Commutative Algebra

D. Zack Garza

Thursday 16th April, 2020

Contents

List of Definitions

List of Theorems

1 Wednesday January 8

Course text: `http://math.uga.edu/~pete/integral2015.pdf`

Summary: The study of commutative rings, ideals, and modules over them.

The chapters we'll cover:

- 1 (Intro),
- 2 (Modules, partial),
- 3 (Ideals, CRT),
- 7 (Localization),
- 8 (Noetherian Rings),
- 11 (Nullstellensatz),
- 12 (Hilbert-Jacobson rings),
- 13 (Spectrum),
- 14 (Integral extensions),
- 17 (Valuation rings),
- 18 (Normalization),
- 19 (Picard groups),
- 20 (Dedekind domains),
- 22 (1-dim Noetherian domains)

In number theory, arises in the study of $\mathbb{Z}_k$, the ring of integers over a number field k, along with *localizations* and *orders* (both preserve the fraction field?).

In algebraic geometry, consider $R = k[t_1, \cdots, t_n]/I$ where k is a field and I is an ideal.

Some preliminary results:

1. In $\mathbb{Z}_k$, ideals factor uniquely into primes (i.e. it is a Dedekind domain).
2. $\mathbb{Z}_k$ has an integral basis (i.e. as a $\mathbb{Z}$-modules, $\mathbb{Z}_k \cong \mathbb{Z}^{[k:\mathbb{Q}]}$).
3. The Nullstellansatz: there is a bijective correspondence

$$\left\{\text{Irreducible Zariski closed subsets of } \mathbb{C}^n\right\} \iff \left\{\text{Prime ideals in } \mathbb{C}[t_1,\cdots,t_n]\right\}.$$

4. Noether normalization (a structure theorem for rings of the form R above).

All of these results concern particularly "nice" rings, e.g. $\mathbb{Z}_k, \mathbb{C}[t_1, \cdots, t_n]$. These rings are

- Domains
- Noetherian
- Finitely generated over other rings
- Finite Krull dimension (supremum of length of chains of prime ideals)
  - In particular, $\dim \mathbb{Z}_k = 1$ since nonzero prime ideals are maximal in a Dedekind domain

- Regular (nonsingularity condition, can be interpreted in scheme-theoretic language)

Note: schemes will have "local charts" given by commutative rings, analogous to building a manifold from Euclidean n-space. General philosophy (Grothendieck): Every commutative ring is the ring of functions on some space, so we should study the category of commutative rings as a whole (i.e. let the rings be arbitrary).
This does not hold for non-commutative rings! I.e. we can't necessarily associate a geometric space to every non-commutative ring. A common interesting example: $k[G]$, the group ring of an arbitrary group. Good references: Lam, 'Lectures on Modules and Rings'.

Example: Let X be a topological space and $C(X)$ be the continuous functions $f : X \longrightarrow \mathbb{R}$. This is a ring under pointwise addition/multiplication. (This generally holds for the hom set into any commutative ring.)

Example: Take $X = [0, 1]$ and $C(X)$ as a ring.

Exercise 1. Show that $C(X)$ is a not a domain.

Hint: find two nonzero functions whose product is identically zero, e.g. bump functions. Note that they are not analytic/holomorphic.

2. Show that it is not Noetherian (i.e. there is an ideal that is *not* finitely generated).
3. Fix a point $x \in [0, 1]$ and show that the ideal $\mathfrak{m}_x = \left\{ f \;\middle|\; f(x) = 0 \right\}$ is maximal.
4. Are all maximal ideals of this form?

Hint: See textbook chapter 5, or Gilman and Jerison 'Rings of Continuous Functions'.

The following is a theorem about topological vector bundles over $C([0, 1])$, see textbook.

Theorem 1.1 ***(Swan).***
There is a categorical equivalence between vector bundles on a compact space and f.g. projective modules over this ring.

So commutative algebra has something to say about other branches of Mathematics!

Definition 1.1.1 (Boolean Spaces)**.**
A topological space is called *boolean* (or a *Stone space*) iff it is compact, hausdorff, and totally disconnected.

Example 1.1.
A projective variety over p-adics with $\mathbb{Q}_p$ points plugged in.

Definition 1.1.2 (Boolean Rings)**.**
A ring is boolean if every element is idempotent, i.e. $x \in R \implies x^2 = x$.

Exercise (Boolean Domains are $\mathbb{F}_2$): If R is a boolean domain, then it is isomorphic to the field with 2 elements.

Lemma 1.2.
There is a categorical equivalence between Boolean spaces, Boolean rings, and so-called "Boolean algebras".

2 Monday January 13

2.1 Logistics

Some topics for final projects

- The cardinal Krull dimension of $\mathrm{Hol}(X)$.
- Galois connections
- Ordinal filtrations
- Lam-Reyes prime ideal principal
- $C(X)$
- $\mathrm{Hol}(X)$
- Semigroup rings
- Swan's Theorem
  - Vector bundles on a compact space
- Boolean rings and Stone duality
- More Nullstellansatz
  - Beyond Hilbert's usual one
- Hochster's Theorem
  - Characterizes Spec R as a topological space, i.e. when is a topological space homeomorphic to the spectrum of some commutative ring.
- Invariant theory (quotients of rings under finite group actions, i.e. R^G for $|G| < \infty$)
  - For $R = k$ a field, this is Galois theory
  - Easy case of geometric invariant theory, when G is infinite
- UFDs
  - What conditions does a ring need to have to ensure unique factorization?
- Euclidean rings
- Claborn (Leedham-Green-Clark): Every commutative group is (up to isomorphism) the class group of some Dedekind domain.
  - A type of inverse problem, class group measures deviation from being a UFD
  - Uses ordinal filtrations, transfinite induction
  - See proof in elliptic curves course

2.2 Rings of Functions

Let k be a field, X a set of cardinality $|X| \geq 2$, and define $k^X \coloneqq \mathrm{Maps}(X.k) = \{f : X \longrightarrow K\}$ is a ring under pointwise addition and multiplication. As a ring, this is a (big!) cartesian product.

Some facts:

- k^X is not a domain (**exercise**), and there are nontrivial idempotents ($e^2 = e$)

  Note: it could be worse and have nilpotents.

- k^X is *reduced*, i.e. it has no nonzero nilpotents, where $z \in R$ is nilpotent iff $\exists n \geq 1$ such that $z^n = 0$.
  - Note: domains are reduced, cartesian products of reduced rings are reduced.
- Every subring of k^X is reduced.

> Moral: should be viewing every ring as functions on some space, but this can't literally be true because of the above restrictions. Nilpotent elements are "hard to view as functions".

- For X a topological space, $C(X)$ the ring of continuous functionals to $\mathbb{R}$, then $C(X) \subset \mathbb{R}^X$.

Exercise: When is $C(X)$ a domain? (Note that we can have products of nonzero functions being identically zero.)

Example: Let R be the ring of holomorphic functions $\mathbb{C}\circlearrowleft$, i.e. $\mathrm{Hol}(\mathbb{C}, \mathbb{C}) \coloneqq \left\{ f : \mathbb{C} \longrightarrow \mathbb{C} \;\middle|\; f \text{ is holomorphic} \right\}$.

The set of zeros of such an f must be discrete, the example of bump functions doesn't go through holomorphically.

This is a domain, not Noetherian, not a PID, but every f.g. ideal is principal (thus this is a Bezout domain, a non-Noetherian analog of a PID).

It has infinite Krull dimension: recall that ideals are prime iff $xy \in \mathfrak{p} \implies x \in \mathfrak{p}$ or $y \in \mathfrak{p}$ iff $R/\mathfrak{p}$ is a domain, and the Krull dimension is the supremum S of lengths of chains of prime ideals (only when S is finite).

If $C \subset (X, \leq)$ is a finite-length chain in a totally ordered set, then the length $\ell(C) = |C| - 1$ (1 less than the number of elements appearing). The *cardinal Krull dimension* of a ring R is the actual supremum.

> Note: in Noetherian rings, there can still be finite but unbounded length chains.

Letting X be a complex manifold (i.e. covered by subsets of $\mathbb{C}^n$ with holomorphic transition functions) and let $\mathrm{Hol}(X)$ be the holomorphic functionals $f : X \longrightarrow \mathbb{C}$. Then $\mathrm{Hol}(X)$ is a domain iff X is connected.

> Note that if X is disconnected, we can take a function that is constant on one component and zero on another, then switch, then multiply to get a zero function.

If X is a compact connected projective variety, then $\mathrm{Hol}(X)$ is just constant functions by the open mapping functions. So $\mathrm{Hol}(X) = \mathbb{C}$, and $\mathrm{carddim}\mathbb{C} = 0$ because for any field there are only two ideals, and here (0) is prime. Moreover, $\mathrm{carddim}\mathrm{Hol}(\mathbb{C}) \geq \alpha_0$.

> Note that for complex manifolds, X is either compact or supports many holomorphic functions.

Theorem 2.1 ***(Function Spaces Can Have Large Unbounded Chains).***
If X is a connected complex manifold which has a nontrivial holomorphic function, i.e. $\mathrm{Hol}(X) \supset \mathbb{C}$, then there exists a chain of prime ideals in $\mathrm{Hol}(X)$ of length $|\mathbb{R}| > \aleph_0$, i.e. it has at least the cardinality of the continuum.

Note: the cardinality could be even bigger!

> Maximals are prime: equivalent to fields are integral domains.

2.3 Rings

Take all rings to be unital, i.e. containing 1. A ring without identity is referred to as an *rng*. In this course, all rings are commutative.

Example: This is a fairly special restriction. Take $(A, +)$ a commutative group and define $\mathrm{End}(A) = \{f : A \longrightarrow A\}$ the ring of group homomorphisms under pointwise addition and composition. This is generally not commutative, i.e. $\mathrm{End}(\mathbb{Z}/(2) \oplus \mathbb{Z}/(2)) = M_2(\mathbb{Z}/(2))$ the ring of matrices with $\mathbb{Z}/(2)$ entries, which is not commutative.

Exercise: Given $(A, +)$, show that $\mathrm{End}(\bigoplus^n A) = M_n(\mathrm{End}(A))$.

Generally, if R is a ring and M is as R-module, then $\mathrm{End}_R(M) = \{f : M \longrightarrow M\}$ of R-module homomorphisms is always a ring under pointwise addition and composition, and is (probably) non-commutative.

3 Wednesday January 15th

Cayley's theorem: For G a group, then there is a canonical injective group homomorphism $\Phi : G \hookrightarrow \mathrm{Sym}(G) \cong S_n$ for $n = |G|$. The map is given by $g \mapsto g\cdot$, i.e. multiplying on the left.

Is there an analog for rings?

Take a similar map:

$$\begin{aligned} R &\longrightarrow \mathrm{End}_{\mathbb{Z}}(R, +) \\ r &\mapsto (x \mapsto rx). \end{aligned}$$

Unfortunately there is no specialization for commutative groups/rings – $\mathrm{Sym}(G)$ for example is noncommutative when $|G| \geq 2$. Similarly, even if R is commutative, $\mathrm{End}(R, +)$ is probably not. As per the Grothendieck philosophy, we find that all rings are a ring of functions on something – namely themselves, since this map is injective.

All rings are commutative here, so take $R^\times = \left\{x \in R \;\middle|\; \exists y \text{s.t.} xy = 1\right\}$. For R a group, $R^\times$ is a commutative group, so this is an interesting invariant.

Another interesting invariant: the class group.

Notation: Let $R^\bullet = R \setminus 0$. An element $x \in R$ is a zero divisor iff there exists $y \in R^\bullet$ such that $xy = 0$. For $x, y \in R$ we write $x \;\middle|\; y$ iff $\exists z \in R$ such that $xz = y$.

R is a domain iff 0 is the only zero divisors, i.e. $xy = 0 \implies x = 0$ or $y = 0$. $(R^\bullet, \cdot)$ is a commutative monoid (group without inverses) iff R is a domain. Observe that R is a field iff $R^\bullet = R^\times$.

For rings R, S we have the usual definition of ring homomorphism, additionally requiring $f(1) = 1$. Note that $f(0) = 0$ follows from $f(x+y) = f(x) + f(y)$, but $f(1) = 1$ does not. Rings have products $R_1 \times R_2$ which is again a ring under coordinate-wise operations. Note that there are canonical projections $\pi_i R_1 \times R_2 \longrightarrow R_i$. There is a dual inclusion $\iota_1 : R_1 \longrightarrow R_1 \times R_2$ given by $x \mapsto (x, 0)$, but these are not ring homomorphisms (although everything is a group homomorphism). This

is because $\iota_1(1) = (1,0) \neq (1,1)$, the identity of $R_1 \times R_2$. Note that 1 always has to map to an idempotent element, i.e. $e^2 = e$, and idempotents are always zero divisors. Also note that the map $x \mapsto 0$ is not a ring homomorphism unless $S = 0$.

Definition 3.0.1 (Ring Morphisms)**.**
A **ring homomorphism** is a map $f : R \longrightarrow S$ is an isomorphism iff it has a two-sided inverse, i.e. there exists a morphism $g : S \longrightarrow R$ with $g \circ f = \mathrm{id}_R$ and $f \circ g = \mathrm{id}_S$.

Exercise Check that this is equivalent to f being a bijection.

Exercise Check that the zero ring is the final object in the category of rings. Show that $\mathbb{Z}$ is the initial object in this category?

R is a subring of S iff $R \subset S$ and the inclusion $R \hookrightarrow S$ is a morphism.

Adjoining elements: Suppose $R \leq S$ is a subring and $X \subset S$ is just a subset. Then there exists a ring $R[X]$ such that

- Top-down description: $R[X] \leq S$ is a subring containing R and X, and is minimal with respect to this property (obtained by intersecting all such subrings)
- Bottom-up description: things resembling $\sum r_i x_i$

Exercise 1.6: Take $R = \mathbb{Z}, S = \mathbb{Q}$, P a arbitrary set of prime numbers. Let $\mathbb{Z}_{\mathcal{P}} = \mathbb{Z}[\left\{ \frac{1}{p} \;\middle|\; p \in P \right\}]$.

a. When do we have $\mathbb{Z}_{\mathcal{P}_1} \cong \mathbb{Z}_{\mathcal{P}_2}$?

Hint: take $P_1 = \{3,7,11\}, P_2 = \{5\}$. Need $P_1 = P_2$!

b. Show that every subring T such that $\mathbb{Z} \leq T \leq \mathbb{Q}$ is of the form $\mathbb{Z}_{\mathcal{P}}$ for some unique set of primes P.

Note that if T is any intermediate ring between R and S, then $R[T] = T$.

3.1 Ideals and Quotients

For $f : R \longrightarrow S$ a ring homomorphism, define $I = \ker f = f^{-1}(\{0\})$. Then I is a subgroup of $(R, +)$, and for all $i \in I$ and all $r \in R$ we have $ri \in I$, since $f(ri) = f(r)f(i) = f(r)0 = 0$. In other words, $RI \subseteq I$.

By definition, an ideal I of R is an additive subgroup of R that satisfies these properties. Is every ideal the kernel of a ring homomorphism? The answer is yes, namely the quotient $\pi : R \longrightarrow R/I$.

Theorem 3.1 ***(Every Ideal Determines a Quotient Ring).***
Let $I \subset (R, +)$, then TFAE:

a. I is an ideal of R, written $I \trianglelefteq R$.
b. There exists a ring structure on the quotient group R/I such that the projection $r \mapsto r + I$ is a ring morphism.

When these conditions hold, the ring structure on R/I is *unique* and we refer to this as the *quotient ring*.

4 Friday January 17th

For a $R \subset T$ a subring of a ring, the set of intermediate rings is a large/interesting class of rings. Recall: uncountably many rings between $\mathbb{Z}$ and $\mathbb{Q}$! Taking R a PID and T its fraction field, a similar result will hold.

Define $I \trianglelefteq R$ as the kernel of a ring morphism. This implies that $I \subset (R, +)$ with the absorption property $RI \subset I$. Conversely, any I satisfying these two properties is the kernel of a ring morphism: namely $R \longrightarrow R/I$. This makes sense as a group morphism.

Exercise Define $xy + I = (x + I)(y + I)$, need to check well-definedness. Write out

$$(x + i_1)(y + i_2) = \cdots$$

Need to check that

$$i_1 y + i_2 x + i_1 i_2 \in I,$$

but the absorption property does precisely this.

Note that if we were in a non-commutative setting, this would define a left ideal. These don't have to coincide with right ideals – there are rings where the former satisfy properties that the latter does not.

Example: The subrings of $R = \mathbb{Z}$ are of the form $n\mathbb{Z}$ for $n \geq 0$, with the usual quotient.

Definition 4.0.1 (Proper Ideals)**.**
An ideal $I \trianglelefteq R$ is *proper* iff $I \subsetneq R$.

Exercise An ideal I is not proper iff I contains a unit.

Exercise R is a field iff the only ideals are $0, R$.

Definition 4.0.2 (Lattice Structure of Ideals)**.**
Let $\mathcal{I}(R)$ be the set of all ideals in R. What structure does it have? It is partially ordered under inclusion. It is a complete lattice, i.e. every element has an infimum (GLB) and a supremum (LUB).

```
Namely, for a family of ideals $\theset{I_j}$, the **infimum** is the intersection and **s
$$
\generators{y} = \theset{ \sum^n r_i y_i \suchthat n\in \NN_{> 0},~ r_i \in R,~ y_i\in y}
.$$
```

Exercise For $I_1, I_2 \trianglelefteq R$, it is the case that $I_1 + I_2 \coloneqq \{i_1 + i_2\} = \langle I_1, I_2 \rangle$.

Theorem 4.1 ***(Lattice Isomorphism Theorem for Rings).***
Let $I \trianglelefteq R$ and $\phi : R \longrightarrow R/I$, and define $\ell(I) = \{I \subset J \trianglelefteq R\}$. Then we can define maps

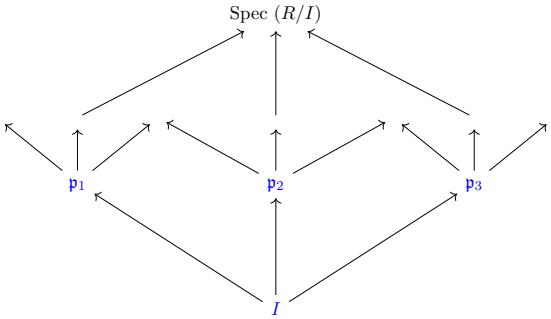
$$\begin{aligned} \Phi : \ell(R) &\longrightarrow \ell(R/I) \\ J &\mapsto \frac{I + J}{J}, \end{aligned}$$

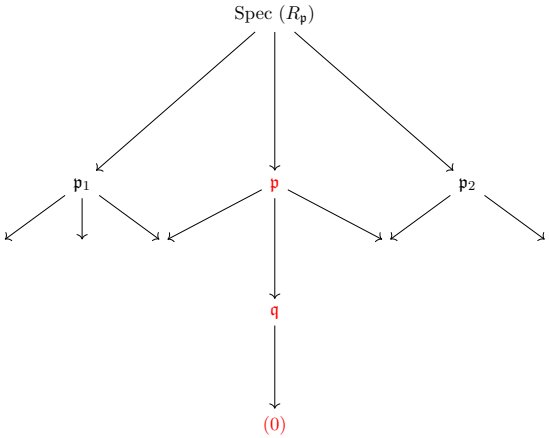
and

$$\Psi : \ell(R/I) \longrightarrow \ell(R)$$
$$J \trianglelefteq R/I \mapsto \phi^{-1}(J).$$

We can check that $\Psi \circ \Phi)(J) = I + J$, and $\Phi \circ \Psi(J) = J$ $(= J/I?)$ So Ψ has a left inverse and is thus injective. Its image is the collection of ideals that contain J, and $\Psi : \ell(R/I) \longrightarrow \ell_I(R)$ **is a bijection** and is in fact a lattice isomorphism with $\ell_I(R) \subset \ell(R)$.

Note that this gives us everything above a given ideal in the ideal lattice (blue); the dual notion will come from localization (red):





Here we take $\mathfrak{p}$ to be a maximal ideal.

Remarks The ideal lattice $\ell(R)$ is

- A complete lattice under subset inclusion,
- A commutative monoid under addition
- A commutative monoid under *multiplication*, which we'll define.

Definition 4.1.1 (Product of Ideals)**.**
For $I, J \trianglelefteq R$, we define

$$IJ = \left\langle ij \;\middle|\; i \in I,\ j \in J \right\rangle.$$

Note that we have to take the ideal generated by products here.

For $\langle x \rangle = (x)$ a principal ideal and $\langle y \rangle$ principal, we do have $(x)(y) = (xy)$. Note that $IJ \subset I \bigcap J$, whereas the sum was larger than I, J.

Exercise Note that $(\ell(R), \cdot)$ has an absorbing element, namely $(0)I = (0)$. For $(M, +)$ a commutative monoid and $M \hookrightarrow G$ a group, then multiplication by x is injective and so for all $y \in M$, $xz = yz \implies x = y$, so M is cancellative.

Question: what if we consider $\mathcal{I}^{\bullet}(R)$ the set of nonzero ideals of R. Does this help? We will see next time.

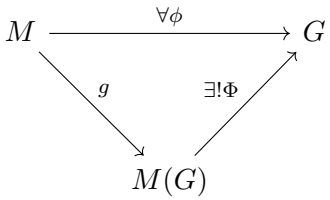
5 Wednesday January 22nd

Let R be a ring and let $\mathcal{I}(R)$ be the set of ideals $I \trianglelefteq R$. This algebraic structure is

- Partially ordered under inclusion
- Forms a complete lattice with sup the ideal generated by a family and inf the intersection.
- Forms a commutative monoid under $I + J$
- Forms a commutative monoid under IJ

For any commutative monoid $(M, +)$, there exists a group completion $G(M)$ such that

- $G(M)$ is a commutative group
- $g : M \longrightarrow G(M)$ is a monoid homomorphism
- For any map $\phi : (M, +) \longrightarrow (G, +)$ into a commutative group, we have the following diagram



So ϕ factors through $M(G)$.

If this exists, it is unique up to unique isomorphism (as are all objects defined by universal properties). It remains to construct it.

Exercise For $(M, +)$ a commutative monoid, show that TFAE

1. There exists an injective $\iota : M \hookrightarrow G$ monoid homomorphism for G some commutative group.
2. The map $g : M \longrightarrow G(M)$ is an injection.
3. M is cancellative, i.e. $\forall x, y, z \in M$ we have $x + z = y + z \implies x = y$, i.e. the map $p_z(x) = x + z$ is injective.

The content here is in $3 \implies 1$.

Definition 5.0.1 (Reduced Monoids)**.**
A commutative monoid is *reduced* iff $M^\times = (0)$, i.e. if "$\forall m \in M \exists n$ such that $m + n = 0$" $\implies$ $m = 0$

Example 5.1.
$(\mathbb{N}, +)$ and $(\mathbb{Z}^+, \cdot)$ are cancellative and reduced.

Definition 5.0.2 (Zero Elements in Monoids)**.**
$z \in M$ is a **zero element** iff $z + x = z$ for all $x \in M$.

Remark If M has a zero element, then $G(M) = \{0\}$.

(0) is a zero element of $(\mathcal{I}(R), \cdot)$, so this is not cancellative. If we take $\mathcal{I}^\bullet$ the set of nonzero ideals with multiplication, then this is a submonoid of $\mathcal{I}(R)$ iff R is a domain.

For R a domain, let $\mathcal{I}_1(R)$ be the set of nonzero principal ideals of R, then $\mathcal{I}_1(R) = R^\bullet/R^\times$, so this is reduced and cancellative.

What is the group completion? In this case, it will consist of fractional ideals.

If R is a PID, then $\mathcal{I}_1^\bullet(R) = \mathcal{I}^\bullet(R)$ is reduced and cancellative.

Example 5.2.
$\mathcal{I}^\bullet \cong (\mathbb{Z}^+, \cdot)$.

Warning: If R is not a PID, then $\mathcal{I}^\bullet(R)$ need not be cancellative.

Exercise Take $R = \mathbb{Z}[\sqrt{-3}]$ and $p_2 \coloneqq \left\langle 1+\sqrt{-3}, 1-\sqrt{-3} \right\rangle$. Show that $|R/p_2| = 2$, $|R/(2)| = 4$, and $p_2^2 = p_2(2)$ and $\left|R/p_2^2\right| = 8$. Conclude that $\mathcal{I}^\bullet(R)$ is not cancellative.

What went wrong here? Take $K = \mathbb{Q}[\sqrt{-3}]$, then $\mathbb{Z}_k[\frac{1+\sqrt{-3}}{2}]$ is the integral closure of $\mathbb{Z}$ in K. $\mathbb{Z}_k$ is a Dedekind domain, and there are inclusions

$$\mathbb{Z} \subset \mathbb{Z}[\sqrt{-3}] \subsetneq \mathbb{Z}[\frac{1+\sqrt{-3}}{2}] \subseteq K.$$

Here the problem is that $\mathbb{Z}[\sqrt{-3}]$ is not a Dedekind domain. If R is a Dedekind domain, then $\mathcal{I}^\bullet(R)$ is cancellative.

