y^2 \rangle$, then similarly R is not F-regular. Last time we showed that R is F-split except when $p = 2$. In the case of $p > 2$, we can consider the condition $f^{p^e-1} \cdot c \notin \mathfrak{m}^{[p^e]}$. Let $c = xy$. We notice that

$$f^{p^e-1} = \sum_{i+j=p^e-1} c_{ij} x^{2i} y^{2j}$$

In this setting, it is clear that either $2i \geq p^e - 1$ or $2j \geq p^e - 1$ for integers i, j. Therefore $c \cdot f^{p^e-1} \in \mathfrak{m}^{[p^e]}$.

Now lets look at some positive examples:

Example 0.5. Consider $R = K[x,y,z]/\langle x^2+y^2+z^2\rangle$, where K is perfect of characteristic > 2. Again, by Fedder's Criterion it goes to show that for any given c, there is a sufficiently large $e \gg 0$ such that $f^{p^e-1}c \notin \mathfrak{m}^{[p^e]}$. That is to say that there exists a monomial of the left hand side of x,y,z-degree less than p^e; $cx^iy^jz^k$ with $i,j,k < p^e$.

$$f^{p^e-1} = \sum_{i+j+k=p^e-1} \binom{p^e-1}{i,j,k} x^i y^j z^k$$

Let m be the maximum of the x,y,z degree of c. It now suffices to show by the above observation that $\binom{p^e-1}{i,j,k} \neq 0$ and $i+m, j+m, k+m < p^e$.

Lemma 0.6 (Lucas's Theorem)**.** $\binom{m}{n}$ *is divisible by* $p > 0$ *if and only if expressing* $n = \sum_{i=1}^k n_i p^i$ *and* $m = \sum_{i=1}^l m_i p^i$*, for some* i*,* $n_i > m_i$*.*

Now, noting that $\binom{p^e-1}{i,j,k} = \binom{p^e-1}{i}\binom{p^e-1-i}{j}$, and that

$$p^e - 1 = (p-1) + (p-1)p + \ldots + (p-1)p^{e-1}$$

Lucas's Theorem allows us to conclude that $\binom{p^e-1}{i,j,k} \neq 0$ for $i = (p-1)p^{e-1}$, $j = p^{e-1}-1$, and $k = 0$. We can choose $e \gg 0$ so that $p^{e-1} - 1 > m$, and this shows that R is F-regular.

Many other examples can be computed in a similar fashion. So the question becomes why are F-regular rings so great? The following 2 results demonstrate it's importance as a singularity class:

Theorem 0.7. *If* R *is an* F*-regular domain, then* R *is Cohen-Macaulay and Normal.*

Cohen-Macaulay was mentioned with regard to its correspondence with depth. Normalcy is another fantastic condition, which in particular isolates your singularities (or irregularities) to height 2 and above prime ideals. In this case we say R is regular in codimension 1.

Definition 0.8. A domain R is called **normal** if R is integrally closed in $K(R) = R_{\langle 0\rangle}$. That is to say, $x \in K(R) \setminus R$ is not the zero of a monic polynomial with coefficients in R. If R is not normal, we call its integral closure in $K(R)$ by R^N (the **normalization** of R).

Theorem 0.7. To show that R is CM requires the techniques of local cohomology. This will be omitted for now.

To show R is normal, we consider the **conductor** of R; $\mathfrak{c} := \mathrm{Ann}_R(R^N/R)$. A ring R is normal if and only if $\mathfrak{c} = R$.

Lemma 0.9. *If* $\varphi \in \mathrm{Hom}_R(F^e_* R, R)$*, the* $\varphi(F_*\mathfrak{c}) \subseteq \mathfrak{c}$*.*

Proof. We can consider $\varphi \otimes 1_{K(R)} : F_*K(R) \to K(R)$. If $x \in \mathfrak{c}$ and $r \in R^N$, then $r\varphi(F_*x) = \varphi(F_* r^{p^e} x)$. But $r^{p^e} \in R^N$, and $x \in \mathfrak{c}$, and therefore $F_* r^{p^e} x \in R$. Therefore, $\varphi(F^e_*\mathfrak{c}) \cdot R^N \subseteq R$. □

To complete the proof, notice that if $\mathfrak{c} \neq R$, then we can take $c \neq 0$ in $\mathfrak{c}$, and find φ such that $\varphi(F_*c) = 1 \in \mathfrak{c}$ by the lemma. This is a contradiction! □