Commutative Algebra

D. Zack Garza

February 28, 2020

Contents

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'.

Theorem of Swan: A theorem about topological vector bundles over $C([0, 1])$, see textbook. 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: A topological space is called *boolean* (or a *Stone space*) iff it is compact, hausdorff, and totally disconnected.

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

Definition: A ring is boolean if every element is idempotent, i.e. $x \in R \implies x^2 = x$.

Exercise: If R is a boolean domain, then it is isomorphic to the field with 2 elements.

Lemma: 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. $\text{Hol}(\mathbb{C}, \mathbb{C}) \coloneqq \left\{ f : \mathbb{C} \longrightarrow \mathbb{C} \;\middle|\; f \text{ is holomorphic} \right\}$.

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 $\text{Hol}(X)$ be the holomorphic functionals $f : X \longrightarrow \mathbb{C}$. Then $\text{Hol}(X)$ 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 $\text{Hol}(X)$ is just constant functions by the open mapping functions. So $\text{Hol}(X) = \mathbb{C}$, and $\text{carddim}\mathbb{C} = 0$ because for any field there are only two ideals, and here (0) is prime. Moreover, $\text{carddimHol}(\mathbb{C}) \geq \alpha_0$.

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

Theorem: If X is a connected complex manifold which has a nontrivial holomorphic function, i.e. $\text{Hol}(X) \supset \mathbb{C}$, then there exists a chain of prime ideals in $\text{Hol}(X)$ 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: 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: 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: 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: 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 $\{I_j\}$, the infimum is the intersection and supremum is defined as $\left\langle I_j \;\middle|\; j \in J \right\rangle$, the smallest ideal containing all of the I_j, i.e. $\langle y \rangle = \left\{ \sum^{n} r_i y_i \;\middle|\; n \in \mathbb{N}_{>0},\ r_i \in R,\ y_i \in y \right\}$.

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: 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

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

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 (?) an ideal in the ideal lattice; the dual notion will come from localization.

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: 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.

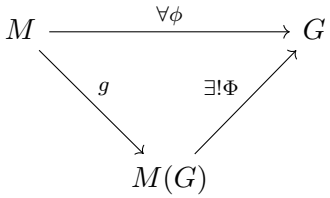
5 Wednesday January 22nd

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 $3 \implies 1$.

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

Definition: $z \in M$ 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: $\mathcal{I}^\bullet \cong (\mathbb{Z}^+, \cdot)$.

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 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

$$\begin{aligned} f^* f_*(I) &\supseteq I \\ f_* f^*(J) &\subseteq J. \end{aligned}$$

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

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

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

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

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

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

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

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 $\mathfrak{m} \in \operatorname{Spec}_{\max}(S)$ that $f^*(\mathfrak{m})$ is prime but need not be maximal.

Exercise: Show that if f is an integral extension, then maximals do pull back to maximals.

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: 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 $\mathfrak{p} \in \operatorname{Spec}(R)$. 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: 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 $\operatorname{Spec}(R_1 \times R_2)$ in terms of $\operatorname{Spec}(R_1)$ and $\operatorname{Spec}(R_2)$.

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 (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