Exercise Does the converse hold?

Things that are too small to be the full rings of integers, and things tend to go wrong (??).

5.1 Pushing / Pulling

Let $f : R \longrightarrow S$ be a ring homomorphism.

We can define a pushforward on the set of ideals $\mathcal{I}(R)$:

$$\begin{aligned} f_* : \mathcal{I}_R &\longrightarrow \mathcal{I}(S) \\ I &\mapsto \langle f(I) \rangle . \end{aligned}$$

and a pullback

$$\begin{aligned} f^* : \mathcal{I}(S) &\longrightarrow \mathcal{I}(R) \\ J &\mapsto f^{-1}(J). \end{aligned}$$

Exercise: Show that $f^{-1}(J) \trianglelefteq R$.

For $I \trianglelefteq R$ and $J \trianglelefteq S$, then

$$f^* f_*(I) \supseteq I$$
$$f_* f^*(J) \subseteq J.$$

Exercise: These are not equal in general, and give examples where equality does and does not hold.

If f is surjective, $f_* f^* J = J$.

Will also hold for localization, which is dual to taking a quotient.

Define $\bar{I} \coloneqq f^* f_*(I)$ and $J^\circ \coloneqq f_* f^*(J)$, the closure and interior respectively. Show that these operations are idempotent.

Definition 5.0.3 (Prime Ideals)**.**
An ideal $\mathfrak{p}$ is *prime* iff $ab \in \mathfrak{p} \implies a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.

Exercise: I is prime iff R/I is a domain.

Definition (Prime Spectrum) Spec $(R) = \{\mathfrak{p} \trianglelefteq R\}$ the collection of prime ideals is the spectrum.

Exercise Show that for $I \trianglelefteq R$, if we define

$$V(I) \coloneqq \left\{ \mathfrak{p} \in \text{Spec } (R) \;\middle|\; p \supseteq I \right\} \subseteq \text{Spec } (R),$$

then $\left\{ V(I) \;\middle|\; I \in \mathcal{I}(R) \right\}$ are the closed sets for a topology on Spec (R) (the Zariski topology).

Exercise If $f : R \longrightarrow S$ and $J \in \text{Spec } (S)$ then $f^*(J) \in \text{Spec } (R)$. Show that $f^* : \text{Spec } (S) \longrightarrow \text{Spec } (R)$ is a continuous map. Conclude that Spec $(\cdot)$ is a functor.

Definition 5.0.4 (Maximal Ideals)**.**
$I \trianglelefteq R$ is **maximal** iff I is proper and is not contained in any other proper ideal.

Exercise I is maximal iff R/I is a field.

Exercise Show that maximal ideals are prime.

Definition 5.0.5 (Max Spectrum)**.**
Let Spec $_{\max}(R)$ be the set of maximal ideals and define $V(I) = \left\{ \mathfrak{m} \in \text{Spec }_{\max}(R) \;\middle|\; \mathfrak{m} \supseteq I \right\}$.

Exercise Show that these form the closed sets for a topology, and that this is the subspace topology for the Zariski topology.

Exercise Show that if $f : R \longrightarrow S$ and $\mathfrak{m} \in \text{Spec }_{\max}(S)$ that $f^*(\mathfrak{m})$ is prime but need not be maximal.

Exercise Show that if f is an integral extension, then maximal ideals pull back to maximal ideals.

6 Friday January 24th

6.1 Ideals and Products

Recall: Prime and maximal ideals.

Fact: If $I \trianglelefteq R$ then there exists a maximal ideal $I \subset \mathfrak{m} \trianglelefteq R$.

Proof .
Use Zorn's lemma.
■

Corollary 6.1.
maxSpec $R \neq \emptyset \iff R \neq 0$.

Later: Multiplicative avoidance, if $S \subset R$ is nonempty with $SS \subset S$, let $I \trianglelefteq R$ with $I \bigcap S = \emptyset$, then

a. There exists an ideal $J \supseteq I$ with $J \bigcap S = \emptyset$ which is maximal with respect to being disjoint from S.

b. Any such ideal J is prime.

Taking $S = \{1\}$ recovers the previous fact.

Exercise Let $f : R \longrightarrow S$ be a ring homomorphism and $\mathfrak{p} \in \text{Spec } (R)$. Show that $f_*(\mathfrak{p})$ need not be prime in S.

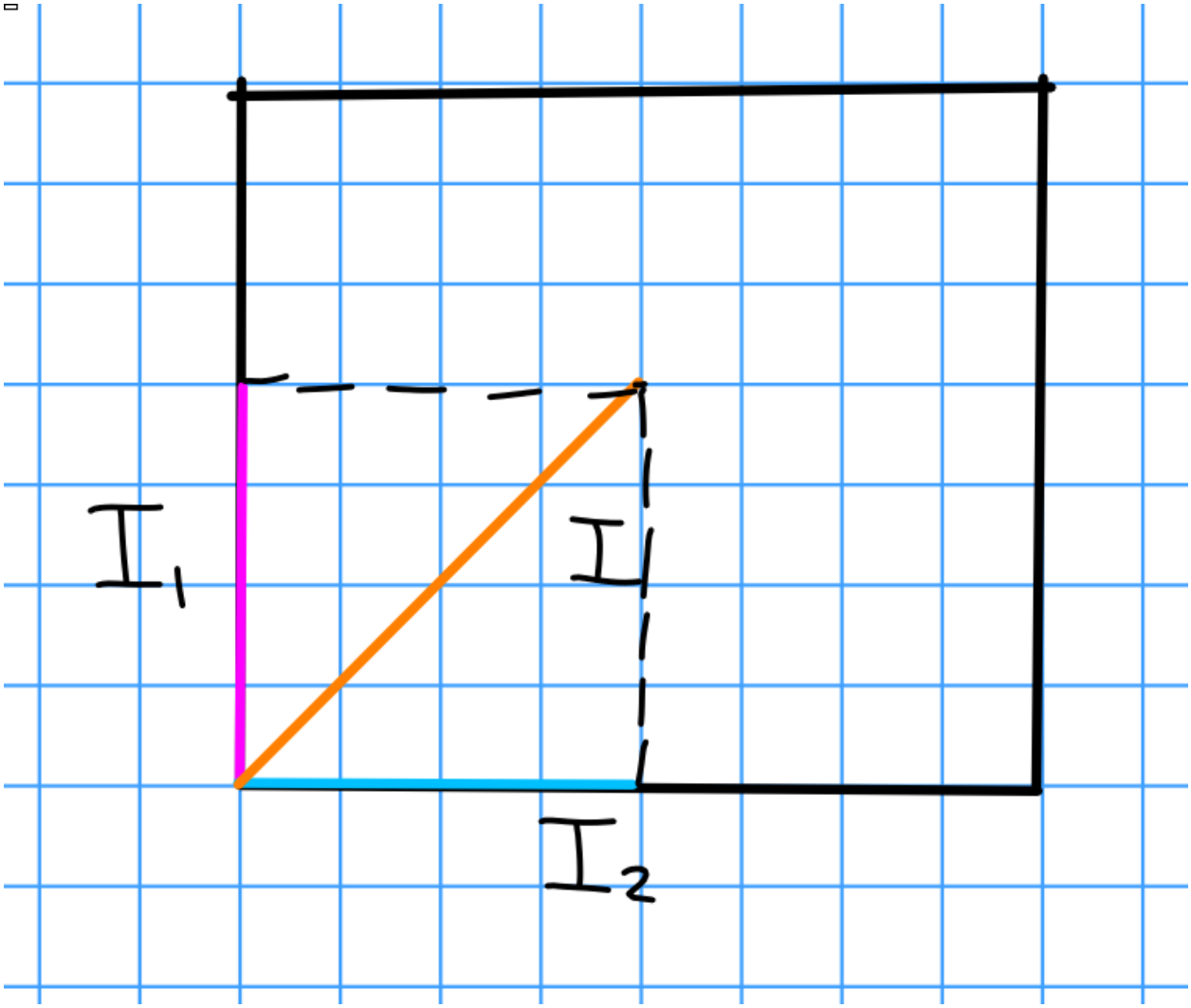
We can consider products of rings, and correspondingly $\mathcal{I}(R_1 \times R_2)$.

Exercise Show that if ϕ is surjective, $\phi(I)$ is an ideal.

Proposition 6.2 ***(Ideals of Products are Products of Ideals).***
Let $I \in \mathcal{I}(R_1 \times R_2)$. Take $\pi_i \longrightarrow R_i$ the projections, and let I_i be the corresponding images of I. Then $I = I_1 \times I_2$.

Note: a suspiciously strong result! Not every group is the cartesian product of some subgroups.

It's clear that $I \subset I_1 \times I_2$.



Proof .
Showing $I_1 \times I_2 \trianglelefteq R_1 \times R_2$ is an ideal, since it equals $\langle I_1 \times \{0\}, \{0\} \times I_2 \rangle$.
To show $I_1 \times I_2 \subseteq I$, show that $I_1 \times 0, 0 \times I_2 \subseteq I$. E.g. $I_1 \times 0 \subseteq I$: take $(x, 0) \in I_1 \times 0$ such that there exists a $y \in R_2$ with $(x, y) \in I$. Then $(x, y) \cdot (1, 0) = (x, 0) \in I$, then similarly $0 \times I_s \subseteq I$. ■

Exercise Use $\mathcal{I}(R_1 \times R_2) = \mathcal{I}(R_1) \times \mathcal{I}(R_2)$ to describe Spec $(R_1 \times R_2)$ in terms of Spec (R_1) and Spec (R_2).

Question: For a ring R, when is $R \cong R_1 \times R_2$ for some nonzero R_1, R_2?

Exercise Show that comaximal ideals correspond with coprime ideals when $R = \mathbb{Z}$.

Theorem 6.3 ***(Chinese Remainder).***
If I_1, I_2 are comaximal, so $I_1 + I_2 = R$, then the map

$$\begin{aligned}\Phi : R &\longrightarrow R/I_1 \times R/I_2 \\ x &\mapsto (x + I_1, x + I_2).\end{aligned}$$

Then $\ker \Phi = I_1 \bigcap I_2 \overset{\text{CRT}}{=} I_1 I_2$ and Φ is surjective, and

$$R/(I_1 \bigcap I_2) = R/I_1 I_2 \cong R/I_1 \times R/I_2.$$

Proof .
Case 1: Let $I_1 + I_2 = R$ and $I_1 \bigcap I_2 = 0$ (equivalently $I_1 I_2 = (0)$), then $R \cong R/I_1 \times R/I_2$.

Conversely, let $R = R_1 \times R_2$ with R_1, R_2 nonzero. Let $e_1 = (1, 0)$ and $e_2 = (0, 1)$. Then $e_1 e_2 = 0$ and $e_2 = (1 - e_1)$, so $0 = e_1(1 - e_1) = e_1 - e_1^2$ and e_1 is idempotent.

So e_1, e_2 are complementary nontrivial idempotents. Then $I_1 I_2 = e_1 e_2 = (0)$, $I_1 + I_2 = \langle e_1, e_2 \rangle = R$, and thus $R = R/e_2 R \times R/e_1 R$. Note that $e_2 R = 0 \times R_2$ and $e_1 R = R_1 \times 0$, thus

$$\begin{aligned}R/e_2 R &= \frac{R_1 \times R_2}{0 \times R_2} = R_1 \\ R/e_1 R &= \frac{R_1 \times R_2}{R_1 \times 0} = R_2.\end{aligned}$$

■

We thus have a correspondence

$$\begin{aligned}\left\{\text{Nontrivial product decompositions } R{=}R_1{\times}R_2\right\} &\iff \left\{I_1{,}I_2 \trianglelefteq R \text{ such that } I_1 I_2{=}0 \text{ and } I_1{+}I_2{=}R\right\} \\ &\iff \left\{\text{Idempotents } e{\neq}0{,}1\right\}.\end{aligned}$$

Thus a ring can be decomposed as a product iff it contains nontrivial idempotents.

Definition 6.3.1 (Connected Rings)**.**
R is connected iff there do not exists nonzero R_1, R_2 such that $R \cong R_1 \times R_2$ iff R does not contain an idempotents $e \neq 0, 1$.

Exercise Show that R is connected iff Spec (R) is connected as a topological space.

Note: Not every ring is a finite product of connected rings.

6.2 Modules

For $(M, +)$ a commutative group, we want an action $R \curvearrowright M$ for R a ring. Recall that $\text{End}(M)$ for a group is a (potentially noncommutative) ring. An R-module structure is a ring homomorphism

$R \longrightarrow \mathrm{End}(M)$. Equivalently, it is a function $R \times M \longrightarrow M$ with $rs(x) = r(sx)$, $r(x+y) = rx + ry$, and $1 \cdot x = x$ for all $x \in M$.

Note that this defines a left R-module, but right/left modules coincide for commutative rings.

Exercise Let M be an R-module and for $m \in M$ define $\mathrm{Ann}(m) = \left\{ r \in R \;\middle|\; xm = 0 \right\} \trianglelefteq R$; show this is in fact an ideal.

Note: skipped chapter on Galois connections, i.e. some binary relation on a pair of sets. This is an instance of such a connection, where $x \sim m \iff xm = 0$.

Exercise For any subset $S \subset M$, define

$$\mathrm{Ann}(S) \coloneqq \left\{ x \in R \;\middle|\; xm = 0 \;\forall m \in S \right\}.$$

Show that $\mathrm{Ann}(S) = \bigcap_{m \in S} \mathrm{Ann}(m)$ and

$$\mathrm{Ann}(M) = \left\{ x \in R \;\middle|\; xM = 0 \right\} = \ker(R \longrightarrow \mathrm{End}(M)).$$

Definition 6.3.2 (Faithful Modules)**.**
M is **faithful** iff $\mathrm{Ann}(M) = 0$ iff $R \hookrightarrow \mathrm{End}(M)$ is an injection.

Exercise Any M is naturally a faithful $R/\mathrm{Ann}(M)$-module.

7 Monday January 27th

7.1 Localization

Consider rings T such that $\mathbb{Z} \subseteq T \subseteq \mathbb{Q}$, and let P be a set of prime numbers. We've shown that if P, Q are two sets of prime numbers, then $\mathbb{Z}_p = \mathbb{Z}_q \iff \mathbb{Z}_p \cong \mathbb{Z}_q \iff P = Q$.

Let R be a domain with fraction field K. Let P be a set of mutually nonassociate prime elements. Note that $p \in R$ is a prime element iff (p) is a prime ideal. We say x, y are associates iff there exists a $u \in R^\times$ such that $y = ux$. Since we're in a domain, (exercise) this is equivalent to $(x) = (y)$.

Fact: We can then consider $R_P \coloneqq R[\left\{ \frac{1}{p} \;\middle|\; p \in P \right\}]$, and the fact is that the previous statement still holds.

But if $R = \mathbb{Z}$, we also have (exercise) if $Z \subset T \subset \mathbb{Q}$ then $T = \mathbb{Z}_p$ for a unique P.

Exercise: How do we find such a P? This comes down to looking at $\frac{a}{b} \in T$ with $\gcd(a, b) = 1$, then $\frac{1}{b} \in T$.

Hint: In a PID, $\gcd(a, b)$ exists and is a $\mathbb{Z}$-linear combination of a and b. The solution should work for an arbitrary PID.

Let R be a domain and S multiplicatively closed (so $(S, \cdot) \leq (R, \cdot)$ is a submonoid). Then S is *primal* if S is generated as a monoid by its prime elements. Suppose that S is *saturated*, i.e. if $s \in S$ and $r \in R$ with $r \mid s$, then $r \in S$.

Can always add in all divisors.

We can then define the localization of R at S,

$$R_s \coloneqq \left\{ \frac{a}{s} \;\middle|\; a \in R, s \in S \right\}.$$

This satisfies $R \subset R_S \subset K$, and is a multiplicative partial group completion. If we took nonzero elements, this would yield exactly the fraction field.

Theorem 7.1 ***(Negata).***
Let R be a Noetherian domain with $S \subset R$ primal as above. If R_S is a UFD, then R is a UFD.

Exercise Show that the converse holds.

Fraction fields are always UFDs? Localizing makes it easier for irreducibles to be prime. This helps prove that some interesting rings are UFDs.

7.2 Modules

If M is an R-module, then an R-submodule $N \leq M$ is a subgroup of $(M, +)$ such that $R \curvearrowright N \subset N$.

Every ring R is an R-module over itself, and the R-submodules of R are precisely the ideals of R.

Can express certain concepts about rings/commutative algebra in the language of modules.

A morphism of R-modules $f : M \longrightarrow N$ is a homomorphism $(M, +) \longrightarrow (N, +)$ such that $f(r \curvearrowright m) = r \curvearrowright f(m)$.

Exercise: Any module morphism that is a bijection is an isomorphism. (Usually true in algebraic settings.)

We can form quotient modules $\dfrac{M}{N}$ which is an R-module with $r \curvearrowright (m + N) = (r \curvearrowright m) + N$, and $M \longrightarrow \dfrac{M}{N}$ is a surjective morphism.

If $I \trianglelefteq R$ is an R-submodule of R, then R/I is an R-module. We have $\operatorname{Ann}(R/I) = I$.

Fact: Every ideal in R is the annihilator of some R-module.

Fact: Suppose R is a ring such that every every nonzero R-module is faithful, then R is a field. The converse also holds.

General idea: we study rings by looking at modules over them.

For an R-module M and $S \subset M$, then we can consider $\langle S \rangle$ the R-submodule generated by S. We can write this as

$$\bigcap_{N \text{ s.t. } S \subset N \subseteq RM} N = \left\{ \sum_{i=1^n} r_i s_i \;\middle|\; r_i \in R, s_i \in S \right\}.$$

We say R is finitely generated iff there exists a finite generating set $S \subset M$. We say M is cyclic iff it is generated by a single element, i.e. $M = \langle s \rangle$.

Let $\{M_i\}_{i\in I}$ be a family of R-modules. Let $\prod_{i\in I} M_i$ be the cartesian product with a coordinate-wise R-action be the direct product. Let

$$\bigoplus_{i\in I} M_i = \left\{(x_i) \in \prod M_i \;\middle|\; x_i \neq 0 \text{ for finitely many } i\right\},$$

which is a submodule of $\prod M_i$. When I is finite, these are equal.

Recall: If R is a PID and M is a finitely generated R-module, then there exist finitely many cyclic R- modules $\{C_1, \cdots, C_n\}$, then $M \cong \bigoplus C_i$.

Exercise: Let R be a ring and C a cyclic R-module, then show that $C \cong R/\mathrm{Ann}(C)$ as R-modules.

We'll later see that the class of rings R such that every R-module is free are exactly fields.

Remark: Let $I \trianglelefteq R$, then I is cyclic as an R-module iff I is principal.

Exercise:

a. Let $I \trianglelefteq R$ for R a domain, then I is indecomposable, i.e. $I \neq M_1 \oplus M_2$ for any nonzero M_1, M_2 R-modules.

b. If R is additionally Noetherian and not a PID, then there exists an $I \trianglelefteq R$ where I is finitely generated, not principal, and so I is not a cyclic R-module.

Converse to structure theorem! Mild assumptions negate cyclic direct sum decomposition.

8 Wednesday January 29th

Coming up: the modules $\bigoplus \mathbb{Z}, \hom_R(M,N), M \otimes_R N$, as well as various properties:

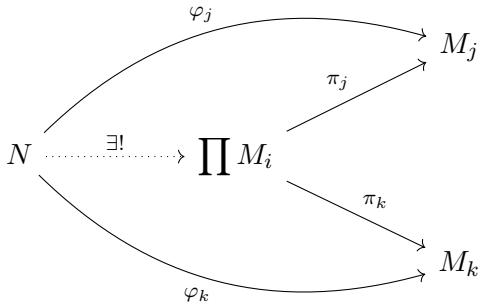
- Torsion
- Torsionfree
- Free
- Projective
- Flat
- Injective
- Divisible

We have a series of implication

$$\text{free} \implies \text{projective} \implies \text{flat} \implies \text{torsionfree}$$

8.1 Universal Mapping Properties

Definition 8.0.1 (Direct Product of Modules)**.**
For a collection $\{M_i\}$ of modules, the **direct product** is characterized by

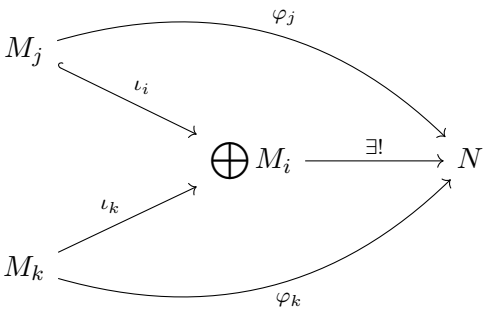


Here we define the canonical projection by $\pi_j(m_1, \cdots, m_j, \cdots) = m_j$.

Fact

$$\hom_R(N, \prod M_i) = \prod \hom_R(N, M_i)$$

Definition 8.0.2 (Direct Sum of Modules)**.**
For a collection $\{M_i\}$ of modules, the **direct sum** is characterized by



Here we define the canonical *injection* by $\iota_j(m) = (0, 0, \cdots, m, 0, \cdots)$. In this case, we can define $\phi(m_1, m_2, \cdots, m_i, \cdots) = \sum \phi_i(m_i)$, which makes sense because cofinitely many of the terms in this sum are zero.

Fact

$$\hom_R(\bigoplus_{s\in S} R, N) = \prod_{s\in S} \hom_R(R, N) = N^S$$

Fact $\hom_R(R, N) \cong N$ via the map $f \in \hom(R, N) \mapsto f(1)$.

8.2 Free Modules

Definition 8.0.3 (Spanning, Linear Independence, and Basis)**.**
For M an R-module and $S \subset M$,

1. S *spans* M if $\langle S\rangle = M$, where $\langle S\rangle$ is the set of all finite linear combinations of elements in S.
2. S is R-linearly independent iff $\sum r_i m_i = 0 \implies r_i = 0$ for all i.
3. S is a *basis* for M iff S is a spanning R-linearly independent subset of M.

If M admits a basis, M is said to be *free*.

Theorem 8.1 ***(Free Modules are Quotients).***

a. If $S = \{s_i\}$ is a basis for M, then there is a surjection

$$\bigoplus_{s\in S} R \longrightarrow M$$
$$r_i \longmapsto \sum r_i s_i.$$

b. For any set S, the module $\bigoplus_{s\in S} R$ has a canonical basis

$$\mathbf{e}_s = (0, 0, \cdots, 0, 1, 0, \cdots, 0)$$

c. If $\phi : \bigoplus_{s\in S} R \longrightarrow M$ is an isomorphism, then $\{\phi(\mathbf{e}_s)\}_{s\in S}$ is a basis for M.

Fact Let F be a free R-module, then $\operatorname{Ann}(F) = R$ if $F = (0)$ and 0 otherwise. Moreover,

- $\operatorname{Ann}(\bigoplus M_i) = \bigcap \operatorname{Ann}(M_i)$
- $\operatorname{Ann}(R) = \{0\}$

Proposition 8.2 ***(Characterization of Freeness in terms of Rings).***
For a ring $R \neq 0$, TFAE:
a. Every R-module is free
b. R is a field

Proof .
$a \implies b$: If R is not a field, then $0 < I \trianglelefteq R$ is proper, and since $\operatorname{Ann}(R/I) = I$, we have $0 < \operatorname{Ann}(R/I) < R$. So $\operatorname{Ann}(R/I)$ is proper, and R/I is thus not a field.
The reverse implication is linear algebra. Every vector space has a basis by AOC (note that this is equivalent to Zorn's Lemma).
■

Fact Every R-module N is the quotient of a free module.

This follows by taking the generating set $S = N$, then $\bigoplus_{n\in N} R \twoheadrightarrow N$ using a previous fact.

Fact N is quotient of a finitely generated free module iff N is finitely generated.

Exercise Show that for $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ a SES of R-modules,

a. If A, C are finitely generated, then so is B.

b. If B is finitely generated, then so is C.

Example 8.1.
It is possible for B to be finitely generated with $A < B$ and A not finitely generated. Let R be non-Noetherian. Equivalently, there exists $I \trianglelefteq R$ that is not finitely generated. So take

$B = R$ and $A = I$. For example, take $M = C([0,1], R)$ the module of continuous functionals, which is non-Noetherian.

Examples of non-Noetherian rings:

1. $\{R_i\}$ where each R_i is infinite and ???; then $\prod R_i$ is non-Noetherian.
2. For k a field, $T = \left\{ t_n \;\middle|\; 1 \leq n < \infty \right\}$, take $R = k[T]$. Then $I = \langle T \rangle$ is not finitely-generated.

Fact If R is a Noetherian ring, then every finitely generated R-module is a Noetherian module.

Example 8.2.
Take $R, M = \mathbb{Z}$, which are free modules, and $S = \{2\}$. Note that S is R-linearly independent in M, but can not be extended to a basis, and $\langle S \rangle = 2\mathbb{Z} \neq \mathbb{Z}$. Similarly, $S' = \{2, 3\}$ can not be reduced to a basis, while $\langle S' \rangle = \mathbb{Z}$.

Question: can M have basis sets of different cardinalities? Answer: sometimes, commutative rings have the *invariant basis property*.

9 Friday January 31st

9.1 Tensor and Hom

Let M, N be R-modules, then we define

$$\hom_R(M, N) \coloneqq \left\{ f : M \longrightarrow N \;\middle|\; f \text{ is an } R\text{-module map} \right\}.$$

Recall that R-module maps satisfy

- $f : (M, +) \longrightarrow (N, +)$ a morphism of abelian groups
- For all $r \in R$, for all $m \in M$, $f(rm) = rf(m)$.

Note that $\hom_R$ is a commutative group, and is in fact an R-module with structure given by $(r \cdot f) \cdot m \mapsto rf(m) = f(rm)$.

Note that the proof of this fact uses commutativity in a key way.

Facts:

$$\begin{aligned} \hom_R(R, N) &= N \\ \hom_R\left(\bigoplus_{s \in S} R_s, N \right) &= N^S \\ \hom_R(M, R) &\coloneqq M^\vee. \end{aligned}$$

Note: Infinite dimensional vector spaces over fields are never isomorphic to its dual.

Exercise: Think about $M^\vee$ and $(M^\vee)^\vee$.

Recall the map

$$\begin{aligned} \iota : M &\longrightarrow (M^\vee)^\vee = \hom_R(\hom_R(M,R),R) \\ x &\mapsto (\ell : M \longrightarrow R \mapsto \ell(x) \in R). \end{aligned}$$

Exercise: If $R = k$ is a field, then show that ι is injective iff $\dim M$ is finite.

Is this always injective? No! Counterexample: Take $R = \mathbb{Z}$ and $M = \mathbb{Z}/p\mathbb{Z}$, then $M^\vee = \hom_{\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}) = 0$.

It can also fail to be surjective in the infinite dimensional case – the space $M^\vee$ is strictly larger than M.

Definition 9.0.1 (Reflexive Modules)**.**
M is *reflexive* if $\iota : M \xrightarrow{\sim} (M^\vee)^\vee$ is an isomorphism.

Exercise: Show the following:

- If M is free and finitely generated, then M is reflexive.
- If $R = k$ is a field, then M is reflexive iff M is finitely generated.
- There exists a ring R and a reflexive R-module M that is not finitely generated.

9.2 Free Torsion Modules

Let R be a domain, and for all $a \in R^\bullet$ the map $[a] : R \longrightarrow R$ is injective, and $[a] \in \hom_R(R,R) = R$.

Definition 9.0.2 (Torsion Submodule)**.**

$$M[\text{tors}] \coloneqq \left\{ m \in M \;\middle|\; \operatorname{Ann}(m) \neq (0) \right\} \leq M$$

is the **torsion submodule** of M.

Definition 9.0.3 (Torsion and Torsionfree Modules)**.**
M is **torsion** iff $M = M[\text{tors}]$, and M is **torsion-free** iff $M[\text{tors}] = (0)$.

Exercise Show that if $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$, then

- Show that if B is torsion then A, C are torsion.
- If A, C are torsion, must B be torsion?
- Show that if B is torsion-free then A is torsion-free but C need not be torsion-free.
- If A, C are torsion-free, must B be torsion-free?

Note: $0 \longrightarrow \mathbb{Z}/2 \longrightarrow \mathbb{Z}/4 \longrightarrow \mathbb{Z}/2 \longrightarrow 0$ is an extension that isn't a semidirect product!

Fact Free modules are torsion-free.

Note that we need to be in a domain to even talk about torsion.

Proposition 9.1 ***(Torsionfree implies submodule of f.g free).***
Let R be a domain and M an R-module. Then
a. $M/M[\text{tors}]$ is torsion-free.
b. If M is finitely generated, then M is torsion free iff M is isomorphic to a submodule of a finitely-generated free module.

Proposition 9.2 ***(Implication Chain).***
Free $\implies$ projective $\implies$ flat $\implies_{R \text{ a domain}}$ torsion-free.

Proof (of (a)).
Let $x \in M/M[\text{tors}]$ such that $\exists r \in R^\bullet$ such that $rx = 0$. Lift x to $\tilde{x} \in M$, then $r\tilde{x} \in M[\text{tors}]$. Then $\exists r' \in R^\bullet$ such that $0 = r'(r\tilde{x}) = (r'r)\tilde{x} \coloneqq r_2\tilde{x}$ for some $r_2 \neq 0$. But then $\tilde{x} \in M[\text{tors}]$, and so $x = 0$ in $M/M[\text{tors}]$.

■

Proof (of (b)).
Let $M = \langle x_1, \cdots, x_r \rangle$ with $r \geq 1$ and $x_i \neq 0$. After reordering, there exists some s with $1 \leq s \leq r$ such that $x_1, \cdots, x_s$ are R-linearly independent, and for all $i > s$, $\{x_j\}_{j \leq s} \bigcup x_i$ is linearly *dependent*.
Then define $F \coloneqq \langle x_1, \cdots, x_s \rangle$; this is a finitely generated free module. If $r = s$, we done.
Otherwise, $r < s$, then $\forall i > r$ there exists an $a_i \in R^\bullet$ such that $a_i x_i \in F$. So we can take $a \coloneqq a_{s+1} \cdots a_r \neq 0$; then $aM \subset F$. Since M is torsion-free, the multiplication maps are injective, so $[a] : M \xrightarrow{\cong} M \subset F$, so $M \hookrightarrow F$ embeds M into a free module.

■

Does this work with M not finitely generated? No, we can't take an infinite product for a. Is every torsion-free module a submodule of a free module? No.

Remark This fails without finite generation, see Theorem 3.56 on ordinal filtration. If R is a PID and F is a free R-module and $M \leq F$ as an R-submodule, then M is free.

Thus if R is a PID, "subfree" $\iff$ free. Does torsion-free imply free? No, take $R = \mathbb{Z}$ and $M = (\mathbb{Q}, +)$, this is not finitely generated and torsion-free but not a free $\mathbb{Z}$-module.

Definition 9.2.1 (Divisible and Uniquely Divisible Modules)**.**
For R a domain, M is *divisible* if $\forall a \in M^\bullet$ iff $[a] : M \twoheadrightarrow M$ is a surjection. M is *uniquely divisible* if for all $a \in M^\bullet$, $[a] : M \xrightarrow{\cong} M$ is an isomorphism, i.e. M is torsion-free and divisible.

Exercise Show that $(\mathbb{Q}, +)$ is a uniquely divisible $\mathbb{Z}$-module.

Exercise Let R be a domain with fraction field K, with $R \neq K$. Show that a nonzero free R-module is not divisible but $(K, +)$ is a divisible torsion-free R-module. Thus $(K, +)$ is a torsion-free module R-module that is not free.

Remark: Finitely generated torsion free modules are embedded in free modules. Note that in the spectrum of properties earlier (projective, free, etc), the two extremes are equal for f.g. PIDs.

Exercise Let R be a Noetherian domain which is not a PID. Then an ideal $I \trianglelefteq R$ with I f.g., not principal, and a torsion-free R-module. Show that since I is not principal, I is not free as an R-module.

So ideals can't contain linearly independent elements, so they have to be free of rank 1 and thus principal. Thus finitely generated torsion-free is strictly *weaker* then free in this setting.

10 Monday February 3rd

Some module topics from Chapter 8.

10.1 Noetherian and Artinian Modules

Definition 10.0.1 (Noetherian Posets)**.**
A poset $(X, \leq)$ is said to satisfy the **ACC** or to be **Noetherian** iff there does not exist an infinite sequence (a chain) $\{x_n\}$ with strict inequalities $x_1 < x_2 < \cdots$. Equivalently, every weakly ascending chain $x_1 \leq x_2 \leq \cdots$ eventually stabilizes, i.e. there exists an N such that $x_N = x_{N+1} = \cdots$.

Definition 10.0.2 (Artinian Posets)**.**
Similarly, a poset satisfies the **DCC** or is **Artinian** iff there does not exist an infinite decreasing sequence $x_1 > x_2 > \cdots$.

Definition 10.0.3 (Order Dual)**.**
For $(X, \leq)$, define the **order dual** $(X^\vee, \leq)$ where $x \leq y \in X^\vee \iff y \leq x \in X$.

Proposition 10.1 ***(Noetherian/Artinian Duality).***
X is Noetherian iff $X^\vee$ is Artinian.

Lemma 10.2.
The ACC holds iff every nonempty subset has a maximum (and similarly the DCC with minimums).

Proof .
Otherwise use AOC to pick elements x_i; if x_i isn't the maximum then there is some $x_{i+1} > x_i$, and this yields an infinite ascending chain iff no maximum.
■

Let M be an R-module, and define $\mathrm{Sub}_R M = \{(R\text{-submodules of } M, \leq)\}$.

Lemma 10.3.
M is Noetherian $\iff$ every submodule $N \leq M$ is finitely generated.

Proof .
Apply the DCC.

■

Exercise Let $M' \subset M$ and $q : M \longrightarrow M/M'$ and $N_1 \subset N_2 \subset M$ such that

- $N_1 \bigcap M' = N_2 = M'$, and
- $q(N_1) = q(N_2)$.

Then $N_1 = N_2$.

Proposition 10.4 ***(2 out of 3 Property for Noetherian/Artinian).***
If $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ is exact and M is Noetherian (resp. Artinian) then M', M'' are both Noetherian (resp. Artinian).

Proof .
Note that $\mathrm{Sub}_R M', \mathrm{Sub}_R M'' \hookrightarrow \mathrm{Sub}_R M$ in an order-preserving manner. If we then have $N_1 \subset N_2 \subset \cdots$ with $N_i \leq M$ submodules of M, we can consider $N_n = \dfrac{N_n + M'}{M'}$, which is weakly increasing in M'.

■

Note: this is how we push forward into quotients.

Thus this chain stabilizes, so for $i, j \gg 0$ we have $N_i + M' = N_j + M'$. So then $N_i \bigcap M' = N_j \bigcap M'$, and by the exercise, $N_i = N_j$ for all $i, j \gg 0$.

Corollary 10.5.
R is Noetherian (resp. Artinian) iff every finitely-generated R-module is Noetherian (resp. Artinian)

Proof .
$\Longrightarrow$: Suppose R is Noetherian. Note that $0 \longrightarrow R \longrightarrow R^2 \longrightarrow R \longrightarrow 0$ since R^2 is an extension of R by R. Thus R^2 is Noetherian, and inductively R^n is a Noetherian R-module.

If M is a finitely-generated R-module, it is a quotient of a finitely-generated free R-module, and in particular $0 \longrightarrow K \longrightarrow R^n \longrightarrow M \longrightarrow 0$ is exact. So M is Noetherian, by the previous proposition (middle of a SES Noetherian $\Longrightarrow$ ends are Noetherian).

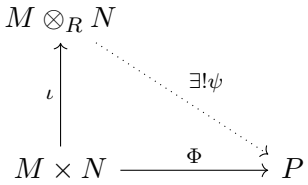
■

10.2 Tensor Products

Motivation from Representation Theory: For G finite, $H \leq G$, and $\rho : G \longrightarrow V$ a finite-dimensional $\mathbb{C}$-representation, this data is equivalent to a $\mathbb{C}[G]$-module structure on V. If W is a representation on H, then $\mathrm{Ind}_H^G W$ is a representation of G given by $V = \mathrm{Ind}_H^G W = W \otimes_{\mathbb{C}[H]} \mathbb{C}[G]$.

Definition 10.5.1 (Tensor Product)**.**
Let M, N be R-modules, then the **tensor product** $M \otimes_R N$ is an object characterized up to canonical isomorphism by the following universal property: If P is an R-module and $\Phi : M \times N \longrightarrow P$ is any bilinear map, then there exists a unique lift such that the following

diagram commutes:



where $\iota : M \times N \longrightarrow M \otimes_R N$ is R-bilinear and for all $(m, n) \in M \times N$, we denote $m \otimes n \coloneqq \iota(m, n)$.

By dimension counting in the finite-dimensional case of vector space, it's clear that ι need not be surjective. In general, elements in $M \otimes_R N$ are *finite sums* of simple tensors, not just simple tensors, i.e. $M \otimes_R N = \langle \iota(m, n) \rangle$.

Proof (existence).
Let F be the free R-module on $M \times N$ with basis $\left\{(m, n) \;\middle|\; m \in M,\ n \in N\right\}$. Mod out by the following relations: for all $m, m_1, M_2 \in M$ and for all $n, n_1, n_2 \in N$ and all $r \in R$,
■

- $(m_1 + m_2) \otimes n - m_1 \otimes n - m_2 \otimes n$
- $m \otimes (n_1 + n_2) - m \otimes n_1 - m \otimes n_2$
- $r(m \otimes n) - (rm) \otimes n$
- $r(m \otimes n) - m \otimes (rn)$

Let $\mathcal{R}$ be the ideal generated by these relations, the define $M \otimes_R N = F/\mathcal{R}$ by $(m, n) \mapsto (m, n) + \mathcal{R}$. Then (straightforward check) the universal mapping property holds.

How do we work with tensor products? Namely, how do we even know whether an arbitrary element is zero or not in this complicated quotient.

- To show $m \otimes n = 0$, use bilinear relations (reduce to relations above)
- To show $m \otimes n \neq 0$, find an R-module and a bilinear map $\psi : M \otimes_R N \longrightarrow P$ such that $\operatorname{im}(m \otimes n) \neq 0$.
- To show $M \otimes_R N \cong X$, show that X satisfies the universal property.

Exercise $R \otimes_R M \equiv M$ by $(r, m) \mapsto r \cdot m$, with $\cdot$ the R-module action on M. Let P be arbitrary, let $\phi : R \times M \longrightarrow P$ be arbitrary, and define $\psi : M \longrightarrow P$ by $m \mapsto \phi(1, m)$.

Exercise $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \equiv \mathbb{Z}/\gcd(n, m)\mathbb{Z}$. Show that every element is both n-torsion and m-torsion.

Proposition 10.6 ***(Existence of Base Change).***
For M and R-module and $f : R \longrightarrow S$, we can create an S-module $S \otimes_R M$ by *base change*.

Definitely the most important concept thus far!

11 Wednesday February 5th

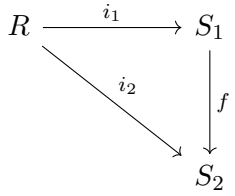
Recall that if M, N are R-modules then there is a map $M \times N \xrightarrow{\Phi} M \otimes_R N$ where $(r, m) \mapsto r \otimes m$ which is universal wrt the property that any bilinear map $\phi : M \times N \longrightarrow A$ factors through Φ

uniquely.

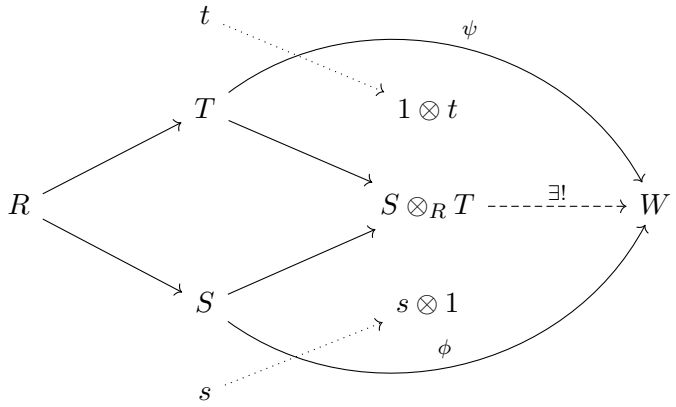
We have a notion of *pullback*, where if $i : R \longrightarrow S$ and N is an S-module then i^*N is an R module with action given by composition $R \xrightarrow{i} S \dot{\to} \mathrm{End}_{\mathbb{Z}}(N)$.

Dually, we have a notion of *base change*, where for M an R-module we can form $i_*M \coloneqq S \otimes_R M$ an S-module where $s(\sum s_i \otimes m_i) = \sum ss_i \otimes m_i$.

An R-algebra is $i : R \longrightarrow S$ a ring morphism, where algebra morphisms $f : S_1 \longrightarrow S_2$ are given by commutative diagrams



For S, T R-algebras, the tensor product $S \otimes_R T$ is an R-algebra with $(s_1 \otimes m_1) \cdot (s_2 \otimes m_2) = s_1 s_2 \otimes m_1 m_2$. Note that the tensor product satisfies the universal property of the direct sum or coproduct:



Exercise Verify the following identities

One: Let M be an R-module and N an S-module with $\iota : R \longrightarrow S$. $\hom_R(M, \iota^*N) = \hom_S(\iota_*M, N) = \hom_S(S \otimes_R M, N)$. What's the map? $s \otimes m \mapsto sf(m)$.

Two: For P and R-module and M, N S-modules, we have $M \otimes_X (i^*N \otimes_R P) = i^*(M \otimes_S N) \otimes_R P$. So for $N = S$, then $M \otimes_S (S \otimes_R P) = M \otimes_R P$.

Three (Good Exercise! Very important!): For M an R-module and $I \trianglelefteq R$, we have $IM \subset_R M$. Show that we can identify the base change as $R/I \otimes_R M = M/I$.

Hint: Show that the RHS satisfies the appropriate universal property.

Four:

- $(\oplus M_i) \otimes_R N = \oplus(M_i \otimes_R N)$.
- The tensor product of free modules is free.
- If F is a free R-module and we base change with $\iota : R \longrightarrow S$ then $S \otimes_R F$ is a free S-module.

Definition 11.0.1 (Invariant Basis Number)**.**
Let R be a ring, then R satisfies the *invariant basis number property* (IBN) iff any two bases for a free left R-module have the same cardinality.

Definition 11.0.2 (Rank Condition)**.**
R satisfies the *rank condition* iff whenever there exists a $q : R^m \twoheadrightarrow R^n$, $n \leq m$.

Definition 11.0.3 (Strong Rank Condition)**.**
R satisfies the *strong rank condition* iff whenever $q : R^m \hookrightarrow R^n$ then $n \leq m$.

Facts If R is commutative or (left)-Noetherian, then strong rank condition $\implies$ rank condition $\implies$ IBN.

Note: this is not obvious, since if R is not Noetherian there are submodules that aren't finitely generated but can still have bounded rank.

Exercise (Non-Commutative) Let k be a field and V an infinite dimensional k-vector space, i.e. $V \cong V \oplus V$. Let $R \coloneqq \mathrm{End}_k(V)$; then R does not satisfy the IBN.

Proposition 11.1 ***(Commutative Rings have Invariant Basis Number).***
If R is nonzero and commutative then R satisfies IBN.

Proof .
Suppose there exist I, J such that $\oplus_{i\in I} R \cong_R \oplus_{j\in J} R$. We want to show that $|I| = |J|$. Since $R \neq 0$, there is a maximal ideal $\mathfrak{m} \in \mathrm{maxSpec}\ (R)$. Since $R/\mathfrak{m}$ is a field, we base change to it to obtain $R/\mathfrak{m} \otimes_R (\bigoplus_{i\in I} R) = \bigoplus_{i\in I} R/\mathfrak{m}$. We know this equals $R/\mathfrak{m} \otimes_R (\bigoplus_{j\in J} R) = \oplus_{j\in J} R/\mathfrak{m}$. So I, J are bases of isomorphic vector spaces and thus $|I| = |J|$ by linear algebra.
■

Definition 11.1.1 (Noetherian and Artinian Modules)**.**
A module M is *Noetherian* iff ACC on submodules, and *Artinian* iff DCC on submodules.

Exercise If $R = k$ is a field and V is a k-vector space, then V is Noetherian iff Artinian iff infinite-dimensional.

Exercise If $R = \mathbb{Z}$, R is Noetherian but not Artinian. Find a $\mathbb{Z}$-module that is Artinian but not Noetherian.

Try all 2^n possibilities for adjectives!

Exercise If R is finite, it is both Artinian and Noetherian, and moreover has only finitely many ideals.

Artinian is much stronger, and implies Noetherian? Converse iff every ideal is maximal. The only Artinian integral domains are fields. Very small class of rings. It's not true that Artinian alone implies finitely many ideals.

Exercise (8.29 in Notes) Let $I = (x^2, xy, y^2) = (xy)^2 \trianglelefteq \mathbb{C}[x, y]$ and take $R = \mathbb{C}[x, y]/I$.

a. Show that a $\mathbb{C}$-basis for R is given by $\{1 + I, x + I, y + I\}$.

b. Deduce that R is Noetherian and Artinian.

c. Show proper ideals of R are precisely the $\mathbb{C}$-subspaces of $\langle x, y\rangle + I$.

d. Deduce that $\mathbb{R}$ has continuum many ideals.

12 Friday February 7th

12.1 Projective Modules

For X a topological space and $\pi : E \longrightarrow X$ a real vector bundle on X. Then $\Gamma(E, X) = \left\{\sigma : X \longrightarrow E \;\middle|\; \pi \circ \sigma = \mathrm{id}_X\right\}$ is naturally a module over the ring $C(X, \mathbb{R})$ of continuous real-valued functions. For $p \in X$, the fibers $\sigma(p) \in \pi^{-1}(p)$ are vector spaces, and we can consider $f(p)\sigma(p)$ for any $f \in C(X, \mathbb{R})$. For trivial bundles $\mathbb{R}^n \times X \xrightarrow{\pi} X$ with a global section

$$\begin{aligned} \sigma : X &\longrightarrow \mathbb{R}^n \times X \\ p &\mapsto (\tilde{\sigma}(p), p). \end{aligned}$$

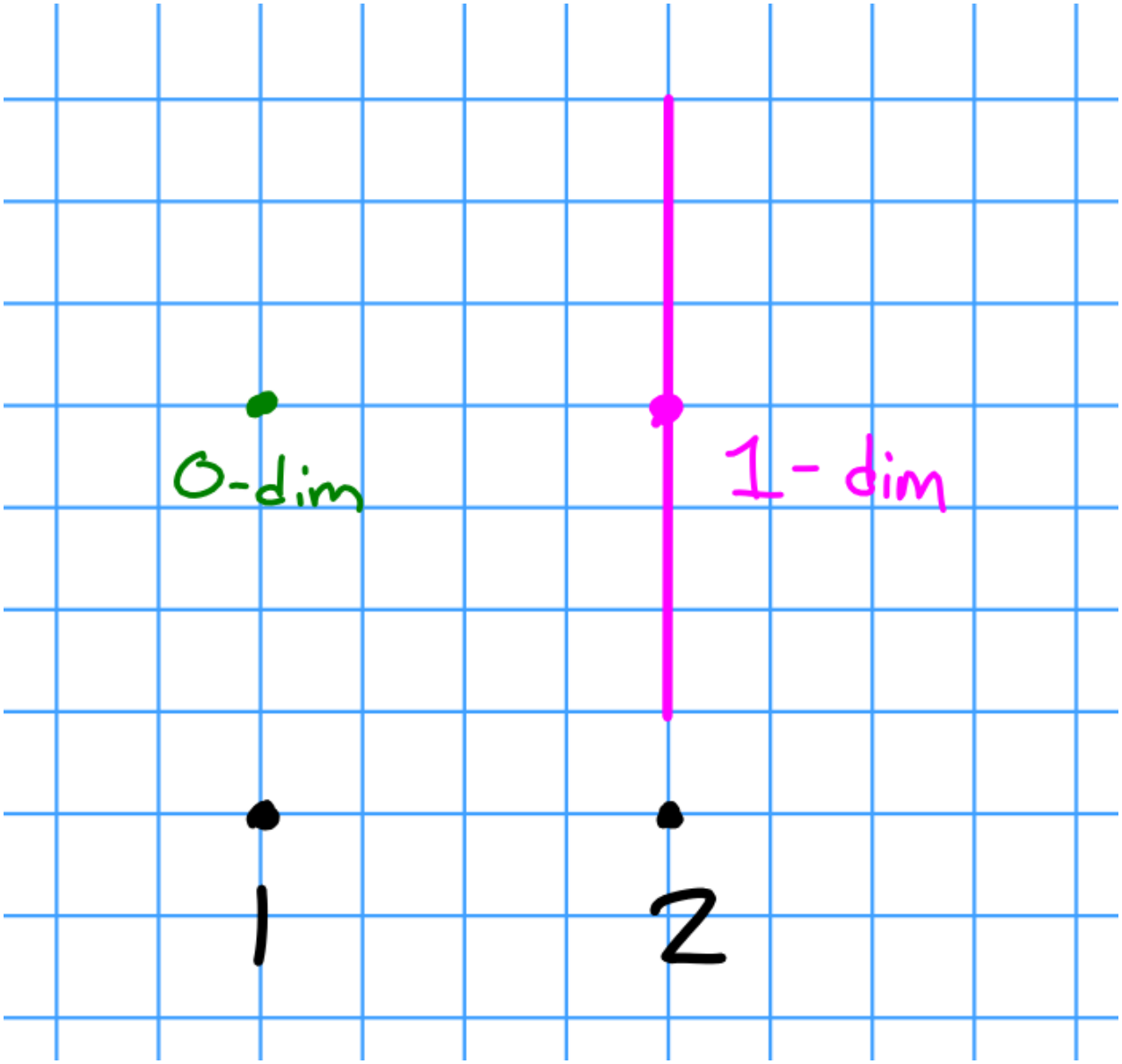
Then $\tilde{\sigma} : X \longrightarrow \mathbb{R}^n$, or equivalently a collection of n continuous functions $\tilde{\sigma}_j \longrightarrow \mathbb{R}$. Thus $\Gamma(X, E) \cong C(X, \mathbb{R})^n$.

Theorem 12.1 ***(Swan).***
Suppose X is compact. Then

a. $\Gamma(X, E)$ is a finitely generated projective $C(X, \mathbb{R})$-module, i.e. π is a direct summand of a trivial vector bundle on X, and

b. There is an equivalence of categories between vector bundles on X and finitely generated projective $C(X, \mathbb{R})$-modules.

Example 12.1.
Let X be the two points space $\{1, 2\}$. Take a 0-dimensional vector space over 1 and a 1-dimensional vector space over 2.



Remark Such cheap examples exist on X iff X is disconnected.

Definition 12.1.1 (Splitting an Exact Sequence)**.**
Recall that it $0 \longrightarrow A \longrightarrow B \xrightarrow{f} C \longrightarrow 0$ is exact, then a **splitting** is a map $\sigma : C \longrightarrow B$ such that $f \circ \sigma = \mathrm{id}_C$. Then $B = A \oplus \sigma(C) \cong A \oplus C$.

Exercise Take $R = \mathbb{Z}$ and find a SES such that $B \cong_{\mathbb{Z}} A \oplus B$ but the sequence is *not* split.

Definition 12.1.2 (Projective Module)**.**
A module P is **projective** iff $0 \longrightarrow M \longrightarrow N \longrightarrow P \longrightarrow 0$ is split.

Exercise Show that free implies projective.

Hint: Lift basis and use universal property.

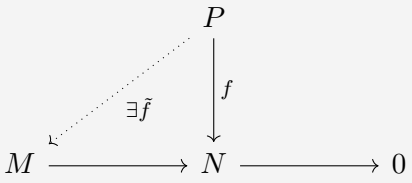
Theorem 12.2 ***(Projective is Direct Summand of Free).***
If P is projective, then there exists a K such that $P \oplus K$ is free.

Idea: summands can be *both* a submodule and a quotient module.

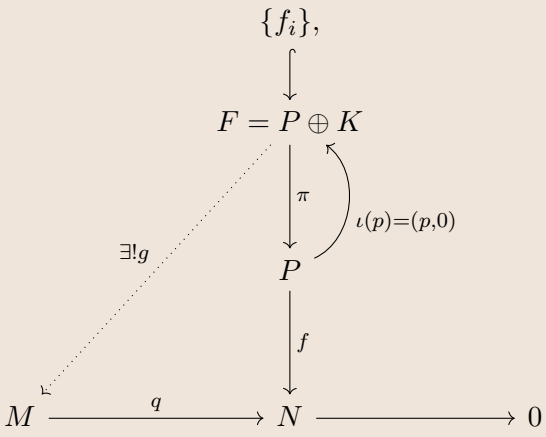
Proof .
Choose a free F and an R-module surjection $q : F \twoheadrightarrow P$ with $K = \ker q$ to obtain $0 \longrightarrow K \longrightarrow F \longrightarrow P \longrightarrow 0$. Since P is projective, this sequence splits and thus $F \cong K \oplus P$ is free.
■

Comment: If P is finitely generated, then we can take K (and hence F) to be finitely generated module. A quotient of a finitely-generated module is also finitely generated, and $F \cong K \oplus P$.

Theorem 12.3 ***(Lifting Property of Projectives).***
If there exists a K such that $P \oplus K$ is free, then P satisfies this lifting property:



Proof .
Choose K such that $P \oplus K$ is free, and let $\{f_i\}_{i \in I}$ be a basis for F. Then write $F = P \oplus K$ and $f_i = p_i + k_i$ where $p_i \in P, k_i \in K$. Then we can construct a unique $g : F \longrightarrow M$ by sending f_i to m_i:



$\{m_i\}$ $\{n_i\}$

Then $q \circ g \circ \iota = (q \circ g) \circ \iota = (f \circ \pi) \circ \iota = f \circ (\pi \circ \iota) = f$ since ι is a section.
■

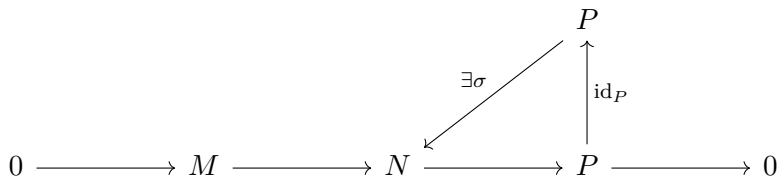
Todo: Revisit!

This P is projective iff

- Every length 2 resolution of P splits.

- P is a direct summand of a free module.
- P satisfies this lifting property.

If P satisfies this lifting property, we have:



Exercise Show free implies projective in as many ways as you can (using any of these properties).

Remark An easy consequence of the lifting property implies that the functor $M \mapsto \hom_R(P, M)$ is covariant and exact.

Natural question: for any new property of modules, is there a class of rings for which this coincides with known properties?

Question: How different is projective from free?

Free $\implies$ projective $\implies$ subfree $\implies_{R \text{ a domain}}$ torsion-free.

For R a PID and M finitely generated, these are all equivalent (hence the diminished importance of projectivity when studying the structure theorem). Recall (Theorem 3.56) that if R is PID, then subfree $\implies$ free and projective $\iff$ free, but $(\mathbb{Q}, +)$ is torsion-free but not free.

Recall Spec $(R_1 \times R_2) =$ Spec $R_1 \coprod$ Spec R_2

Example 12.2 (Projective does not imply free):*)**.**
Let R_1, R_2 be rings and consider $R = R_1 \times R_2$. Then recall that $I \trianglelefteq R$ implies $I = I_1 \times I_2$ for $I_i \trianglelefteq R_i$. Take $M_1 \coloneqq R_1 \times 0 \trianglelefteq R$, and $M_2 \coloneqq 0 \times R_2 \trianglelefteq R$.

Then $M_1 \oplus M_2 = M_1 + M_2 = R$, so both R_i are projective. They are not free though, since $\text{Ann} M_1 = M_2$ and vice-versa.

Example 12.3.
Let $R = \mathbb{C} \times \mathbb{C}$, so Spec $R = \{1, 2\}$, then $M_1 = \mathbb{C} \times 0 \longrightarrow$ Spec R, and we can construct "cheap" bundles in analogy to the disconnected topological case.

Next question: What is an example of a nonfree projective module over a domain.

13 Wednesday February 12th

13.1 Projective Modules and Ideals

Summary: Free $\implies$ projective $\implies$ flat $\implies_{R \text{ a domain}}$ torsion free. Moreover, projective $\implies$ reflexive.

If M, N are cyclic R-modules, then $\operatorname{Ann}(M \otimes_R N) = \operatorname{Ann}M + \operatorname{Ann}N$. Does this hold for every M, N? The answer is no; we have $\operatorname{Ann}(M \otimes_R N) \supseteq \operatorname{Ann}M + \operatorname{Ann}N$. See MSE post: let $I \trianglelefteq R$ and M an R-module, we have $M \otimes_R R/I = M/IM$. Is there an equality $\operatorname{Ann}(M/IM) = \operatorname{Ann}(M) + I$? No, take $R = \mathbb{C}[x, y]$.

Recall that an R-module is *reflexive* iff $\iota : M \longrightarrow (M^\vee)^\vee$ is an isomorphism, where $M^\vee = \hom_R(M, R)$. This is injective for R a field, and then surjective iff R is finite-dimensional. As shown in the problem sessions, finitely generated free modules are reflexive.

Exercise: Show that direct summands of reflexive modules are reflexive, and $M_1 \oplus M_2$ is reflexive iff M_i are reflexive. Conclude that finitely generated projective modules are reflexive.

Example 13.1.
To get a projective module that is not free, take $\mathbb{C}^2 = (\mathbb{C} \times 0) \oplus (0 \times \mathbb{C}) = \mathbb{C}^2$, which is free, so the summands are projective, but not free.

Note: this corresponds to taking a vector bundle over a disconnected space, and letting the fibers just be different dimensions.

Letting the summands above be I, J, note that $I + J = R$ and $IJ = 0$, which is a comaximality condition.

Lemma 13.1 ***(3.17).***
Let $I, J, K_1, \cdots, K_n \trianglelefteq R$. Then

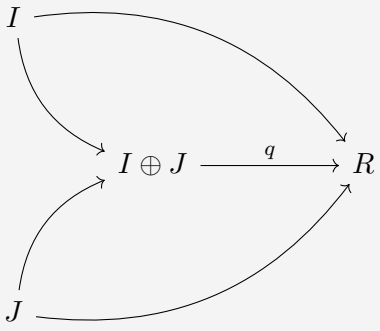
a. $(I + J)(I \bigcap J) \subseteq IJ$

b. If $I + J = R$ (so I, J are comaximal), then $I \bigcap J = IJ$.

c. If $I + k_i = R$ for all $1 \leq i \leq n$ then $I + K_1 \cdots K_n = R$.

Proof .
Omitted.
■

Theorem 13.2 ***(First Isomorphism Theorem for Rings).***
Let R be a domain, $IJ \trianglelefteq R$ such that $I + J = R$. We can form a map:



where

$$\begin{aligned} q : I \oplus J &\longrightarrow R \\ (i,j) &\mapsto i+j. \end{aligned}$$

Then

a. q is surjective

b. $\ker q = \left\{(x,-x) \;\middle|\; x \in I \bigcap J\right\} \cong_R I \bigcap J = IJ$.

c. There is a SES $0 \longrightarrow IJ \longrightarrow I \oplus J \xrightarrow{q} R \longrightarrow 0$, and since R is projective, $I \oplus J \cong_R IJ \oplus R$.

d. If IJ is principal (so $IJ \cong_R R$) then I is projective.

See "monogenic". This gives a criterion for determining if ideals are projective.

Exercise Let $R = \mathbb{Z}[\sqrt{-5}]$ with $\mathfrak{p}_1 = \left\langle 3, 1+\sqrt{-5} \right\rangle$ and $\mathfrak{p}_2 = \left\langle 3, 1-\sqrt{-5} \right\rangle$.

a. Show that $R/\mathfrak{p}_1 \cong R/\mathfrak{p}_2 \cong \mathbb{Z}/3\mathbb{Z}$.

b. Show $\mathfrak{p}_1 + \mathfrak{p}_2 = R$.

c. Show $\mathfrak{p}_1\mathfrak{p}_2 = \langle 3 \rangle$.

d. Show neither $\mathfrak{p}_1, \mathfrak{p}_2$ are not principal.

e. Conclude $\mathfrak{p}_1 \cong_R \mathfrak{p}_2$ is a finitely generated projective but *not* free R-module.

13.2 The Picard Group

Definition 13.2.1 (Picard Group)**.**
Let R be a domain with fraction field K, we'll define *picard group* Pic (R) in the following way: For $I \trianglelefteq R$ with $I \neq 0$. we say I is invertible iff there exists a $J \trianglelefteq R$ such that IJ is principal. Then Pic (R) is the set of invertible ideals modulo the equivalence $I \sim J$ iff there exist $a, b \in R^\bullet$ such that $\langle a \rangle I = \langle b \rangle J$.
This is a group under $[I] + [J] = [IJ]$ (check that this is well-defined).

Note that if I is principal, then $[I] = 1$ is the identity, and if $IJ = \langle x \rangle$, then $[I][J] = [\langle x \rangle] = 1$.

Fact If I is invertible, then I is a projective R-module.

Fact (Stronger) If $I \trianglelefteq R$ in a domain, then

- I is invertible iff I is a projective R-module.
- $[I] = 1$ in Pic R iff I is principal iff I is a free R-module.

Proof .
Later!
■

Every nontrivial element gives a projective but not free R-module! Note that Pic $R = 0$ for R a PID.

Definition 13.2.2 (Dedekind Domain and Class Group)**.**
R is a *Dedekind domain* iff every nonzero $I \trianglelefteq R$ is invertible, and Pic R is referred to as the *class group* of R.

In this case, Pic $R = 0$ iff every ideal is principal iff R is a PID.

So the class group measures how far R is from a PID. Any Dedekind domain that is not a PID yields projectives that aren't free.

Rings of integers over number fields are Dedekind domains.

> Embarrassingly open problem: are there are infinitely many number fields K such that the ring of integers $\mathbb{Z}_K$ is a PID, or equivalently Pic $\mathbb{Z}_K = 0$?

Example 13.2 (Important)**.**
Let k be a field and $n \in \mathbb{Z}^+$, and define $R \coloneqq k[t_1, \cdots, t_n]$. Since k is a PID, R is a PID, and every finitely generated module over a PID is free.

Theorem 13.3 ***(Bass, 1962).***
Let R be connected (recall: rules out silly case!) and noetherian. Then every infinitely generated (i.e. *not* finitely generated) projective module is free.

So we can restrict our attention to the finitely generated case.

> Analogy: is every topological vector bundle trivial? E.g. for $\mathbb{C}^n$, yes. Are all holomorphic bundles trivial? In general, no, see Stein manifolds.

Question (Serre, 1950s): Is every projective R-module free?

Answer: Yes, showed by Quillen, Suslin 1976. See book about this by T.Y. Lam.

Upcoming: Algebraic K-theory, built from f.g. projective R-modules. Trivial in K_0 doesn't quite imply free, usually weaker. Tries to analyze distinction between projective and free. Also some results about flat modules.

14 Friday February 14th

Let R be a ring and consider $K_0(R)$.

> Measures difference between f.g. projective and free modules over R.

Define $(M(R), +) \coloneqq$ the commutative monoid of isomorphism classes of f.g. projective R-modules with addition given by direct sum, i.e. $[P] + [Q] = [P \oplus Q]$ with identity the zero modules, and $K_0(R) = G((M(R), +))$ is the group completion, which any map $M(R) \longrightarrow G$ a group factors through.

Concretely, any element of $K_0(R)$ is of the form $[P] - [Q]$, where $[P_1] - [Q_1] \sim [P_2] - [Q_2]$ iff $[M] + [P_1] + [Q_2] = [M] + [P_2] + [Q_2]$ for every finitely generated projective R- module M. Note that excluding the R here fails transitivity and thus doesn't yield an equivalence relation.

If P, Q are finitely generated projective R-modules, then $[P] = [Q]$ iff $\exists M$ such that $P \oplus M \cong Q \oplus M$ iff there exists N a finitely generated projective such that $M \oplus N \cong R^n$ for some n, i.e. $P \oplus R^n \cong Q \oplus R^n$. In such a case, we say P, Q are stably isomorphic.

Note that $[P] = 0$ iff $[P]$ has rank zero, or $[P] \oplus R^n \cong R^n$. Also note that $[P] \cong [Q]$ can occur without necessarily having $P \cong Q$ as modules.

We can actually make $K_0(R)$ into a ring with $[P] \cdot [Q] \coloneqq [P \otimes_R Q]$.

> Note that the tensor product of two finitely-generated R-modules is still finitely generated as an R-module.

Example: Let R be a PID, then $M(R)$ is a commutative semiring (no additive inverses) and is equal to $(\mathbb{N}, +, \cdot)$ (occurs whenever)very finitely generated projective is free). Similarly $G(R) = (\mathbb{N}, +, \cdot)$. Since R has invariant basis number, there is always an injective group morphism

$$\begin{aligned}(\mathbb{Z}, +) &\mapsto (K_0(R), +) \\ n &\mapsto [R^n].\end{aligned}$$

> Yields no cancellation among free modules. We want to essentially ignore this case, so we'll mod out.

Definition 14.0.1 (Reduced Group)**.**
The reduced K group is given by $\tilde{K_0}(R) \coloneqq (K_0(R), +)/(\mathbb{Z}, +)$.

Note that $[P] = [G]$ in $\tilde{K_0}(R)$ iff there exist m, n such that $P \oplus R^m \cong Q \oplus R^n$. Moreover $[P] = 0$ iff $\exists m, n$ such that $P \oplus R^n \cong R^n$. In this case we say P is *stably free*.

Exercise If P is a projective module (possibly not finitely generated) then there exists a free module F such that $P \oplus F$ is free.

Example 14.1.
For $n \in \mathbb{Z}$, define $R_n \coloneqq \mathbb{R}[t_0, \cdots, t_n] / \left\langle \sum t_i^2 - 1 \right\rangle$. This is the ring of polynomial functions on the n-sphere. To construct a stably free module that is not free, take TS^n for any n for which it's trivial.

By Poincare Hopf, need euler characteristic zero, which happens when n is odd. Tangent bundle also trivial for lie groups.

Theorem 14.1 ***(Bott-Milnor).***
This happens iff $n \in \{1, 3, 7\}$.

If every module is free, they are stably free, yielding $K_0 = 0$.

Fact: If R is a dedekind domain, $\tilde{K_0}(R) = \text{Pic}\ (R)$, the ideal class group.

> So f.g. projectives need not be free, since ideals need not be principal. Theorem of Clayborn: Pic (R) can be any commutative group!

Analogy: bundles are locally trivial, are projective modules "locally free"? We'll need localization to make sense of this, but such a theorem turns out to be true.

Definition 14.1.1 (Local Ring)**.**
A local ring is a ring R with a unique maximal ideal, usually written $(R, \mathfrak{m})$.

Exercise R is local iff $R \setminus R^\times \trianglelefteq R$ is an ideal.

Localizing in the right way will yield local rings.

Lemma 14.2.
Let $q : R \longrightarrow R/\mathfrak{m}$ and $x \in R$, then $x \in R^\times \iff q(x) \in (R/\mathfrak{m})^\times$.

Proof .
The forward implication holds for any ring. The converse doesn't usually (think $\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z}$). But if $q(x) \in (R/\mathfrak{m})^\times = R/\mathfrak{m} \setminus 0$, then $x \in R \setminus \mathfrak{m} = R^\times$.
■

Theorem 14.3 ***(Projective Modules Over Local Rings are Free).***
A f.g. projective module over a local ring is free.

This turns out to be true with "f.g." dropped, but that is a harder theorem.

To prove this, we'll need the following:

Theorem 14.4 ***(Corollary of Nakayama's Lemma).***
For $(R, \mathfrak{m})$ a local ring and M a finitely generated R-module. Take a finite collection $\{m_i\}$ such that $\{\overline{m}_i\} \in M/\mathfrak{m}M$ are generators as an $R/\mathfrak{m}$ module. Then M is generated by $\{x_i\}$.

Usually identified *as* Nakayama's Lemma.

Proof (of first theorem).
Let P be a f.g. projective R-module for R a local ring. Choose Q such that $P \oplus Q = R^n$. By base change, $P/\mathfrak{m}P \oplus Q/\mathfrak{m}Q = (R/\mathfrak{m})^n$.
So choose $R/\mathfrak{m}$ bases $\{\bar{p}_i\}^a$ of $P/\mathfrak{m}P$ and $\{\bar{q}_j\}^b$ of $Q/\mathfrak{m}Q$. Choose any lifts $p_i \in P, q_j \in Q$. Let $A \in M_{n,m}(R)$ be the matrix formed by setting the first columns to p_i and the remaining to q_j. Then $\det(A) \mod \mathfrak{m} \in (R/\mathfrak{m})^\times$, and by the lemma, $\det(A) \in R^\times$ and thus A is invertible. So $\{p_i, q_j\}$ are R-linearly independent, so $\{p_i\}$ span P by Nakayama's lemma. Thus P is a free R-module.
■

14.1 Flat Modules

Why are projective modules called such? See notes, characterization in terms of linear algebra and projection operators.

Suppose we have a SES of R-modules and we tensor with some R-module M:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N_1 & \hookrightarrow & N_2 & \twoheadrightarrow & N_3 & \longrightarrow & 0 \\ \downarrow & & \downarrow & & \downarrow{\scriptstyle \cdot \otimes_R M} & & \downarrow & & \\ \cdots & \longrightarrow & \cdots & \longrightarrow & N_1 \otimes_R M & \longrightarrow & N_2 \otimes_R M & \twoheadrightarrow & N_3 \otimes_R M \longrightarrow 0 \end{array}$$

Note that the induced map of the injection need not remain an injection.

Example 14.2.
Take $\mathbb{Z} \mapsto \times 2\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z}$, then taking $\cdot \otimes \mathbb{Z}/2\mathbb{Z}$ yields $\mathbb{Z}/2\mathbb{Z} \xrightarrow{\times 2} \mathbb{Z}/2\mathbb{Z}$, which is the zero map.

Definition 14.4.1 (Flat Modules)**.**
A module M is **flat** iff $M \otimes_R \cdot$ is exact, i.e. if $N_1 \hookrightarrow N_2 \implies M \otimes_R N_1 \hookrightarrow M \otimes_R N_2$.

Proposition 14.5 ***(Flat Implies Torsionfree in Domains).***
If R is a domain, then flat $\implies$ torsionfree.

Proof .
For the contrapositive, suppose M is not torsionfree, then there exists some nonzero $r \in R^\bullet$ and $0 \neq m \in M$ such that $rm = 0$. Then take $R \xrightarrow{\times r} R$, which is injective since R is a domain. Then tensoring with M yields $M \xrightarrow{\times r} M$, which has nonzero kernel by assumption.
■

Exercise (Important) Let M_i be a family of R-modules, then $\bigoplus_i M_i$ is flat iff M_i is flat for all i.

Use the fact that tensor commutes with direct sum, use functoriality of direct sum to sum maps.

Proposition 14.6 ***(Projective Implies Flat).***
Projective $\implies$ flat.

We now have the chain:

$$\text{Free} \implies \text{projective} \implies \text{flat} \implies_{R \text{ a domain}} \text{torsionfree}.$$

Proof (easy).
By the exercise, P projective implies existence of a Q where $P \oplus Q$ is free, so it's enough to show that free $\implies$ flat. If F is free, $F \cong \oplus_i R$, so F is flat iff R is flat. But $R \otimes_R R = R$, which does not change a SES at all.
■

So flat is somewhere between projective and torsionfree.

The next theorem is related to Cayley-Hamilton.

Theorem 14.7 ***(Existence of Minimal Polynomials).***
Let M be a finitely generated R-module with generators $\{x_i\}$ and $I \trianglelefteq R$, and take $\phi \in \mathrm{End}_R(M)$ such that $\phi(M) \subseteq IM$. Then there exist a set of coefficients $\{a_i\}^n$ such that $\phi^n + a_{n-1}\phi^{n-1} + \cdots + a_1\phi + a_0 = 0 \in \mathrm{End}_R(M)$.

Proof (Sneaky).

For all $i \leq n$, there exists a set $\{a_{ij}\}_{j=1}^n \subset I$ such that $\phi(x_i) = \sum_{j=1}^n a_{ij}x_j$. Equivalently, for all i,

$$\sum_{j=1}^n (\delta_{ij}\phi - a_{ij}) = 0.$$

Let P be a matrix with entry i, j equal to $\delta_{ij}\phi - a_{ij} \in M_{n\times n}(R[\phi])$ where $R[\phi] \leq \mathrm{End}_R(M)$ is the subalgebra generated by ϕ. Note that this makes the base ring commutative, so this matrix makes sense. We can rewrite this as $P \cdot [x_1, x_2, \cdots, x_n]^t = 0$.
Claim: If S is a ring and $P \in M_{n\times n}(S)$, then there is an identity

$$P\mathrm{adj}(P) = \mathrm{adj}(P)P = \det(P)I_n.$$

> Note that expanding this in the 2×2 case yields a collection of polynomial identities, which tend to remain true in arbitrary rings (see "permanence of polynomial identities").

Then $\det(P)I_n\mathbf{x} = \mathrm{adj}(P)M\mathbf{x} = \mathbf{0}$ (often called **the determinant trick**). Thus $\det(P)x_i = 0$ for all i. But then $\det(P)M = 0$, and since M is a faithful $R[\phi]$-module, we have $\det(P) = 0$. Then thinking of ϕ as a variable, expanding the determinant yields a monic polynomial in ϕ with coefficients that are products of a_{ij}, which are in I.

■

Note the analogy to $\det(I\lambda - A)$, so this yields the usual characteristic polynomial in the case of fields.

Theorem 14.8 ***(NAK, a.k.a Nakayama-Azumaya-Krull).***
Let $J \trianglelefteq R$ be an ideal and $M \in \mathrm{R} - \mathrm{mod}$ finitely generated such that $JM = M$. Then
a. $\exists x \in R$ such that $x \cong 1 \mod J$ and $xM = 0$.
b. Suppose $J \in \mathcal{J}$ (the Jacobson radical), i.e. J is in every maximal ideal; then $M = 0$.

Note that if R were local, this reduces to a simple case.

Proof (of (a)).
Apply the previous proposition to $\phi = \mathrm{id}_M$ and $I = J$; then the polynomial relation reduces to the existence of some $x = 1 + a_{n-1} + \cdots + a_0$ with $a_i \in J$, and this is equal to the zero endomorphism and thus $xM = 0$ and $x = 1 \mod J$ as desired.

■

Proof (of (b)).
If $J \in \mathfrak{m}$ for all $\mathfrak{m} \in \mathrm{maxSpec}\ (R)$, then if $x = 1 \mod J$ and $x = 1 \mod \mathfrak{m}$, this forces $x \notin \mathfrak{m}$ and so $x \in R^\times$. So if $yx = 1$ and \$xM = 0 \$, then $0 = yxM = M$.

■

Corollary 14.9.
Suppose $J \in \mathcal{J}$ and $M \in \mathrm{R}-\mathrm{mod}$ is f.g. with $N \leq_R M$ a submodule such that $JM + N = M$, then $N = M$.

Proof .
Apply part (b) above to M/N. If M is f.g. then so is M/N, and $J(M/N) = \dfrac{JM+N}{N} = M/N$ (just from pushing into quotients).
■

Definition 14.9.1 (Non-generator)**.**
An element $x \in M$ is a *non-generator* if whenever S is a generating set for M, then $S \setminus x$ is still a generating set.

Thus if you're trying to find generators for a module, it never helps to add elements of J.

Corollary 14.10.
Let $J \in \mathcal{J}$, $M \in \mathrm{R}-\mathrm{mod}$ f.g., $x_1, \cdots, x_n$ such that $\{\bar{x}_i\} \in M/JM$ are generators. Then M is generated by $\{x_i\}$.

Proof .
Take $N = \langle \{x_i\} \rangle \leq M$. Then im $(N) \subset M/JM$ is given by im $(N) = \dfrac{N+JM}{JM} = \dfrac{M}{JM}$ since im (N) was assumed a generating set. But then $N = M$ by the previous corollary.
■

Theorem 14.11 ***(3.44, Generalized NAK).***
Let $J \trianglelefteq R$, $M \in \mathrm{R}-\mathrm{mod}$ f.g., then $JM = M \iff J + \mathrm{Ann}M = R$.

Proof .

$\impliedby$ $JM = M \iff M/JM = 0 \iff \mathrm{Ann}M/JM = R$, and $\mathrm{Ann}M/JM = \mathrm{Ann}(M \otimes R/J) \supseteq J + \mathrm{Ann}M = R$.
$\implies$: Exercise.
■

Exercise Why does this imply part (b) in NAK?

Use the assumption that $J, \mathrm{Ann}M$ are comaximal, and $J \in \mathcal{Z}$, which forces $\mathrm{Ann}M = R$ and thus $M = 0$.

15 Monday February 17th

Last time: R is a ring, M a finitely-generated R-modules, $J \trianglelefteq R$.

Theorem 15.1 ***(Nakayama).***
If $M = JM$, then there exists an $x \in R$ with $x = 1 \mod (J)$ such that $xM = (0)$.

Theorem 15.2 ***(Generalized Nakayama).***
$M = JM \iff J + \mathrm{Ann}M = R$.

Proof .
The reverse implication is immediate, the forward is by Nakayama.
■

15.1 Injective Modules

Exercise Show that for $R = R_1 \times R_2$ and $M = M_1 \times M_2$, M_i is an R_i-module.

Recall that every R-module is free $\iff$ R is a field.

Question: What is the analogous condition for every R-module to be projective?

Answer: Every SES

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$$

of R-modules splits.

Focusing on M_2: every submodule M_1 of M_2 is a direct summand.

Theorem 15.3 ***(Characterization of Semisimplicity).***
For an R-module M, TFAE

1. Every submodule of M is a direct summand.
2. M is a direct sum of simple modules (semisimple).
3. M is generated by its simple submodules.

Definition 15.3.1 (Simple Modules)**.**
M is **simple** iff $\exists 0 \subsetneq N \subsetneq_R M$.

In this case, $M \cong R/\mathrm{Ann}M$ (i.e. cyclic, monogenic) and the $\mathrm{Ann}M$ is maximal.

Proof .
Omitted, see chapter 8 of notes.
■

Thus every R-module is projective iff every R-module is semisimple.

Definition 15.3.2 (Injective Modules)**.**
Dually, now focusing on M_1, every SES starting with M_1 is split iff whenever $M_1 \leq M_2$, M_1 is a direct summand. In this case we say M_1 is *injective*.

Proposition 15.4 ***(Characterization of Semisimple Modules).***
For R a ring, TFAE

1. Every SES of R-modules splits
2. Every R-module is projective
3. Every R-module is semisimple
4. Every R-module is injective
5. (Claim) R is itself a semisimple R-module.

Proof .
$3 \implies 5$ is clear, and we'll prove $5 \implies 3$ shortly using *Baer's Criterion.*
■

Definition 15.4.1 (Semisimple Rings)**.**
R is **semisimple** iff for all $I \trianglelefteq R$, there exists a $J \trianglelefteq R$ such that $I \oplus J = R$. Moreover, $\operatorname{Ann}(I) = J$ and $\operatorname{Ann}(J) = I$.

Exercise (easy) If R_i are semisimple, $R_1 \times R_2$ is semisimple.

Corollary 15.5.
Fields are semisimple, so any finite product of fields is semisimple.

In fact, the converse is true:

Theorem 15.6 ***(Semisimple Rings are Products of Fields).***
If R is semisimple, then R is a product of fields.

Note that everything works here for left modules over non-commutative rings.

Let R be a ring.

Theorem 15.7 ***(Wedderburn-Artin).***
A ring[a] R is semisimple iff $R \cong \prod_{i=1}^{r} M_{n_i}(D_i)$ a product of matrix rings over division rings.

[a] Potentially non-commutative, but reduces to previous theorem in commutative case.

Let $0 \longrightarrow M_1 \xrightarrow{\iota} M_2 \longrightarrow M_3 \longrightarrow 0$ be a SES.

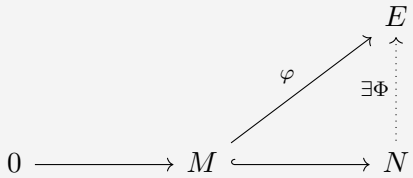
Note that splitting is slightly stronger than $M_2 \cong M_1 \oplus M_3$.

This sequence is split iff there exists a retraction $\pi : M_2 \longrightarrow M_1$ such that $\iota \circ \pi = \mathrm{id}_{M_2}$. In this case, $M_2 \cong \iota(M_1) \oplus \ker \pi$.

Definition 15.7.1 (Injective Modules)**.**
An R-module E is *injective* iff every SES $0 \longrightarrow E \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$ admits a retraction $\pi : M_2 \longrightarrow E$.

Theorem 15.8 ***(Characterization of Injective Modules).***
For an R-module E, TFAE
1. E is injective

2. Reversing arrows of projective condition, there exists a lift of the following form:



3. If $M \hookrightarrow N$, then $\hom(N, E) \twoheadrightarrow \hom(M, E)$.
4. The contravariant functor $\hom(\,\cdot\,, E)$ is exact.

Not big difference: no analog of being a direct summand of a free module! Free modules are usually not injective.

Example 15.1.
$\mathbb{Z}$ is a free but not injective $\mathbb{Z}$-module. Take $0 \longrightarrow \mathbb{Z} \xrightarrow{\times 2} \mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$. If this splits, we would have $\mathbb{Z} \cong \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ as $\mathbb{Z}$-modules.

Why isn't this true? $\mathbb{Z}$ is a domain, the LHS is torsionfree, and the RHS has torsion.

Example 15.2.
Suppose now R is a domain and not a field, then let a be a non-unit and run the same argument with multiplication by a. This would yield $R \cong R \oplus R/aR$, where the LHS is torsionfree and the RHS has torsion. So R itself need not be an injective R-module.

Definition 15.8.1 (Self-Injective Modules)**.**
A ring R is *self-injective* iff R is injective as an R-module.

Example 15.3.
A field or a semisimple ring.

Claim 15.9.
Let $\tilde{R}$ be a PID, π a prime element, $n \in \mathbb{Z}^+$, then take $R \coloneqq \tilde{R}/(\pi^n)$. Then R is self-injective.

Example 15.4.
Let $R = \mathbb{Z}/p^n\mathbb{Z}$, and let M be a finite p-primary commutative group (i.e. a p-group). Then $\exp M = p^n \iff \operatorname{Ann} M = (p^n)$. M is a faithful $\mathbb{Z}/p^n\mathbb{Z}$-module, so there exists an element $x \in M$ such that $\#\langle x \rangle = p^n$. There is a SES of $\mathbb{Z}/p^n\mathbb{Z}$-modules

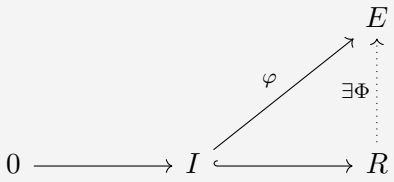
$$0 \longrightarrow \langle x \rangle \longrightarrow M \longrightarrow M/\langle x \rangle \longrightarrow 0.$$

Since $\langle x \rangle \cong \mathbb{Z}/p^n\mathbb{Z}$, which is self-injective, so there exists a module N such that $M = \langle x \rangle \oplus N \cong \mathbb{Z}/p^n\mathbb{Z} \oplus N$. Continuing on N yields a decomposition of M into a sum of cyclic submodules.

Conclusion: a finitely generated torsion module over a PID is a direct sum of cyclic modules.

In general, to show a module is injective, we need to consider lifts over all pairs of modules $M \hookrightarrow N$. How to do this in practice?

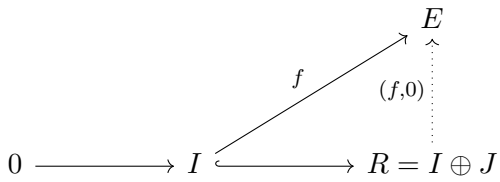
Theorem 15.10 ***(Baer's Criterion).***
If suffices to check the lifting condition for $N = R$ and $M = I \trianglelefteq R$. I.e. if there is a lift of the following form:



then E is injective.

Proof .
Omitted for time.
■

Application Let R be a semisimple R-module and let E be any R-module. Let $I \trianglelefteq R$, and $f \in \hom(I, E)$. If R is semisimple, then there exists a $J \trianglelefteq R$ such that $R = I \oplus J$. So extend f to $f \oplus 0$, which yields a lift:



Exercise Prove the claim that R is self-injective for $R = \tilde{R}/(\pi^n)$ above.

16 Monday February 24th

16.1 Divisible Modules

We know that injective implies divisible, and uniquely divisible implies injective. Fact: quotients of divisible modules are divisible

Exercise If R is a domain that is not a field and M is a finitely-generated divisible R-module, then $M = 0$.

Proof (of exercise).
Claim: for any ring R, any nonzero f.g. R-module M has a nonzero cyclic (monogenic) quotient given by modding out by all but one of the generators. Thus if M admits a finitely generated

divisible R-module, it admits a cyclic module.
Then $M \cong R/\mathrm{Ann}M$, and there are two cases:

- $\mathrm{Ann}M = 0$, in which case $M \cong R$. Then choosing $r \in R^\bullet \setminus R^\times$, then $[r] : R \longrightarrow R$ is *not* a surjection.
- Otherwise, choose $x \in \mathrm{Ann}(M) \setminus \{0\}$. Then $\times x : R \longrightarrow R$ is the same map as $\times 0 : R \longrightarrow R$, so it is not surjective.

■

Fact: there is a classification of divisible (iff injective) $\mathbb{Z}$-modules:

- $(\mathbb{Q}, +)$, since the fraction field of any domain is divisible.
- $(\mathbb{Q}/\mathbb{Z}, +) = \bigoplus_{\text{primes}} \mathbb{Q}_p/\mathbb{Z}_p$, where $\mathbb{Q}_p/\mathbb{Z}_p = \lim \mathbb{Z}/p^n\mathbb{Z}$. This is isomorphic to the group of p power roots of unity. On the other hand, $\mathbb{Q}/\mathbb{Z}$ is the group of *all* roots of unity

Fact (Classification of Divisible $\mathbb{Z}$-Modules: Any divisible $\mathbb{Z}$-module is isomorphic to a direct sum of copies of

- $(\mathbb{Q}, +)$
- $(\mathbb{Q}_p/\mathbb{Z}_p, +)$

Note that any direct sum of divisible groups is still divisible. Moreover, this decomposition is unique.

16.2 Toward Localization

Proposition 16.1 ***(Multiplicative Avoidance).***
Let $S \subset R$ with $SS \subset S$, $1 \in S$, $0 \notin S$. Define $\mathcal{I}(S) = \left\{ I \trianglelefteq R \;\middle|\; I \bigcap S = \emptyset \right\}$. Then

1. $\mathcal{I}(S) \neq \emptyset$
2. Every element of $\mathcal{I}(S)$ is contained in a maximal element of $\mathcal{I}(S)$.
3. Every maximal element of $\mathcal{I}(S)$ is prime.

Proof .
In parts:

a. $(0) \in \mathcal{I}(S)$ by construction.
b. Standard Zorn's lemma argument.
c. Let $I \in \mathcal{I}(S)$ be a maximal element, and let $x, y \in R$ such that $xy \in I$ with $x \notin I$. Then $\langle x, I\rangle \supsetneq I$, so $S \bigcap \langle x, I\rangle \neq \emptyset$ by maximality. I.e., there exists $s_1 \in S$ such that $s_1 = i_1 + ax$ for some $a \in R$. Continuing this way, if $y \notin I$, produce an $s_2 = i_2 + by_1$ for some $b \in R$. Since S is multiplicatively closed, $s_1 s_2 \in S$. But we also have $s_1 s_2 = (i_1 + ax)(i_2 + by) \in I$, a contradiction.

■

See Kaplansky's Commutative Algebra book.

Proposition 16.2 ***(Prime Ideals Behave Like Primes).***
Let $\mathfrak{p} \in \mathrm{Spec}\ (R)$ and $I_1, \cdots, I_n \trianglelefteq R$, then if $\mathfrak{p} \supset \prod I_i$, then $\mathfrak{p} \supset I_i$ for some i.

Proof .
Suppose $\mathfrak{p} \supsetneq I_i$ for any i, and let $x_i \in I_i \setminus \mathfrak{p}$. Consider $x := \prod x_i \in \prod I_i \subset \mathfrak{p}$; then since $\mathfrak{p}$ is prime, some $x_i \in \mathfrak{p}$.

■

Corollary: If $\mathfrak{p} \supset I^n$, then $\mathfrak{p} \supset I$.

I.e. prime ideals are radical.

16.3 Radicals

Definition 16.2.1 (Nilpotent Elements)**.**
An *element* $x \in R$ is *nilpotent* iff $x^n = 0$ for some $n \in \mathbb{Z}$. An *ideal* is *nilpotent* iff $I^n = (0)$ for some n, and is *nil* iff every element $x \in I$ is nilpotent.

Proposition 16.3 ***(Nilpotent Implies Nil).***
Nilpotent $\implies$ nil.

Proof .
If $I^n = (0)$, then for any $x \in I$, $x^n \in I^n = (0)$ so $x^n = 0$.

■

Proposition 16.4 ***(Nil and f.g implies nilpotent).***
If I is finitely generated and nil, then I is nilpotent.

Proof .
Let $I = \langle x_1, \cdots, x_n \rangle$. Then for each i, choose $e_i \in \mathbb{Z}$ such that $x_i^{e_i} = 0$. The (check) $I^{\sum e_i} = (0)$.

■

Definition 16.4.1 (Nil)**.**
An ideal is nil iff all generators are nilpotent.

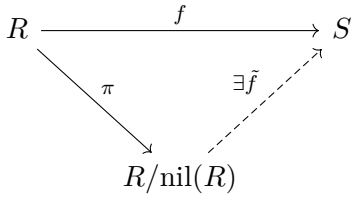
Corollary: If R is Noetherian, I is nilpotent iff I is nil.

Exercise Exhibit a ring with an ideal that is nil but not nilpotent. (Note: need to choose a non-Noetherian ring, e.g. a polynomial ring in infinitely many indeterminates $\{t_i\}$, and consider $\left\langle t_n^n \;\middle|\; n \in \mathbb{N} \right\rangle$.

Definition 16.4.2 (Nilradical)**.**
The *nilradical* of R, $\operatorname{nil}(R)$, is the set of all nilpotent elements.

Proposition 16.5 ***(Universal Property of Nil).*** a. $\operatorname{nil}(R) \trianglelefteq R$, since $a^n = b^n = 0 \implies (xa + yb)^{2n} = 0$.

b. $R/\operatorname{nil}(R)$ is reduced, and this quotient map is universal wrt morphism into a reduced ring. I.e., if $R \longrightarrow S$ with S reduced, there is commutative diagram



c. $\operatorname{nil}(R) = \bigcap_{\text{prime ideal}} \mathfrak{p}$.

Proof (of c).
$\subseteq$: If $x \in \operatorname{nil}(R)$, then $x^n = 0$ for some n, so $x^n \in \mathfrak{p}$ and since $\mathfrak{p}$ is prime, $x \in \mathfrak{p}$.
$\subseteq$: We'll show that if x is not nilpotent, then it avoids some prime ideal. Define $S \coloneqq \left\{x^n \;\middle|\; n \in \mathbb{N}\right\}$; since x is not nilpotent, S is multiplicatively closed and does not contain zero, so by a previous result, there is some $\mathfrak{p} \in \operatorname{Spec}(R)$ such that $S \bigcap \mathfrak{p} = \emptyset$.

■

Definition 16.5.1 (Radical Ideals)**.**
An ideal $I \trianglelefteq R$ is *radical* iff for all $x \in R$ there exists an n such that $x^n \in I \implies x \in I$.

Proposition 16.6 ***(Prime Implies Radical).***
Prime ideals are radical.

Idea: the set of radical ideals is much easier to work with than the set of prime ideals.

17 Wednesday February 26th

17.1 Radicals

For R a ring, we defined $\operatorname{nil}(R) \coloneqq \left\{x \in R \;\middle|\; \exists n \in \mathbb{N},\ x^n = 0\right\} \trianglelefteq R$. We had a theorem: $\operatorname{nil}(R) = \bigcap_{\mathfrak{p} \in \operatorname{Spec}(R)} \mathfrak{p}$.

Definition 17.0.1 (Radical of an Ideal)**.**
(Flat Implies Torsionfree in Domains)
For $I \trianglelefteq R$, we define $\operatorname{rad}(I) = \left\{x \in R \;\middle|\; \exists n,\ x^n \in I\right\} \supseteq I$.

Fact $I \trianglelefteq R$. To see this, note that for any $I \trianglelefteq R$, then $\operatorname{nil}(R/I) \trianglelefteq R = \operatorname{rad}(I)$.

Definition 17.0.2 (Radical Ideals)**.**
I is a *radical ideal* iff $I = \operatorname{rad}(I)$.

Example 17.1.
Prime ideals are radical.

Definition 17.0.3 (Closure Operators)**.**
Define a *closure operator* $\ell : I \mapsto \text{rad}(I)$. In general, if $(X, \leq)$ is a poset, then a Moore closure operator is a map $c : X \longrightarrow X$ satisfying

1. $c(c(x)) = c(x)$
2. $x \leq c(x)$
3. $x \leq y \implies c(x) \leq c(y)$.

This is most often applied to X the family of subsets of a set A and $\leq$ subset inclusion. Note that this doesn't completely correspond to a topological closure, since this would also require preservation of intersections.

Related to Galois connections, not covering in this class but good for a final topic.

We can produce a nice characterization: $\text{rad}(I) = \text{nil}(R/I) = \bigcap_{\mathfrak{p} \in R/I} \mathfrak{p} = \bigcap_{\mathfrak{p} \supseteq I} \mathfrak{p}$

Exercise (easy) If $\{I_i\}$ is any family of radical ideals, then $\bigcap_i I_i$ is radical.

Exercise Let $R = \mathbb{Z}$. What are the radical ideals? $(0), (p)$, but (p^2) is not radical – i.e. $(0), (n)$ for n squarefree.

Fact I is radical iff R/I is reduced. Noting that by the CRT, $\mathbb{Z}/n\mathbb{Z} \cong \prod \mathbb{Z}/p_i^{a_i}\mathbb{Z}$, which is reduced iff $a_i = 1$ for all i. If R is a PID, $\pi_1 \cdots \pi_r$ radical ideals, then $(\pi_1 \cdots \pi_r)$ nonassociate prime elements ??

Exercise Let R be a ring, $\mathfrak{p}_1 \neq \mathfrak{p}_2$ prime ideals.

1. Must $\mathfrak{p}_1\mathfrak{p}_2$ be radical?
2. If $\mathfrak{p}_1 + \mathfrak{p}_2 + R$, then $\mathfrak{p}_1\mathfrak{p}_2 = \mathfrak{p}_1 \bigcap \mathfrak{p}_2$, and is thus radical.

Product may be smaller than intersection in general.

Proposition 17.1 ***(Algebraic Properties of Radicals).***
Let $I, J \trianglelefteq R$.

a. $I \subset \text{rad}(I)$, $\text{rad}(\text{rad}(I)) \subset \text{rad}(I)$, and $I \subset J \implies \text{rad}(I) \subset \text{rad}(J)$.

b. $\text{rad}(IJ) = \text{rad}(I \bigcap J) = \text{rad}(I) \bigcap \text{rad}(J)$

c. $\text{rad}(I + J) = \text{rad}(\text{rad}(I) + \text{rad}(J))$

d. $\text{rad}(I) = R \iff I = R$

e. $\text{rad}(I^n) = \text{rad}(I)$ for $n \geq 1$

f. If R is Noetherian and $J \subset \text{rad}(I)$, then $J^n \subset I$ for some $n \geq 1$.

So for Noetherian rings, two radicals are equal iff powers of each ideal land in the other.

Proof (of (b)).
$IJ \subseteq I \bigcap J$ and thus $\text{rad}(IJ) \subset \text{rad}(I \bigcap J)$. If $x \in \text{rad}(I \bigcap J)$, there exists an n such that

$x^n \in I \bigcap J$. Then $x^{2n} = x^n x^N \in IJ \implies x \in \operatorname{rad}(IJ)$.

■

Proof (of b).
Since $I \bigcap J \subset I, J$, we have $\operatorname{rad}(I \bigcap J) \subset \operatorname{rad}(I) \bigcap \operatorname{rad}(J)$. If $x \in \operatorname{rad}(I) \bigcap \operatorname{rad}(J)$, then $x^n \in I, x^m \in J$ for some n, m, so $x^{m+n} \in I \bigcap J \subset \operatorname{rad}(I \bigcap J)$.

■

Proof (of (f)).
By replacing R with R/I, assume $I = (0)$, then $J \in \operatorname{nil}(R)$ and since R is Noetherian, J is nilpotent and $J^n = (0)$ for some n.

■

So we simplify things by passing from I to $\operatorname{rad}(I)$. There is a class of rings for which it's feasible to understand all *radical* ideals, and hopeless to understand *all* ideals.

Example 17.2.
Take $R = \mathbb{C}[x]$, a PID. Suppose $I \trianglelefteq R$ and $\operatorname{rad}(I) = x^n$, then $I = (x^n)$. So this is no big deal, it's just an extra integer parameter.

Now instead take $R = \mathbb{C}[x, y]$, and let $I = \langle x, y \rangle$. Note that applying (f) above to $J = \operatorname{rad}(I)$, we find that $I \supset \langle x, y \rangle^n$ for some n. But note that $\langle x, y \rangle^n = \left\langle x^n, x^{n-1}y, \cdots, xy^{n-1}, y^n \right\rangle$.

Exercise Suppose $I \supset \langle x, y \rangle^2$. For such I, $\dim_{\mathbb{C}} R/I < \infty$. So for each d, try to find all ideals I such that $\operatorname{rad}(I) = \langle x, y \rangle$ and $\dim_{\mathbb{C}} R/I = d$.

Note that these correspond to "fat points" in algebraic geometry. The idea $\langle x, y \rangle$ corresponds to a fat point at zero. When doing AG, we hope to restrict attention entirely to radical ideals.

Definition 17.1.1 (Jacobson Radical)**.**
The *Jacobson radical* is defined by $\mathcal{J}(R) = \bigcap_{\mathfrak{m} \in \operatorname{maxSpec}(R)} \mathfrak{m}$.

Fact $\mathcal{J}(R) \supset \operatorname{nil}(R)$, since not every prime ideal is maximal.

Example 17.3.
If $(R, \mathfrak{m})$ is a local domain, then $\operatorname{nil}(R) = 0$ and $\mathcal{J}(R) = \mathfrak{m}$.

Exercise Let R be a domain, show that $\mathcal{J}(R[t]) = (0)$.

Proposition 17.2 ***(Characterization of Jacobson Radical in Terms of Units).***
$x \in \mathcal{J}(R) \iff 1 \pm xR \subset R^\times$.

Exercise Show directly that $x^n = 0 \implies \forall y, 1 - xy \in R^\times$.

18 Friday February 28th

18.1 Radicals: The Jacobson Radical

Definition 18.0.1 (The Jacobson Radical)**.**
$\mathcal{J}(R) = \bigcap \mathfrak{m} \in \text{maxSpec } (R)\mathfrak{m}$.

For a noncommutative ring, instead of intersecting just two-sided ideals, need to intersect either left ideals *or* right ideals (the intersections turn out to be equivalent).

Fact If R is finite dimensional over a field, then $\mathcal{J}(R) = 0 \iff R$ is semisimple. By Wedderburn, this happens iff $R = \prod M_{n_i}(D_i)$.

Definition 18.0.2 (Semiprimitive)**.**
A ring is *semiprimitive (or $\mathcal{J}$-semisimple or Jacobson-semisimple)* iff $\mathcal{J}(R) = 0$.

Proposition 18.1 ***(Characterization of Jacobson Radical).***
$x \in \mathcal{J}(R) \iff 1 - xR \subset R^\times$.

Proof .
Let $x \in \mathcal{J}(R)$ and suppose $1 - xy \notin R^\times$, so $1 - xy \in \mathfrak{m}$ for some maximal ideal. But then $x \in \mathfrak{m}$, so $xy \in \mathfrak{m}$, so $1 = \mathfrak{m} + xy \in \mathfrak{m}$, a contradiction.
■

Suppose instead that $x \notin \mathcal{J}(R)$, so there exists some maximal such that $\langle m, x\rangle = R$. Thus for $y \in R, m \in \mathfrak{m}$, we have $1 = m + xy$ so $1 - xy = m \in \mathfrak{m}$ and thus $1 - xy \notin R^\times$.

In other words, $R^\times + \mathcal{J}(R) \subset R^\times$, and is the largest ideal with this property. Thus the elements are "close to zero" in the sense that it doesn't take you outside of the unit group.

18.2 Proposition (Commutative Algebra Analog of Euclid IX.20: Infinitely Many Primes)

Let R be a domain, then recall that $p \in R^\bullet$ is irreducible iff $p \notin R^\times$ and $p = xy \implies x \in R^\times$ or $y \in R^\times$. If p is irreducible and $u \in R^\times$, then up is irreducible and associate to p, and $(up) = (p)$.

Define an *atom* to be the principal ideal generated by an irreducible element.

Define a *Fursentenberg domain* to be a domain such that $x \in R^\bullet \setminus R^\times$ has an irreducible divisor. Note that we have a chain of implication, UFD $\implies$ Noetherian = ACC $\implies$ ACC on principal ideals $\implies$ nonzero nonunits factor into irreducibles (atomic domain) $\implies$ Fursentenberg. So this is a weak factorization condition.

Exercise Let $R = \text{Hol}(\mathbb{C})$ be the ring of holomorphic functions, which is a domain by the identity theorem. Show that R is semiprimitive, Furstenberg but not atomic.

Theorem 18.2 ***(Euclidean Criterion).***
Let R be a domain, not a field, and semiprimitive.

a. There exists a sequence of pairwise comaximal elements $\{a_n\}_n^\infty$ such that $\langle a_m, a_N\rangle = R$ for $m \neq n$.
b. If R is Forstenburg, then there is a sequence of primitive pairwise comaximal *irreducible* elements, and thus infinitely many atoms.

Note that applying this to $R = \mathbb{Z}$, the only unit ideals are generated by ± 1, and the result follows immediately.

Proof .
Exercise.

■

For what class of rings does this criterion apply?

Application For R a Noetherian domain, then by Hilbert's basis theorem $R[t]$ is Noetherian and semiprimitive. So by the above result, $R[t]$ is has infinitely many elements. Most interesting for $R = \mathbb{F}_q$, since for e.g. $R = \mathbb{R}$ we can consider ideals $(x - r)$.

Fact

a. If $I, J \trianglelefteq R$ and $r(I) + r(J) = R$, then $I + J = R$, and $r(r(I)) + r(J) = r(I + J)$.
b. If $I, J_1, \cdots, J_n \trianglelefteq R$ and $I + J_i = R$ for each i, then $I + \prod I_i = R$.
c. Suppose $I_1, \cdots, I_n$ are pairwise comaximal, then $\prod I_i = \bigcap I_i$ (note: could be smaller and general).

Theorem 18.3 ***(Chinese Remainder).***
Suppose R is arbitrary with $I_1, \cdots, I_n \trianglelefteq R$ pairwise comaximal. Then there is a natural map

$$\begin{aligned}\Phi : R &\longrightarrow \prod_{i=1}^n R/I_i \\ r &\mapsto (r + I_1, \cdots, r + I_i).\end{aligned}$$

1. Φ is surjective, and $\ker \Phi = \bigcap I_i$.
2. By pairwise primality, $R/\prod I_i \cong \prod R/I_i$.

Note that as modules, both sides are cyclic.

Proof .
By induction on n, with trivial base case.
Let $R' \coloneqq \prod_{i=1}^{n-1} R/I_i$ and assume by induction that $\Phi' : R \longrightarrow R'$ is surjective by induction. Let $(r', \bar{s}) \in R' \times R/I_n$. By hypothesis, $\ker \Phi' = \prod_{i=1}^{n-1}$. So there exists an $r \in R$ such that $\Phi'(r) = r'$.
Lifting to $s \in R$ such that $s + I_n = \bar{s} + I_n$.

By assumption, $I' + I \coloneqq \left(\prod_{i=1}^{n-1} I_i\right) + I_n = R$. So there exist $x \in I', y \in I_n$ such that $s - r = x + y$. Note that $\Phi'(r+x) = r'$ since $x \in \ker \Phi$, so

$$r_x = r + x + y = x \mod I_n.$$

But then $\Phi(r+x) = (r', s)$.

■

Exercise (Converse to CRT (Good for Problem Sessions)) Let $I_1, \cdots, I_n \trianglelefteq R$. If $\prod R/I_i$ is a cyclic R-module, then the I_i are pairwise comaximal.

Immediately reduce to $n = 2$ case. Also a nice proof using tensor products, use characterization of $R/I \otimes R/J$.

18.3 Monoid Rings

Here let R be a ring* (potentially noncommutative) and $(M, \cdot)$ a monoid (i.e. a group without requiring inverses).

Goal: we want to define a *monoid ring* $R[M]$.

If M is finite, the definition is unambiguous, but for infinite M we require an extra condition. In this case we define the *big monoid ring* $R[[M]]$.

Example 18.1.
For R a nonzero ring and $M = (\mathbb{N}, +)$, $R[M] = R[t]$, and $R[[M]] = R[[t]]$.

Step 1: suppose M is finite, then $R[M] =_{\mathrm{R-mod}} R^M = \{f : M \longrightarrow R\}$, the set of *all* functions. Note that $(f+g)(m) = f(m) + g(m)$, and define a new multiplication $(f * g)(m) \coloneqq \sum_{(x,y) \in M^2,\ xy = m} f(x)g(y)$, the *convolution product*. One must check that this actually satisfies the axiom of a ring, since we are building this by hand. This is a ring iff R is a ring and $(M, *)$ is commutative.

There is an identity, namely $1 \mapsto 1$ and $x \mapsto 0$ for $x \neq 1$. Distributivity isn't difficult, but we need to check that $*$ is associative. This follows from $((f * g) * h)(m) = \sum_{x,y,z \in M^3,\ xyz = m} f(x)g(y)h(z) = (f * (g * h))$.

Define $[m] \cdot [n] = [mn]$, then check that $\left(\sum_{m \in M} r_m [m]\right)\left(\sum_{m \in M} s_m [m]\right) = ?$.

19 Monday March 2nd

19.1 Semigroup and Monoid Rings

For today, let R be a ring*, so not necessarily commutative, and $(M, \cdot)$ be a nonzero monoid, we then define the monoid ring $R[M]$ by the following condition:

If M is infinite and *divisor-finite*, i.e. for all $m \in M$, the set $\{(x, y) \in M^2 \mid xy = m\}$ is finite.

Note that M finite implies divisor-finite, and M a group and divisor-finite implies finite.

For S a set, the free commutative monoid on S is given by $\bigoplus_{s \in S}(\mathbb{N}, +)$.

Example 19.1.
$(\mathbb{Z}^{>0}, \cdot) = \bigoplus_{n=1}^{\infty}(\mathbb{N}, +)$ by the fundamental theorem of arithmetic. The map is given by

$$M = \prod_{i=1}^{n} {p_i}^{t_i} \mapsto (t_i).$$

We define the *big monoid ring* $R[[M]]$. Note that $R[M]$ and $R[[M]]$ are commutative iff R, M are commutative. For $R[M]$, we try $R[M] = R^M = \{f : M \longrightarrow R\}$ with pointwise addition and instead of point wise multiplication, we take the *convolution product*

$$(f * g)(m) \coloneqq \sum_{xy=m} f(x)g(y).$$

Note that this is a finite sum $\iff$ M is divisor-finite. Moreover, if M is divisor-finite, then this defines $R[[M]]$.

For any M, we define $R[M]$ as above not R^M but rather $\bigoplus_{m \in M} R \subset R^M$, i.e. those $f : M \longrightarrow R$ with finite support, so for all f, $\{m \in M \mid f(m) \neq 0\} < \infty$.

Note that this makes the convolution product again a finite sum.

For M divisor-finite, $R[M] \hookrightarrow R[[M]]$, but in general the latter is larger.

Define $[m] = \delta_m$, and expand $f = \sum_{m \in M} r_m[m]$. Forming the product fg comes down to defining what $[m_1] * [m_2] \coloneqq [m_1 m_2]$ should be. We saw that this yields an associative product, since both ways of associating parentheses yield a sum that ranges over triples.

For $M = (\mathbb{N}, +)$, we find $R[M] = \sum_n r_n[n]$ where $[n] * [m] \coloneqq [n + m]$, so we can define $[n] \coloneqq t^n$, so this is $R[t]$.

More generally, take $M = \bigoplus_{s \in S}(\mathbb{N}, +)$ for S an arbitrary set, then

$$R[M] \coloneqq R[\{t_s \mid s \in S\}]$$

is a multivariate polynomial ring.

Consider also $M = (\mathbb{Z}, +)$. Since this construction should be functorial, there should be a containment $R[(\mathbb{Z}, +)] \supset R[(\mathbb{N}, +)] = R[t]$. In this case, $M \cong R[t, t^{-1}]$, the ring of Lauren polynomials.

We can also identify $R[[(\mathbb{N}, +)]] = R[[t]]$ is the ring of formal power series over R, since we're dropping the finiteness condition.

Note that $R = \mathbb{Z}$ is not divisor finite, so we can't necessarily take $R[[M]]$.

Proposition 19.1 ***(When Monoid Rings are Domains).***
For R a ring and $(G, +)$ a commutative group, $R[G]$ and $R[[G]]$ are domains iff R is a domain and G is torsionfree.

Note that R being a domain is necessary because it occurs as a subring via $r \mapsto r[1]$.

Proof (Idea).
See notes. If $g \in G[\text{tors}] \setminus \{0\}$, then $[g] - [0]$ is a zero divisor. ■

See Kaplansky's Group Ring Conjecture.

Exercise Let R be a field, identify the fraction field of $R[[t]]$. Should be formal, finite-tailed Lauren series – but what does this mean?

There is a universal property of monoid rings: Let R be a ring, $(M, \cdot)$ a commutative monoid. Let B be an R-algebra. Then $\hom_{\text{R}-\text{alg}}(R[M], B) = \hom_{\text{monoid}}(M, (B, \cdot))$ given by restriction.

Thus if $f : M \longrightarrow B$ is a monoid morphism, there exists a unique map

$$F : R[M] \longrightarrow B$$
$$\sum r_m[m] \mapsto \sum r_m f(m).$$

Note that this is the only possible map that could extend f.

Exercise Check that this gives an R-algebra morphism.

Note that the monoid ring is thus adjoint to the forgetful functor $\text{R} - \text{alg} \longrightarrow \text{Monoids}$.

Note that if $M = \bigoplus_{s \in S} (\mathbb{N}, +)$, then

$$\hom_{\text{Monoid}}(M, T) = \hom_{\text{Set}}(S, T),$$

i.e. it is fully determined by where it sends basis elements.

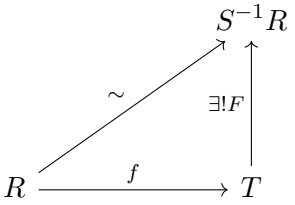
This yields a universal mapping property for polynomial rings, i.e. $\hom_{\text{R}-\text{alg}}(R[T], B) = \hom_{\text{Set}}(T, B)$.

19.2 Localization

Let $S \subset R$ with $SS \subset S$, with $1 \in S$, then there exists a ring $S^{-1}R$ and a ring morphism $\iota : R \longrightarrow S^{-1}R$ such that

1. For all $s \in S$, $\iota(s) \in (S^{-1}R)^\times$

2. ι is universal for property 1, i.e.



Remark: when R is a domain, this reduces to the fraction field construction, i.e. $(R^\bullet)R = K = ff(R)$. For S any multiplicatively closed subset,

$$S^{-1}R = R[\frac{1}{s} \;\Big|\; s \in S].$$

Make sense of partial group completion of a monoid with respect to a submonoid.

Construction: We'll define $S^{-1}R = (R \times S)/\sim$, where

$$(r_1, s_1) \sim (r_2, s_2) \iff \exists s \in S \text{ such that } sr_1s_2 = sr_2s_1.$$

Recall that this stabilization is needed, and becomes clear if you try to carry out the construction without it. If R is a domain, the s appearing can just be canceled.

Define maps

$$(r_1, s_1) + (r_2, s_2) \coloneqq (r_1s_2 + r_2s_1, s_1s_2)$$
$$(r_1, s_1) \cdot (r_2, s_2) \coloneqq (r_1r_2, s_1s_2)$$

Need to check that this is well-defined.

Exercise Check that localization satisfies the universal mapping property.

Question: what is $\ker(R \longrightarrow S^{-1}R)$ where $R \mapsto (r, 1)$? This has to do with the s that appears in the stabilization.

20 Wednesday March 4th

For R a ring and $S \subset R$ such that $S^2 \subset S$ and $1 \in S$, there exists a ring $S^{-1}R$ and a ring morphism $\iota : R \longrightarrow S^{-1}R$ such that

1. $\iota(S) \subset (S^{-1}R)^\times$, and
2. ι is universal for such morphisms, i.e every $R \xrightarrow{f} T$ with $f(S) \subset T^\times$ lifts to $S^{-1}R \xrightarrow{\tilde{f}} T$.

Last time we constructed it as $R \times S/\sim$ where $(r_1, s_1) \sim (r_2, s_2)$ iff there exists an $s \in S$ such that $sr_1s_2 = sr_2s_1$ (needed to obtain transitivity).

We then have $\iota(r) = [(r, 1)]$; what is its kernel? If $(r, 1) \sim (0, 1)$ then there exists $s \in S$ such that $s \cdot r \cdot 1 = s \cdot 1 \cdot 0 = 0$, so $\mathrm{Ann}(r) \bigcap \ker \iota \neq \emptyset$. Note that if $0 \in S$ then $\ker \iota = R$ and thus $S^{-1}R = 0$. Conversely, if $0 \notin S$, then $\mathrm{Ann}(1) \bigcap S = \emptyset$, so $S^{-1}R \neq 0$. Thus $S^{-1}R = 0$ iff $0 \in S$.

Example 20.1.
For $f \in R$, $R_f \coloneqq S_f^{-1}R$ where $S_f = \left\{1, f, f^2, \cdots\right\}$, then $R_f = 0 \iff f \in \mathrm{nil}(R)$.

Definition 20.0.1 (Saturated Multiplicatively Closed Sets)**.**
A multiplicatively closed set S is *saturated* iff for $s \in S, f \in R$ with f dividing S, then $f \in S$.
Denote the $\overline{S}$ the saturation of S obtained by adding all divisors, then $S^{-1}R = \overline{S}^{-1}R$.

Recall link to early problem of characterizing rings between $\mathbb{Z}$ and $\mathbb{Q}$. There are more localizations than such rings, since localizing at n is as good as localizing at kn.

If R is a domain, then for any S with $0 \notin S$, there is a diagram

$$\begin{array}{ccc} R & \hookrightarrow & S^{-1}R \\ & & \downarrow \\ & & K \end{array}$$

where $K = ff(R)$.

In any ring, take S to be the nonzero divisors, then there is a maximal injective localization.

$$\begin{array}{ccc} \iota R & \hookrightarrow & S^{-1}R \\ & & \downarrow \\ & & \text{Total fraction field} \end{array}$$

Can generalize results from domains to arbitrary rings this way.

Exercise Take R_1, R_2 nonzero rings, $R = R_1 \times R_2$, and take $S = R_1 \times \{1\}$. What is $S^{-1}R$? (First figure out the kernel of the localization.)

20.1 Pushing and Pulling

Note that we can push/pull for quotients and get back what we started with – want something similar for localization.

Consider the map $\iota : R \longrightarrow S^{-1}R$.

Lemma 20.1.
$I \trianglelefteq R$ implies that $\iota_*(I) = \left\{ \dfrac{x}{s} \;\middle|\; x \in I, s \in S \right\}$.

Proof .
Easy.
■

Proposition 20.2 ***(Push-Pull Equality for Ideals in Localizations).***
For all $J \trianglelefteq S^{-1}R$,

$$\iota_* \iota^* J = J.$$

Proof .
Note that we always have containment, just need to show reverse containment.
■

Lemma 20.3.
For $I \trianglelefteq R$,

$$i_*(I) = S^{-1}R \iff I \bigcap S \neq \emptyset.$$

Proposition 20.4 ***(Properties of Spec for Localization).***

a. For $\mathfrak{p} \in \text{Spec } (R)$, TFAE:
- $\iota_*\mathfrak{p} \in \text{Spec } (S^{-1}R)$
- $\iota_* \subsetneq S^{-1}R$
- $\mathfrak{p} \bigcap S = \emptyset$

b. If $\mathfrak{p} \bigcap S = \emptyset$, then $\iota^*\iota_*\mathfrak{p} = \mathfrak{p}$.

Corollary 20.5.
i^* and i_* are mutually inverse, order-preserving bijections

$$\text{Spec } (S^{-1}R) \underset{i_*}{\overset{i^*}{\rightleftarrows}} \left\{ \mathfrak{p} \in \text{Spec } (R) \;\middle|\; \mathfrak{p} \bigcap S = \emptyset \right\}.$$

Lemma 20.6.
For $I \trianglelefteq R$, S a multiplicatively closed set, let $f : R \twoheadrightarrow R/I$ be the quotient map and $\overline{S} \coloneqq q(S)$. Then

$$\begin{aligned} S^{-1}R/IS^{-1}R &\xrightarrow{\cong} \overline{S}^{-1}(R/I) \\ \frac{a}{s} + IS^{-1}R &\mapsto \frac{a+I}{s+I}. \end{aligned}$$

Thus localizing commutes with taking quotients.

Let $\mathfrak{p} \in \text{Spec } (R)$, then $S_\mathfrak{p} \coloneqq R\text{Set}minus\mathfrak{p}$ is multiplicatively closed. (Note that localizing at any non-prime ideal gives you the zero ring.) Let $R_\mathfrak{p} \coloneqq S_\mathfrak{p}^{-1}R$.

Proposition 20.7 ***(Complements of Prime Ideals are Local? Extremely Important!).***
$R_\mathfrak{p}$ is a local ring with a unique maximal ideal $\mathfrak{p}R_\mathfrak{p}$,

Proof .
The poset $\text{Spec } (R_\mathfrak{p}) = \left\{ q \in \text{Spec } (R) \;\middle|\; q \bigcap (R \setminus \mathfrak{p}) = \emptyset \iff q \leq \mathfrak{p} \right\}$.
■

This gives us a way to construct a local ring from *any* maximal ideal. Perhaps the most important construction thus far.

Exercise Let $(R, \mathfrak{m})$ be local and $S \subset R$ be multiplicatively closed. Show that $S^{-1}R$ need **not** be local.

20.2 Localization for Modules

Let M be an R-module and $S \subset R$ multiplicatively closed. We want $S^{-1}M$ to satisfy:

- $S^{-1}M$ is an R-module
- There is a morphism $M \longrightarrow S^{-1}M$ such that for all $s \in S$, the map $S^{-1}M \xrightarrow{[s]} S^{-1}M$ is an isomorphism, i.e. $S \longrightarrow \mathrm{End}_R(S^{-1}M)$ with $i(S) \subset \mathrm{End}_R(S^{-1}M)$
- This is universal wrt the above property.

There are two potential constructions.

Construction 1: Adapt the $S^{-1}R$ construction, defining $S^{-1}M = M \times S/\sim$.

Construction 2: Define $S^{-1}M \coloneqq S^{-1}R \otimes_R M$, where $\iota : M \longrightarrow S^{-1}M$ where $m \mapsto 1 \otimes m$.

It can be checked that these both satisfy the appropriate Universal mapping property.

Exercise If M is an R-module, then M has an $S^{-1}R$-module structure iff S acts invertibly (so $[s] : M \longrightarrow M$ is invertible), and if so the structure is unique.

21 Monday March 30th

We'll cover localization and Noetherian rings.

We'll need some local to global results.

Corollary 21.1.
If R is a domain with fraction field K, then

$$\bigcap_{\mathfrak{m} \in \mathrm{maxSpec}\ R} R_{\mathfrak{m}} = R$$

It follows from this that the analogous statement for prime ideals holds.

Proposition 21.2 ***(7.11 in the notes).***
Let $M_1, M_2 <_R M$ be sub R-modules of M, then $(M_1 :_M M_2) = \left\{ x \in R \;\middle|\; xM_2 \subseteq M_1 \right\}$ is equal to $\mathrm{Ann}\left(\frac{M_1 + M_2}{M_1}\right)$. So the colon is an ideal. Suppose that $S \subset R$ be a multiplicatively closed subset satisfying

a. If M is finitely generated, $S^{-1}\mathrm{Ann}M = \mathrm{Ann}S^{-1}M$.
b. If M_2 is finitely generated, then $S^{-1}(M_1 : M_2) = (S^{-1}M_1 : S^{-1}M_2)$.

Proof (of Proposition).
Omitted, see notes.

■

Proof (of Corollary).
We want to show that $R \hookrightarrow \bigcap R_{\mathfrak{m}}$. If $x \in K \setminus R$ and $I \coloneqq (R : Rx) \coloneqq \left\{ r \in R \;\middle|\; rx \in R \right\}$, note that $1 \notin I$. Thus I is a proper ideal, so let $\mathfrak{m} \in \operatorname{maxSpec} R$ with $\mathfrak{m} \supset I$. Then $(R\mathfrak{m} : R\mathfrak{m}x) = I_{\mathfrak{m}} =? \subset \mathfrak{m}R_{\mathfrak{m}}$ which is a proper ideal in $R\mathfrak{m}$. So 1 is not in the colon ideal.
■

These colon ideals aren't the obvious thing to look at, but come up in applications to algebraic geometry and number theory.

Remark For $I, J \trianglelefteq R$, we have $(I :_R J) = \left\{ x \in R \;\middle|\; xJ \subset I \right\}$. Thus this construction formalizes the idea of a "quotient I/J". This works for ideals in a domain, but also for *fractional ideals*.

Definition 21.2.1.
A *fractional R-ideal* is a nonzero R-submodule I of K such that there exists an $x \in R^{\bullet}$ such that $xI \subset R$.

Any ideal is a fractional ideal by taking $x = 1$. Note that some books define fractional ideals as finitely generated R-submodules, but this isn't a great definition.

Exercise (Easy) If $I \subset K$ is finitely generated, then I is a fractional ideal.

Idea: scale all generators.

Note that I is a fractional R-ideal iff $(R :_K I) = \left\{ x \in K \;\middle|\; xI \subset R \right\}$ is nonzero.

Next up: local-global theory for lattices.

Theorem 21.3.
Let R be a domain with fraction field K and V a finite dimensional K-vector space. Let $\Lambda \subset V$ be a finitely generated R-submodule. Then $\bigcap_{\mathfrak{m} \in \operatorname{maxSpec} R} \Lambda_{\mathfrak{m}} = \Lambda$.

Note that if $V = K$ and $\Lambda = R$, this recovers the previous theorem. Thus a global lattice over an integral domain can be recovered in terms of its localizations.

Next up: rounding out some theorems about projective and free modules.

Theorem 21.4 ***(Kaplanksy, Very Important!).***
A projective module over a local ring is free.

We proved this for finitely generated modules, which is the most important case. Note that projective modules are *locally free*, i.e. if M is a projective R-module then for all $\mathfrak{p} \in \operatorname{Spec} R$, $M_{\mathfrak{p}}$ is a free $R_{\mathfrak{p}}$-module.

We'll now define a notion of "the least number of generators" locally.

Definition 21.4.1 (Rank Function)**.**
Suppose M is a finitely generated R-module. For $\mathfrak{p} \in \operatorname{Spec} R$, denote $k(\mathfrak{p}) = ff(R/\mathfrak{p})$ the

residue field at $\mathfrak{p}$. We have $R \twoheadrightarrow R/\mathfrak{p} \hookrightarrow k(\mathfrak{p})$, so we define the rank function as

$$\begin{aligned} \operatorname{rank}_M : \operatorname{Spec} R &\longrightarrow \mathbb{N} \\ \mathfrak{p} &\mapsto \dim_{k(\mathfrak{p})} M \otimes_R k(\mathfrak{p}). \end{aligned}$$

where the RHS is base-changing to $k(\mathfrak{p})$ to get a finite dimensional vector space over $k(\mathfrak{p})$.

Exercise Show the following properties of the rank function for M, N finitely generated R-modules:

a. $\operatorname{rank}_{M\oplus N} = \operatorname{rank}_M + \operatorname{rank}_N$ and $\operatorname{rank}_{M\otimes_R N} = \operatorname{rank}_M \cdot \operatorname{rank}_N$.
b. Compute the rank function on $\mathbb{Z}/n\mathbb{Z}$ for $R = \mathbb{Z}$.
c. For R a PID, compute rank_M.

- Taking $\mathfrak{p} = p\mathbb{Z}$ in $\mathbb{Z}$ yields a delta function at p.
- If M is finitely generated and free, then

$$\operatorname{rank}_M(\mathfrak{p}) = \dim_{k(\mathfrak{p})} R^n \otimes_R k(\mathfrak{p}) = \dim_{k(\mathfrak{p})} \bigoplus_{i=1}^{n} R \otimes_R k(\mathfrak{p}) = \dim_{k(\mathfrak{p})} k(\mathfrak{p})^n = n.$$

- If M is locally free, then for all $\mathfrak{p} \in \operatorname{Spec} R$, we have $M_{\mathfrak{p}} \cong R_{\mathfrak{p}}^{\operatorname{rank}_M(\mathfrak{p})}$.

$$\begin{array}{ccc} R & \longrightarrow & R_{\mathfrak{p}} \\ & \searrow & \downarrow \\ & & k(\mathfrak{p}) \end{array}$$

  - Thus the rank can be thought of as the fiberwise dimension for bundles.
- If M is *stably free*, i.e. there exists an $m, n \in \mathbb{N}$ such that $M \oplus R^m \cong R^n$, then $\operatorname{rank}_M = n - m$.

Note that projective implies locally free. In order for a finitely generated projective module to be free, it must have constant rank function. The geometric analog here would be that the fibers having constant dimension is necessary for a bundle to be trivial.

Proposition 21.5 ***(Determining if a Projective is Free).***
Suppose M is finitely generated projective of constant rank n. Then M is free iff M can be generated by n elements.

22 Wednesday April 1st

Let M be a finitely generated R-module, then we define a rank function

$$\begin{aligned} \operatorname{rank}_M : \operatorname{Spec} R &\longrightarrow \mathbb{N} \\ \mathfrak{p} &\mapsto \dim_{k(\mathfrak{p})} M \otimes_R k(\mathfrak{p}) \end{aligned}$$

where $k(\mathfrak{p}) = ff(R/\mathfrak{p})$.

Question: If $\mathfrak{p}_1 \subset \mathfrak{p}_2$, how do the ranks compare?

Example: Take $R = \mathbb{Z}$ and $M = \mathbb{Z}\oplus\mathbb{Z}/(10)$, then take $(0) \subseteq (p)$. Then $\operatorname{rank}_M((0)) = \dim_{\mathbb{Q}} M \otimes_{\mathbb{Z}} \mathbb{Q} =$

1. However,

$$\operatorname{rank}_M((p)) = \begin{cases} 2 & p = 2, 5 \\ 1 & \text{else} \end{cases}.$$

If M is locally free, e.g. projective, and $\mathfrak{p}_1 \subseteq \mathfrak{p}_2$ then $M_{\mathfrak{p}_1} = M_{\mathfrak{p}_2} \otimes_{R_{\mathfrak{p}_2}} R_{\mathfrak{p}_1}$ is a canonical isomorphism. Then

$$R_{\mathfrak{p}_1}^{\operatorname{rank}\mathfrak{p}_1} = M_{\mathfrak{p}_1} = M_{\mathfrak{p}_2} \otimes_{R_{\mathfrak{p}_2}} = R_{\mathfrak{p}_2}^{\operatorname{rank}\mathfrak{p}_2} \otimes R_{\mathfrak{p}_1} \cong R_{\mathfrak{p}_1}^{\operatorname{rank}\mathfrak{p}_2}.$$

Thus $\operatorname{rank}(\mathfrak{p}_1) = \operatorname{rank}(\mathfrak{p}_2)$. In other words, tensor to the fraction field and take the dimension.

Proposition 22.1.
If M is finitely generated projective of constant rank n then M is free $\iff$ M can be generated by n elements.

Lemma 22.2.
If M is finitely generated projective and $I \in \mathcal{J}(R)$, then M/IM free implies M is free.

Nakayama: "finite generators in quotient" lifts to finite generators in total module.

Proof .
$M/IM \cong (R/I)^n$ since it's finitely generated and free, so this fits the hypothesis of Nakayama's lemma. So the last number of generators for M is n. Then for any $\mathfrak{m} \in \operatorname{maxSpec} R$, then after base change we get a diagram

$$\begin{array}{ccc} \mathfrak{m} & \longrightarrow & M/IM \\ & \searrow & \downarrow{\scriptstyle \twoheadrightarrow} \\ & & M/\mathfrak{m}M \end{array}$$

Since $M/\mathfrak{m}M$ is free of finite rank n, ???????.

■

Corollary 22.3.
If R is *semilocal* and M is a finitely generated projective module, then M is free $\iff$ rank_M is constant.

Proof .
$\implies$: We know free modules have constant rank function.
$\impliedby$: $\operatorname{maxSpec} R = \{\mathfrak{m}_1, \cdots, \mathfrak{m}_n\}$, and $\mathcal{J}(R) = \bigcap_{i=1}^{n} \mathfrak{m}_i = \prod_{i=1}^{n} \mathfrak{m}_i$. Thus $R/\mathcal{F}(R) = \prod_{i=1}^{n} R/\mathfrak{m}_i$, and $M/\mathcal{J}(R)M \cong \prod_{i=1}^{n} M/\mathfrak{m}_i M$. So we just need to show that the dimension is independent of i. But this follows from the rank function being constant, since the rank equals the dimension for each factor.

■

Proposition 22.4 ***(Flatness is Local).***
For M an R-module, then M is flat $\iff$ $M_{\mathfrak{p}}$ is flat for all $\mathfrak{p} \in \operatorname{Spec} R$ $\iff$ $M_{\mathfrak{m}}$ is flat for all $\mathfrak{m} \in \operatorname{maxSpec} R$.

Noetherian: f.g. projective iff locally free.

Theorem 22.5 ***(7.2, Extremely Important Result).***
For an R-module M, TFAE

- M is finitely generated and projective
- M is finitely presented and locally free
- There exist $f_1, \cdots, f_n \in R$ such that $\langle f_1, \cdots, f_n \rangle = R$ and for all $1 \leq i \leq n$, M_{f_i} is a free R_{f_i}-module.

Here M_{f_i} means localize at the powers of f_i, i.e. $M \otimes R_{f_i}$.

Corollary 22.6.

- Finitely generated and flat implies projective.
- For M finitely generated and R Noetherian, projective $\iff$ locally free $\iff$ flat (important!)

A module M is Z-locally free (Zariski) iff there exists elements $f_i \in R$ such that $\langle f_i \rangle = R$ and M_{f_i} is free for all i. Note that Z-locally free implies locally free.

Example: $R = \prod_{i=1}^{\infty} \mathbb{F}_2$ and let $I \trianglelefteq R$ not be finitely generated. Note that R is not Noetherian since it's an infinite product of nonzero rings – just identify as functions $\mathbb{F}_2^{\mathbb{Z}}$ and take the maximal ideal where the first coordinate is zero (?). Then R/I is an R-module is finitely generated and flat (even though R isn't a domain) but not projective, locally free but not Z-locally free. Thus the conditions in the hypotheses of the corollary are necessary, particularly being Noetherian.

22.1 Chapter 8: Noetherian Rings

For $(X, \leq)$ a poset, then X is *Noetherian* iff it satisfies the ACC, i.e. there does not exist an order-embedding $\mathbb{Z}^+ \hookrightarrow X$, and X is *Artinian* iff it satisfies the DCC, i.e. there's no embedding $\mathbb{Z}^- \hookrightarrow X$.

Note that X is Noetherian iff $X^\vee$ is Artinian, where $X^\vee$ is given by $x \leq^\vee y \iff y \leq x$. We'll generally be interested in the poset of submodules of a given module and set inclusion.

Recall that M is Noetherian $\iff$ every submodule is finitely generated, which is easy to show.

Exercise Show that for $\mathbb{Z}$-modules, Noetherian and Artinian are two different conditions by exhibiting the 4 possibilities.

Theorem 22.7.
R is Artinian iff R is Noetherian and $\dim R = 0$, i.e. prime ideals are maximal, $\operatorname{maxSpec} R = \operatorname{Spec} R$.

So Artinian is much much stronger than Noetherian.

23 Friday April 3rd

Recall that the definition of a normal series for G a group.

Theorem 23.1 ***(Jordan Holder).***
Any two composition series for the same group G are equivalent (same isomorphism classes of quotients and multiplicities).

There is an analog of this for modules, even over a noncommutative ring: this is just a sequence of submodules inclusions, since normality is automatic. There is similarly a notion of Schreir refinement. For p groups, the composition factors have to be cyclic of order p. On one hand, we could fix the series and ask for what modules have a compatible composition series – this is the extension problem, and is difficult in general. Here we will fix the module and see what the possible composition series are.

Question: When does an R- module admit a finite composition series?

Answer: When R is both Noetherian and Artinian.

Suppose that M satisfies the ACC and DCC. Then there exists a minimal simple module $M_1 < M$, an M_2 properly containing M_1 such that M_2/M_1 is simple, and so on. This sequence of inclusions terminates due to the ACC, so this yields a finite composition series.

Definition 23.1.1 (Length)**.**
?

Proposition 23.2 ***(Length is Additive over SESs).***
For $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$, M has finite length iff M', M'' do, and $\ell(M) = \ell(M') + \ell(M'')$.

Dream of commutative algebra: every theorem at the level of generality of "Let M be a module over a Noetherian ring".

Proposition 23.3.
Quotients and localizations of Noetherian rings are Noetherian.

Proposition 23.4.
For $I \trianglelefteq R$, $\mathcal{I}(R/I) \hookrightarrow \mathcal{I}(R)$ is an isotone inclusion of posets.

Thus Noetherian-Artinian properties in the RHS imply the same properties in the LHS. For localizations, we also have $\mathcal{I}(S^{-1}R) \hookrightarrow \mathcal{I}(R)$ by push-pull properties.

Proposition 23.5.
If R is an Artinian domain, then R is a field.

Proof .
For the contrapositive, let $a \in R^\bullet \setminus R^\times$, then $(a) \supsetneq (a^2) \supsetneq \cdots$ is an infinite descending chain. ■

Theorem 23.6.
For R Artinian,
a. $\dim_{\text{Krull}} R = 0$.
b. $\mathcal{J}(R) = \text{nil}(R)$.
c. $\text{maxSpec } R = \{\mathfrak{m}_i\}_{i=1}^n$ is finite.
d. $\text{nil}(R)$ is a nilpotent ideal.

Proof .

a. If $\mathfrak{p} \in \text{Spec } k$, $R/\mathfrak{p}$ is an Artinian domain and thus a field, so $\mathfrak{p}$ is maximal.
b. Produce a descending chain $\mathfrak{m}_1 \supset \mathfrak{m}_1\mathfrak{m}_2 \supset \cdots$ and suppose that $\prod^n \mathfrak{m}_i = \prod^{n+1} \mathfrak{I}$, then $\prod^n \mathfrak{m}_i \subset \mathfrak{m}_{n+1}$ and thus $\mathfrak{m}_{n+1} \supset \mathfrak{m}_i$ for some i, which is a contradiction.
c. ?
d. ?

■

Theorem 23.7 ***(Akizuki-Hopkins).***
R is Artinian $\iff$ R is Noetherian and $\dim R = 0$.

24 Monday April 6th

Last time: a characterization of Artinian rings, the Akizuki-Hopkins theorem

Theorem 24.1 ***(Akizuki-Hopkins).***
R is Artinian iff R is Noetherian with Krull dimension 1, i.e. all primes are maximal.

Proposition 24.2.
Suppose $(R, \mathfrak{m})$ is Noetherian and local. Then either
1. $\mathfrak{m}^n \gneq \mathfrak{m}^{n+1}$ for all n, or
2. $\mathfrak{m}^n = (0)$ for some n.

Moreover, (2) holds iff R is Artinian.

Proof .
If $\mathfrak{m}^n = \mathfrak{m}^{n+1}$ for some n, then by Nakayama $\mathfrak{m}^n = (0)$.
If R is Artinian, then (1) can not hold, so (2) must hold. Conversely, if (2) holds, then $\mathfrak{m} \in \text{nil} R = \bigcap_{\text{Spec } R} \mathfrak{p}$, but this can only happen if $\text{Spec } R = \{\mathfrak{m}\}$ is precisely one ideal. But then every prime ideal is maximal.

■

Note that Artinian rings have finitely many maximal ideals.

Theorem 24.3 ***(Primary Decomposition).***

Let R be a nonzero Artinian ring and suppose maxSpec $R = \{\mathfrak{m}_i\}^n$. Then $R = \prod_{i=1}^n \mathfrak{r}_i$ where $\mathfrak{r}_i \coloneqq R_{\mathfrak{m}_i}$.

Note that for $R = \mathbb{Z}$ and $N = \prod_{i=1}^n p_i^{a_i}$, this recovers $Z/N\mathbb{Z} = \prod_{i=1}^n \mathbb{Z}/p_i^{a_i}\mathbb{Z}$.

Punchline: Artinian rings split as a product of local rings. Modules over local rings are free, and thus simple, so this gives a local-to-global principle. Moreover, every localization is a projection onto one of the factors.

Exercise For R Artinian, show that every $x \in R$ is either a unit or a zero divisor. Thus R is its own total fraction ring.

Exercise For a ring R, TFAE

1. R is semilocal (finitely many maximal ideals).
2. $R/\mathcal{J}(R)$ is Artinian.
3. $R/\mathcal{J}(R)$ has finitely many ideals.

Most important theorem in the course: Hilbert's basis theorem!

Theorem 24.4 ***(Hilbert's Basis).***

If R is Noetherian, then $R[t]$ is Noetherian.

Proof .

Toward a contradiction, let $J \trianglelefteq R[t]$ that is not finitely generated. Construct a sequence $\{f_n\}$ and take $J_n \coloneqq \langle f_1, \cdots, f_n\rangle \subseteq J$. This can be done by taking $f_0 = 0$ and f_{n+1} any element of J/J_n of minimal degree. Note that this ensures that $\deg f_n \leq \deg f_{n-1}$.

Set a_n to be the leading coefficient of f_n, and let $I = \langle\{a_i\}\rangle$. Since R is Noetherian, I is finitely generated, so there is some $N \in \mathbb{Z}$ such that $I = \langle a_1, \cdots, a_N\rangle$.

Thus $a_{n+1} = \sum_{i=1}^N u_i a_i$ for some $u_i \in R$. So set $g \coloneqq \sum_{i=1}^N u_i f_i t^{\deg f_{N+1} - \deg f_i}$. Then $g \in J_N$ and $f_N \in J/J_n$ and $f_{N+1} - g \in J \setminus J_N$.

Now the leading term of g is $\sum u_i a_i = a_{N+1}$, and since $\deg g = \deg f_{N+1}$ where a_{N+1} is also the leading term of f_{N+1}. Thus $\deg(f_{N+1} - g) < \deg f_{N+1}$, contradicting minimality.

■

Theorem 24.5.

R Noetherian implies that $R[[t]]$ is Noetherian.

Exercise If R is a ring with $R[t], R[[t]]$ both Noetherian, then R is Noetherian.

Idea: use the fact that quotients of Noetherian rings are again Noetherian.

Corollary 24.6 ***(Single Most Important Result!).***
If R is Noetherian then every finitely generated R-algebra is Noetherian.

If such an algebra is finitely generated by n generators, it's a quotient of $R[x_1, \cdots, x_n]$.

Some historical notes on the Hilbert Basis Theorem: Given G a group and T a ring, we can consider actions $G \longrightarrow \text{Aut}(R)$ and the ring of invariants $T^G = \left\{ t \in T \;\middle|\; gt = t \;\forall g \in G \right\} \subset T$. Note that Galois theory fits into this framework. For a classical example, consider $T = \mathbb{C}[t_1, \cdots, t_n]$. Then $G \subset \text{GL}(n, \mathbb{C}) \curvearrowright T$ by linear automorphisms, i.e. it acts on each t_i by taking it to some linear combination of t_j. Note that G can be chosen to be "nice", i.e. a linear algebraic group.

Question: is T^G finitely generated as a $\mathbb{C}$-algebra? Hilbert proved that this is true when G is a linear algebraic group, and the main step was the basis theorem. Previously, people were proving these kinds of theorems for a single group at a time, whereas this encompassed all of them simultaneously!

> Quote by Gordon: "This is not Mathematics, this is theology."

This is an early triumph of abstraction in algebra, as opposed to writing out lines upon lines of equations for single proofs. How effective is this proof? This doesn't necessarily lead to a good algorithm for finding a finite generating set, see computational commutative algebra.

Exercise For k a field, $k[x, y]$ is Noetherian. Show that $k[y, xy, x^2y, \cdots]$ is not Noetherian.

Note that things work out very nicely for Noetherian rings of dimension 0 and 1, but many theorems fail in higher dimensions.

Exercise (Possibly difficult to prove) Show that every k-subalgebra of $k[x]$ is Noetherian.

25 Wednesday April 8th

Theorem 25.1 ***(Krull Intersection, 8.39).***
For R Noetherian and $I \trianglelefteq R$ a proper ideal,

a. If there exists an $x \in \bigcap_{i=1}^{\infty} I^n$, then $x \in xI$.
b. Suppose either R is a domain or $I \subset \mathcal{J}(R)$, then $\bigcap I^n = (0)$.

Proof .

a. Omitted.
b. If $x \in \bigcap I^n$, then (a) implies that there exists an $a \in I$ such that $x = xa$. Then $x(1-a) = 0$. Since R is a domain and $a \neq 0$, then $1 - a$ is not a zero divisor.

■

Exercise Exhibit a proper ideal $I \trianglelefteq R$ Noetherian such that $\bigcap_n I^n \neq (0)$.

> Note: there is a very small ring that will work.

Exercise (Recommended, Difficult Calculus) Consider $R = \{f : \mathbb{R} \longrightarrow \mathbb{R}, f \in C^\infty\} \subset \mathbb{R}^{\mathbb{R}}$ and $\mathfrak{m} \coloneqq \left\{ f \in R \;\middle|\; f(0) = 0 \right\}$.

1. Show $\mathfrak{m} \trianglelefteq R$ and $R/\mathfrak{m} = \mathbb{R}$ and thus $\mathfrak{m}$ is maximal.
2. Show $\mathfrak{m} = (x)$.
3. Show that for all $n \in \mathbb{Z}$, we have $\mathfrak{m}^n = (x^n) = \left\{ f \;\middle|\; f(0) = f'(0) = \cdots - f^{n+1} = 0 \right\}$.
4. Show that $\bigcap \mathfrak{m}^n = \left\{ f \;\middle|\; T_0(f) \equiv 0 \right\} \neq (0)$
5. Show that $f \notin f\mathfrak{m}$ (so $f \neq xg$ for some other smooth g) therefore R is not Noetherian.

Start with a smooth function vanishing at zero, divide by x, define value at zero to make it continuous. Example: $f(x) = e^{-1/x^2}$ for $x \neq 0$ and $f(0) = 0$.

Theorem 25.2 ***(Principal Ideal Theorem / Krull's Hauptfdealsatz).***
For R Noetherian, $x \in R \setminus R^\times$, $\mathfrak{p} \in \operatorname{Spec}(R)$ *minimal over* (x) (to be explained). Then $\operatorname{ht}(\mathfrak{p}) \leq p$, where we recall that that height is given by the number of ideals below it.

Corollary 25.3.
Every nonzero ring has a minimal prime.

In particular if $\mathfrak{p} = (x)$ is a prime ideal in a Noetherian ring, $\operatorname{ht}(\mathfrak{p}) \leq 1$.

Corollary 25.4.
Under these conditions, if x is not a zero divisor then $\operatorname{ht}(\mathfrak{p}) = 1$.

Proof .
We can reduce R to $R_{\mathfrak{p}}$ (using how ideals are pushed into localizations). Then $R_{\mathfrak{p}}$ is a Noetherian local ring of krull dimension 0, hence is Artinian by Akazuki. By a previous theorem, $\mathfrak{p}R_{\mathfrak{p}}$ is thus nilpotent.

So there exists an n such that $x^n = 0$ in $R_{\mathfrak{p}}$ which is thus in the kernel of the localization map, and there exists an $a \in R/\mathfrak{p}$ such that $ax^n = 0$ in R. Since x is not a zero divisor, so multiplication by x (and all compositions) is injective, x^n is not a zero divisor and thus $a = 0$. But since $a \in R/\mathfrak{p}$, so $a \neq 0$, a contradiction.

■

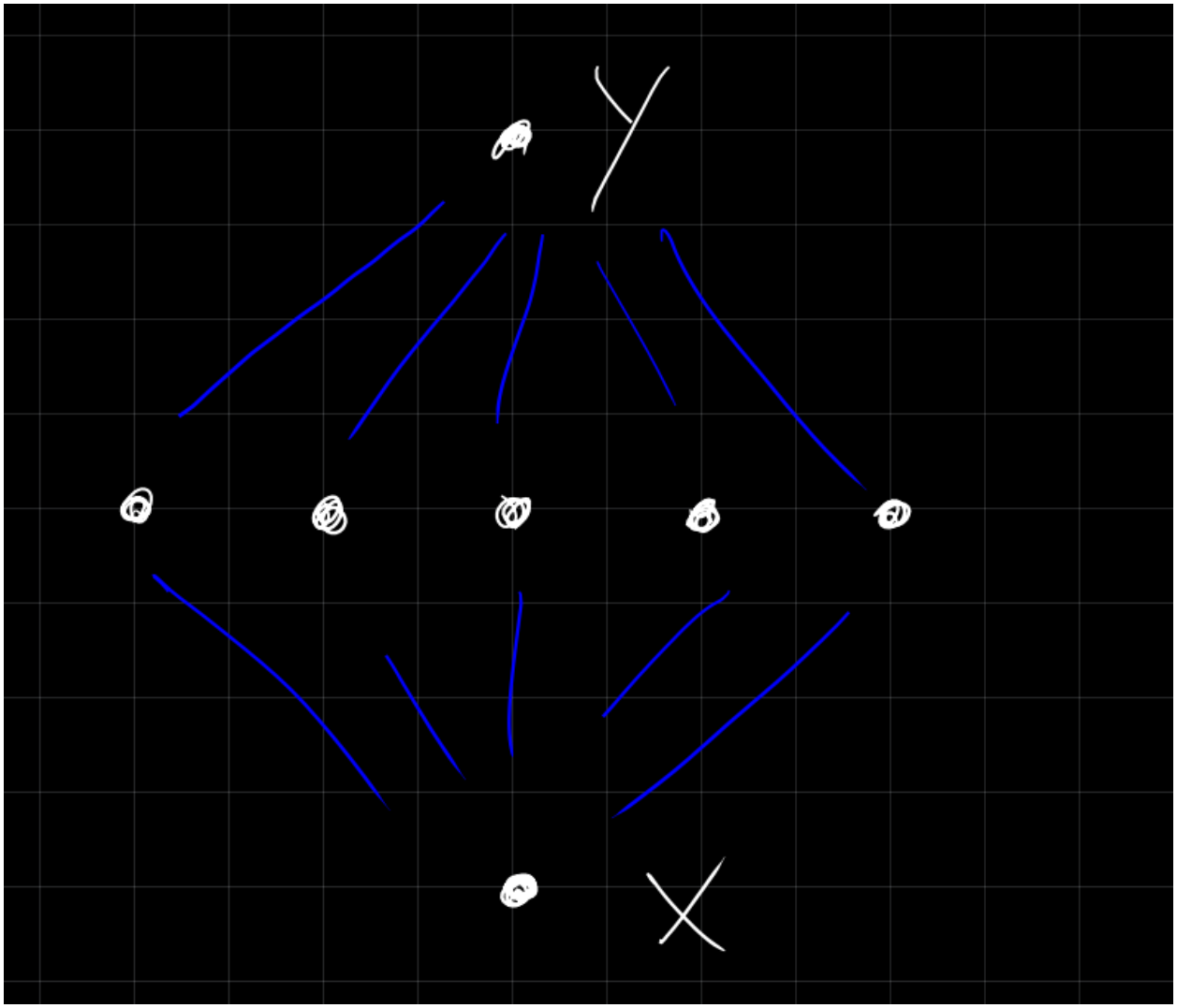
Thus the number of generators of a prime ideal in a Noetherian ring is bounded below by its height.

Lemma 25.5 ***(Page 44).***
For $\mathfrak{p}, \{\mathfrak{q}_i\} \in \operatorname{Spec}(R)$, if $\mathfrak{p} \subset \bigcup_i \mathfrak{q}_i$ then $\mathfrak{p} \subset \mathfrak{q}_i$ for some i.

Proof omitted.

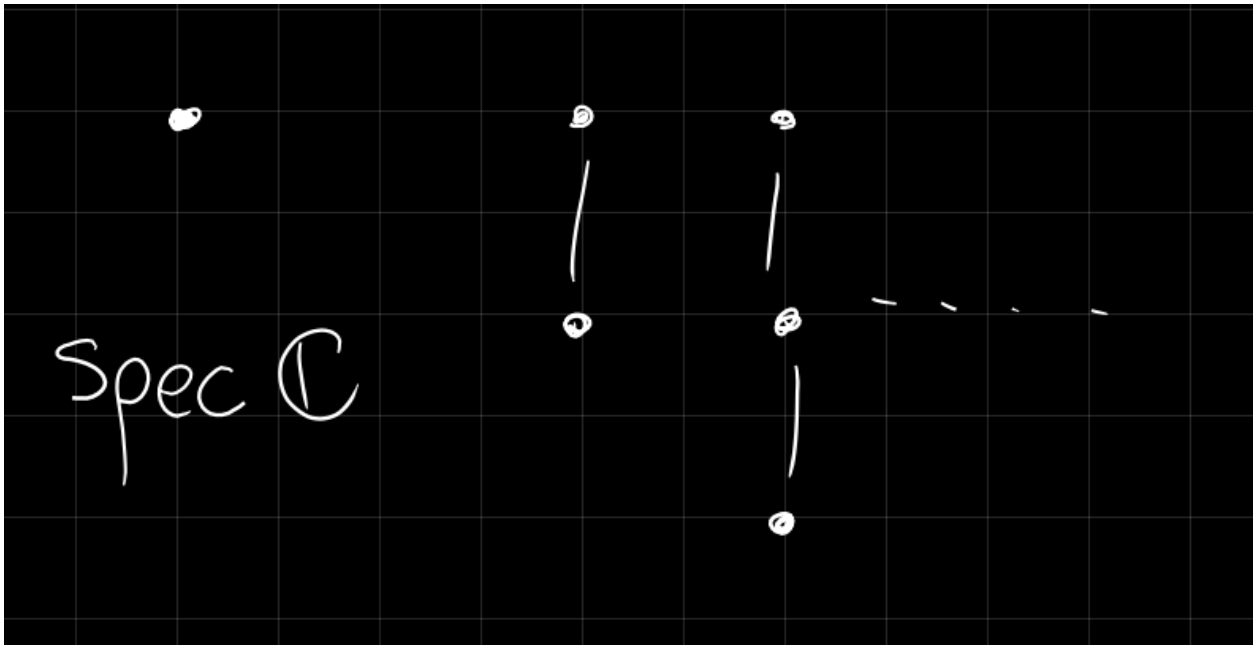
Exercise In $R = \mathbb{C}[x, y], \mathfrak{m} \coloneqq \langle x, y \rangle$, show that $\operatorname{ht}(\mathfrak{m}) \geq 2$ and $\mathfrak{m}$ is the union of all of the principal ideals it contains. Thus the finiteness in the previous lemma is necessary.

For $(X, \leq)$ a poset and $x \leq y$, we define the interval $(x, y) \coloneqq \left\{ z \in X \;\middle|\; x \leq z \leq y \right\}$:



Corollary 25.6.
For $\mathfrak{p} \subset \mathfrak{q}$ a proper containment in a Noetherian ring, $(\mathfrak{p}, \mathfrak{q})$ is either empty or injective.

Note that this implies that for possible line order of length n, there is a ring with Spec (R) having that structure.



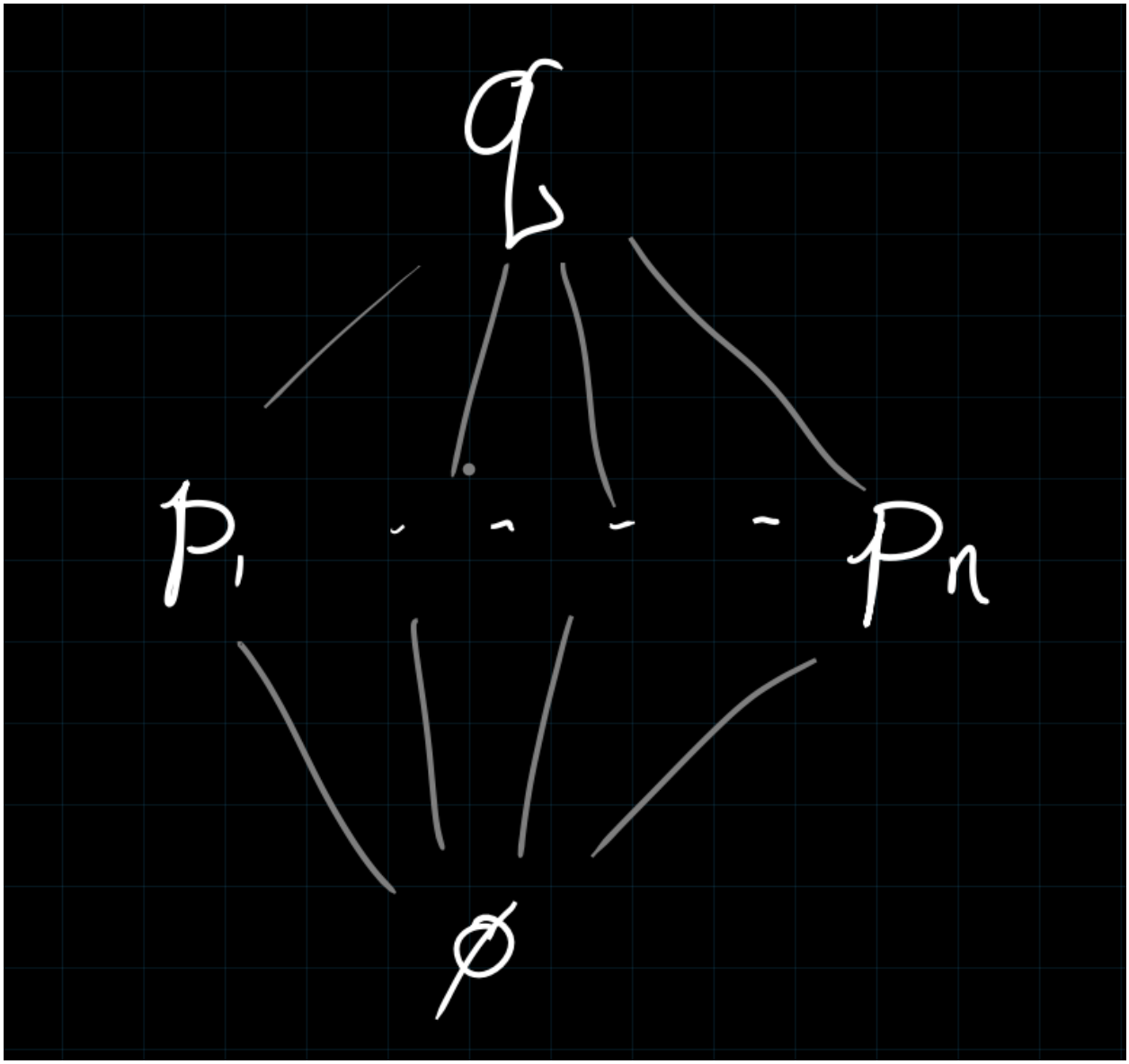
26 Friday April 10th

Last time: prime avoidance, for $\mathfrak{p}, \{\mathfrak{q}_i\} \in \operatorname{Spec} R$, if $\mathfrak{p} \subset \bigcup \mathfrak{q}_i$, then $\mathfrak{p} \subset \mathfrak{q}_i$ for some $\mathfrak{q}_i$.

Theorem 26.1.
For R Noetherian and $\mathfrak{p} \subsetneq \mathfrak{q} \in \operatorname{Spec} R$, then $(\mathfrak{p}, \mathfrak{q}) \coloneqq \{\mathfrak{n} \in \operatorname{Spec} R \text{ s.t. } \mathfrak{p} \subsetneq \mathfrak{n} \subsetneq \mathfrak{q}\}$ is either empty or infinite.

Proof .
Wlog by passing from R to $R/\mathfrak{p}$, assume $\mathfrak{p} = (0)$, and toward a contradiction assume that the theorem doesn't hold. Then $(\emptyset, \mathfrak{q}) = \{\mathfrak{p}_i\}$, and by prime avoidance, there exists an $x \in \mathfrak{q} \setminus \bigcup \mathfrak{p}_i$ and thus $\mathfrak{q}$ is a minimal prime over x. By Hauptfidealsatz, $\operatorname{ht}(\mathfrak{q}) \leq 1$, but this is a contradiction because $\operatorname{ht}(\mathfrak{q}) \geq 2$.

■



Proposition 26.2 ***(Generalized Hauptfidealsatz).***
For R Noetherian, $I = \langle x_1, \cdots, x_n \rangle \trianglelefteq R$, if $\mathfrak{p} \in \operatorname{Spec} R$ is minimal over I, then $\operatorname{ht}(\mathfrak{p}) \leq n$.

Corollary 26.3.
If $\mathfrak{p} \in \operatorname{Spec}(R)$ for R Noetherian, then R needs at least $\operatorname{ht}(\mathfrak{p})$ generators.

Complete intersection: minimal number of defining equations.

Last item on Noetherian rings, used to prove Nullstellensatz:

Lemma 26.4 ***(Artin-Tate Lemma).***
If R is Noetherian and $R \subset T \subset S$ with S finitely generated as a T-module and finitely-generated as an R-algebra, then T is finitely generated as an R-algebra.

26.1 Boolean Rings

Definition 26.4.1.
A ring R is *Boolean* if every element is idempotent, i.e. $x^2 = x$ for all $x \in R$.

Exercise If R is Boolean, then

1. $R = R^\times$,
2. Every quotient is Boolean,
3. Every subring is Boolean,
4. (More interesting) every ideal is radical.

Exercise Suppose R is Boolean.

1. If R is a domain then $R \cong \mathbb{Z}/2\mathbb{Z}$.
2. $\dim R = 0$

Exercise If R is Boolean and local, then $R \cong \mathbb{Z}/2\mathbb{Z}$.

Proposition 26.5.
For R Boolean, TFAE:

1. R is finite.
2. R is Noetherian.
3. Spec R is finite.

In any of these cases, $(\mathbb{Z}/2\mathbb{Z})^n$.

Proof .

- $1 \implies 2$ is clear because any finite ring is Noetherian.
- $2 \implies 3$: using Akazuki-Kopkins, R is Artinian and thus Spec $R = \text{maxSpec } R$ is finite.
- $3 \implies 1$: By a previous exercise, since maxSpec R is finite, $R/\mathcal{J}(R)$ is a finite product of fields (by CRT essentially). Then $\mathcal{J}(R) = \text{nil}(R) = \{0\}$ therefore R is a finite product of fields, forcing $R \cong \prod \mathbb{Z}/2\mathbb{Z}$.

■

26.2 Stone Duality

This leads to Stone duality, an early example of categorical equivalence. Let R be a Boolean ring, Spec $R \subset$ maxSpec R equipped with the Zariski topology generated by the basis $\{U(f) \text{ s.t. } \mathfrak{m} \in \text{Spec } R,\ f \notin \mathfrak{m}\}_f$ Then $V(f) \coloneqq \text{Spec } R \setminus U(f) = \{\mathfrak{m} \in \text{Spec } R \text{ s.t. } f \in \mathfrak{m}\}$. For any R, $V(f)$ is closed and $V(f) \subseteq U(1-f)$.

But R is boolean iff $f(1-f) = 0$, and if $1 - f \notin \mathfrak{m}$, then $f \in \mathfrak{m}$ and thus $V(f)$ is open. So Spec R has a base of clopen sets, which is referred to as a *zero-dimensional* space. Moreover Spec R is also Hausdorff, and we'll later see that Spec R is Hausdorff iff $\dim R = 0$.

Exercise For any R, Spec R is quasicompact (where compact is quasicompact and Hausdorff).

Spec R is zero-dimensional and compact. Fact:

- A zero-dimensional Hausdorff space is totally disconnected,

- A totally disconnected locally compact space is ?

X is a Boolean space if it is ? and compact, iff compact and totally disconnected.

There is a notion of *Stone space*, equivalently a profinite space is an inverse limit of finite discrete spaces, which happens iff compact and totally disconnected.

To any Boolean topological space X we attached its *characteristic ring* $C(X)$. The elements are clopen subsets of X with $U + V \coloneqq U \Delta V = U \setminus V \bigcup V \setminus U$ and $U \cdot V \coloneqq U \bigcap V$. Note that any algebra of sets can be made into a ring in this way, and we note that $U \cdot U = U \bigcap U = U$, so $C(X)$ is a Boolean ring.

26.2.1 Statement of Stone Duality

For notation, set $M(R) \coloneqq \operatorname{Spec} R$, and define functors

$$\left\{Boolean rings\right\} \leftrightarrows_{C}^{M} \left\{Boolean spaces\right\}.$$

This gives a mutually inverse pair of functors which are naturally isomorphic to the identity, i.e. there is a canonical isomorphisms $C(M(R)) \cong R$ and $M(C(X)) \cong X$.

Exercise There exists a ring R and $x, y \in R$ such that $(x) = (y)$ but there exists a $u \in R^{\times}$ such that $x = uy$

27 Monday April 13th

27.1 Nullstellansatz

Let k be a ring (later a field) and $R_n \coloneqq k[t_1, \cdots, t_n]$. If $x \in k^n$ and $f \in R_n$, we can evaluate f at x since $f(x) \in k$, and we thus get an evaluation map

$$\begin{aligned} E : R_n &\longrightarrow k^{k^n} \\ f &\mapsto (x \mapsto f(x)) \end{aligned}$$

which is a ring homomorphism, where the RHS is regarded as a large direct product of rings.

When can we identify polynomials (abstract elements of a ring) with the corresponding polynomial *function*?

Exercise Suppose k is a domain.

a. If k is infinite, then E is injective but not surjective.
b. If k is finite, the E is surjective but not injective.

Definition 27.0.1 (Incidence Relation)**.**
Put a relation on $R \times k^n$ where $f \sim x \iff f(x) = 0_R$.

We'll define an antitone Galois connection

$$\mathcal{I}(R) \leftrightarrows_{I}^{V} 2^{k^n}$$

where the RHS is the powerset. We define V which takes an ideal and yields a subset of k^n,

$$V(J) = \left\{ x \in k^n \;\middle|\; \forall f \in J,\ f(x) = 0 \right\}$$
$$I(S) = \left\{ f \in R \;\middle|\; \forall x \in S,\ f(x) = 0 \right\}.$$

That this forms an ideal is immediate.

The pair (I, V) are antitone (order-reversing) and fits into the (extremely general formal) framework of Galois connections. This can be seen by writing $V(J) = \bigcap_{f \in J} V(f)$ and $I(S) = \bigcap_{x \in S} I(\{x\})$. Therefore (by the formalism) there are associated closure operators:

1. $2^{k^n} \circlearrowleft, S \mapsto \overline{S} \coloneqq V(I(S))$
2. $\mathcal{I}(R) \circlearrowleft, J \mapsto \overline{J} \coloneqq I(V(J))$.

These are both *isotone* maps (order-preserving) and are closure operators on posets, i.e. they satisfy

- $(X, \leq) \mapsto (X, \leq), x \leq y \implies C(x) \leq C(y)$ (isotonicity)
- $x \leq C(x)$
- $C(C(x)) = C()$ (idempotence)

By construction, $\overline{S} = \left\{ x \in k^n \;\middle|\; f(s) = 0 \implies f(x) = 0 \right\}$ and $\overline{J} = \left\{ f \in k^n \;\middle|\; g(x) = 0 \forall g \in S \implies f(x) = 0 \right\}$.

Example: Take k a field, $S \subset k$. Then

$$\overline{S} = \begin{cases} S & S \text{ is finite} \\ k & \text{else} \end{cases}.$$

Exercise For k a field, show that for all $S_1, S_2 \subset k$, we have $\overline{S_1 \bigcup S_2} = \overline{S}_1 \bigcup \overline{S}_2$.

This mirrors what closures in a topological space would do, so $S \longrightarrow \overline{S}$ is in fact a *Kuratowski* closure operator and therefore is the closure operator for a unique topology (here, the Zariski topology, where the closed subsets are given by $V(I)$). For $n = 1$, the Zariski topology on k is the cofinite topology. If k is finite, this is discrete, and is very coarse and non-Hausdorff when k is infinite since any two open sets intersect.

These maps satisfy a *tridempotence* relation, i.e. $VIV = V$ and $IVI = I$, and are antitone *bijections* when restricted to closed sets.

Exercise The closure operator on ideals never satisfies the Kuratowski property.

So we don't have a topology on the ring/ideal side, since even unions of ideals may fail to be ideals. We take the description sending $S \longrightarrow \overline{S}$ to be fairly explicit, but what is the corresponding description for $J \longrightarrow \overline{J}$?

For all $S \in k^n$, $I(S) \trianglelefteq k[t_1, \cdots, t_n]$, we use the fact that $f^n(x) = 0 \implies f(x) = 0$ and thus $I(S) = \mathrm{rad} I(S) = \bigcap_{\mathfrak{p} \supset I(S)} \mathfrak{p}$, and $V(J) = V(\mathrm{rad} J)$. Moreover, for all $J \trianglelefteq R$, we have $\mathrm{rad} J \subset \overline{J}$.

Passing from an ideal to its radical is a closure operator, so does $\overline{J} = \mathrm{rad} J$ for all $J \trianglelefteq R$? Not for all k, e.g. take $k = \mathbb{R}, n = 1, J = \left\langle t^2 + 1 \right\rangle$. Then $V(J) = \emptyset$, but $\overline{J} = I(\emptyset) = \mathbb{R}[t]$ vacuously. Note that $\mathbb{R}/J \cong \mathbb{C}$, so J is maximal and hence radical, so $\overline{J} \supsetneq \mathrm{rad} J = J$.

What went wrong? Potentially $\bar{k} \neq k$.

Exercise Let k be a field, fix $n \in \mathbb{Z}^+$, and show that if all $\mathfrak{m} \in \text{maxSpec } (R)$ satisfy $\overline{\mathfrak{m}} = \text{rad}\mathfrak{m}$, then L is algebraically closed.

Exercise Suppose $k = \bar{k}$ is algebraically closed and $n = 1$, show that for all $J \trianglelefteq k(t)$, we have $\overline{J} = \text{rad}J$.

Theorem 27.1 ***(Hilbert's Nullstellansatz).***
If $k = \bar{k}$ and for all $n \in \mathbb{Z}^+$ and $J \trianglelefteq R = k[t_1, \cdots, t_n]$, $\overline{J} = I(V(J)) = \text{rad}J$ Therefore I, V induces a galois correspondence

$$\left\{\begin{matrix}\text{Radical ideals} \\ \text{of } k[t_1, \cdots, t_n]\end{matrix}\right\} \iff \left\{\begin{matrix}\text{Zariski closed subets} \\ \text{of } k^n\end{matrix}\right\}.$$

Exercise If $k = \bar{k}$, show that the above theorem implies the *weak Nullstellansatz*, i.e. the map $I : k^n \xrightarrow{\cong} \text{maxSpec } k[t_1, \cdots, t_n]$ where $\mathbf{x} \mapsto \mathfrak{m}_x = I(\{\mathbf{x}\}) = \langle t_1 - x_1, \cdots, t_n - x_n \rangle$ is a bijection.

Try without using the formalism of Galois connections.

Proof sketch: we'll spend most of our time proving the weak Nullstellansatz, and use a trick to bootstrap up to the full theorem. The closure operator is only the radical for algebraically closed – what is the closure operator for other fields.

28 Wednesday April 15th

Recall that we had mutually inverse maps V, I and for $J \trianglelefteq R$, we had a closure $\overline{J} = I(V(J))$ and $\overline{S} = V(I(S))$.

Hilbert's Nullstellensatz says that if $k = \bar{k}$, then for all J, we have $\overline{J} = \text{rad}J$ and there is a Galois correspondence between radical ideals of $k[x_1, \cdots, x_n]$ and Zariski closed subset of $\mathbb{A}^n_k$. The weak Nullstellensatz gives a correspondence between maximal ideals and points of k^n.

For $S = \overline{S} = k^n$, we have $S = \bigcup_{x \in S} \{x\}$ and by the Galois correspondence, we find that if J is radical then $J = \bigcap \mathfrak{m} \supset J\mathfrak{m}$.

Definition 28.0.1.
A ring R is *Jacobson* if every radical ideal is the intersection of the maximal ideals containing it, i.e. for all $I \trianglelefteq R$ we have $\text{rad}I = \bigcap_{\mathfrak{m} \supset I} \mathfrak{m}$

Exercise For $x \in k^n$, define $\mathfrak{m}_x \coloneqq I(\{x\}) = \left\{ f \in R \;\middle|\; f(x) = 0 \right\}$.

1. Show that $\mathfrak{m} = \langle t_1 - x_1, \cdots, t_n - x_n \rangle$ and $R/\mathfrak{m}_x = k$.
2. Show that the following map is injective:

$$\begin{aligned} I : k^n &\longrightarrow \text{maxSpec } R \\ x &\mapsto \mathfrak{m}_x. \end{aligned}$$

3. Show that $I(k^n) = \left\{ \mathfrak{m} \in \text{maxSpec } R \;\middle|\; R/\mathfrak{m} = k \right\}$.

Hint: consider the images of $t_1, \cdots, t_n$ in $R/\mathfrak{m}$.

The following result will imply the weak nullstellensatz:

Lemma 28.1 ***(Zariski, 1947).***
Let k be a field, R a finitely generated k-algebra, $\mathfrak{m} \in \operatorname{maxSpec} R$. Then $[R/\mathfrak{m} : k] < \infty$. Equivalently, if K/k is a field extension that is finitely generated as a k-algebra, then K is finitely generated as a k-vector space.

Proof .

Case 1: $K = k(\alpha_1, \cdots, \alpha_n)$ is algebraic.
In this case you get the obvious tower of extensions where each extension is finite, so $[K : k]$ is finite.
Case 2: K/k is not algebraic.
We can choose a transcendence basis $t_1, \cdots, t_n$, and since K is finitely generated as a field extension over k, the transcendence degree is finite. Then $k \subset k(t_1, \cdots, t_n) \subset K$ and K is algebraic over $k(t_1, \cdots, t_n)$, so $[K : k(t_1, \cdots, t_n)] < \infty$. By the Artin-Tate lemma, $k(t_1, \cdots, t_n)/k$ is a finitely generated k-algebra. But then $k(t_1, \cdots, t_n)$ is finitely generated over $k(t_1, \cdots, t_{n-1})$, so it suffices to consider the case of one variable. In other words, we need to show that for all k, $k(t)$ is not a finitely generated k-algebra.
Supposing otherwise, let $\{r_i(t)\}$ be a finite set of rational functions that are generators. Factor each r_i as f_i/g_i Since $k[t]$ is a PID with infinitely many primes, i.e. infinitely many nonassociate irreducible polynomials. So choose q monic, irreducible, not equal to any of the f_i; then $\frac{1}{q \notin k[f_1, \cdots, f_n]}$, a contradiction.

■

So rational function fields are not finitely generated over their base fields, or even finitely generated over their polynomial rings.

Exercise Show that a PID is Jacobson iff Spec R is infinite.

Exercise Show that R is Jacobson iff for every $\mathfrak{p} \in \operatorname{Spec} R$, we have $\mathfrak{p} = \bigcap_{\mathfrak{p} \subset \mathfrak{m} \in \operatorname{maxSpec} R} \mathfrak{m}$.

Proposition 28.2 ***(Rabinovitch? Trick).***
For k a field and $n \in \mathbb{Z}^+$, $k[t_1, \cdots, t_n]$ is a Jacobson ring.

To see why the weak nullstellensatz and this trick imply the Nullstellensatz, we show that for $J \trianglelefteq R = k[t_1, \cdots, t_n]$, $\operatorname{rad} J = \overline{J} = I(V(J)) = I(V(\operatorname{rad} J)) = \overline{\operatorname{rad} J}$, so wlog we can assume J is radical and show that $\overline{J} = J$.

Taking J a radical ideal, $J = \bigcap_{\mathfrak{p} \subset J} \mathfrak{p} \overset{\text{RT}}{=} \bigcap_{\mathfrak{m} \supset J} \mathfrak{m} \overset{\text{WN}}{=} \bigcap_{a \in k^n, \mathfrak{m}_a \supset J} \mathfrak{m}_a$. Then $J \subset \mathfrak{m}_a$ iff for all $f \in J$, $f(a) = 0$, i.e. $a \in V(J) = \bigcap_{a \in V(J)} I(\{a\}) = I(V(J)) = \overline{J}$.

Next time: proof of RT.