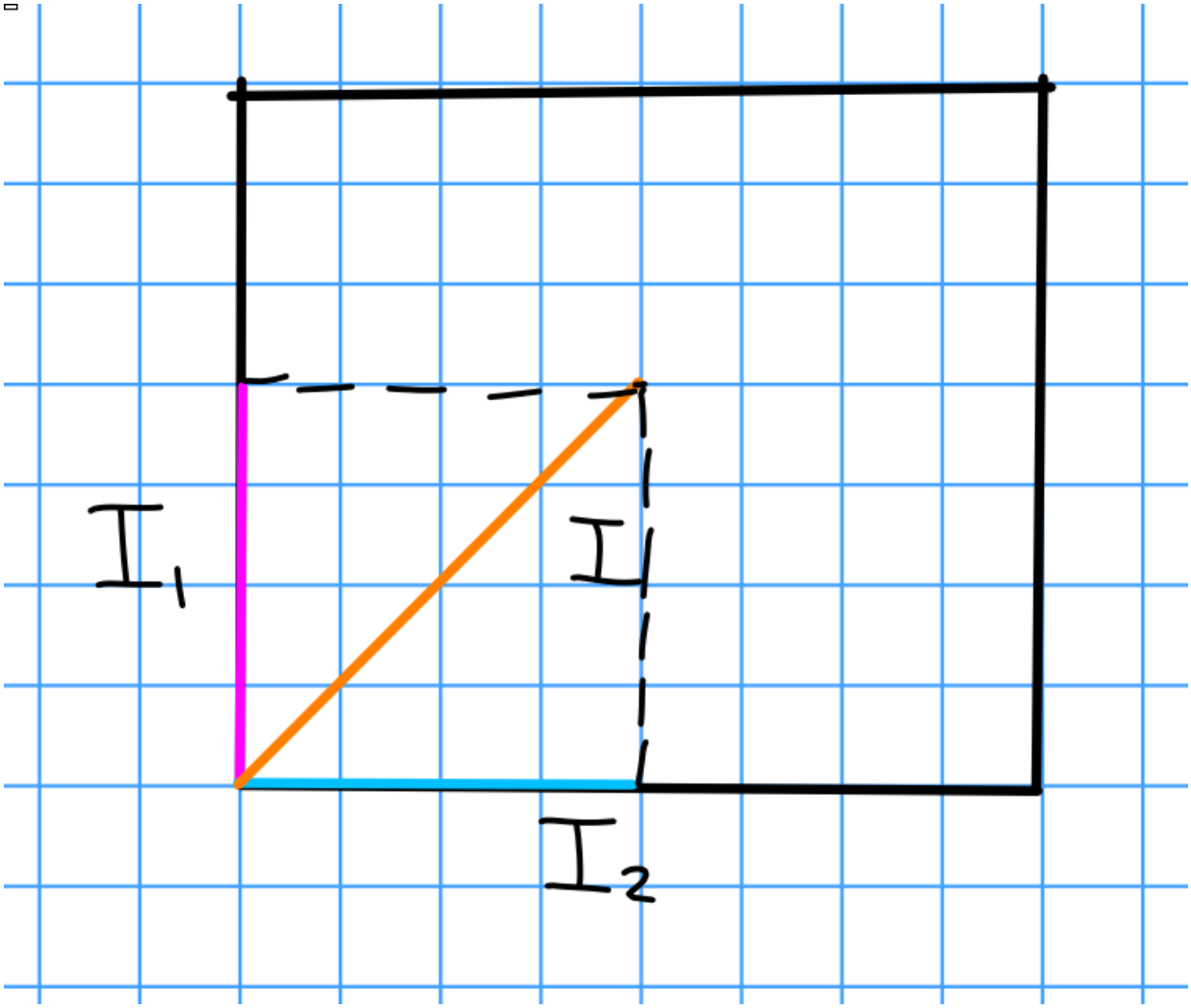


Figure 1: Image

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

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

$$R/e_2 R = \frac{R_1 \times R_2}{0 \times R_2} = R_1$$
$$R/e_1 R = \frac{R_1 \times R_2}{R_1 \times 0} = R_2.$$

■

We thus have a correspondence

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

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

Definition: 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 $\operatorname{Spec}(R)$ 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 $\operatorname{End}(M)$ for a group is a (potentially noncommutative) ring. An R-module structure is a ring homomorphism $R \longrightarrow \operatorname{End}(M)$. 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 $\operatorname{Ann}(m) = \left\{ r \in R \;\middle|\; xm = 0 \right\} \trianglelefteq R$; 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 $x \sim m \iff xm = 0$.

For any subset $S \subset M$, define $\operatorname{Ann}(S) \coloneqq \left\{ x \in R \;\middle|\; xm = 0 \;\forall m \in S \right\}$. Show that $\operatorname{Ann}(S) = \bigcap_{m \in S} \operatorname{Ann}(m)$ and $\operatorname{Ann}(M) = \left\{ x \in R \;\middle|\; xM = 0 \right\} = \ker(R \longrightarrow \operatorname{End}(M))$.

Definition: M is faithful iff $\text{Ann}(M) = 0$ iff $R \hookrightarrow \text{End}(M)$ is an injection.

Exercise: Any M is naturally a faithful $R/\text{Ann}(M)$-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 $r \;\middle|\; s$, 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 (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 $\mathrm{Ann}(R/I) = I$.

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 Friday January 31st

8.1 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: 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.

8.2 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: $M[\text{tors}] \coloneqq \left\{ m \in M \;\middle|\; \text{Ann}(m) \neq (0) \right\} \leq M$ is the torsion submodule of M.

Definition: 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: 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: 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: 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. So f.g. torsion-free is strictly weaker then free in this setting.

9 Monday February 3rd

Some module topics from Chapter 8.

9.1 Noetherian and Artinian Modules

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

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

Proposition: X is Noetherian iff $X^\vee$ is Artinian.

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

Proof: Apply DCC.

■

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

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

Then $N_1 = N_2$.

Proposition: 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: 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.

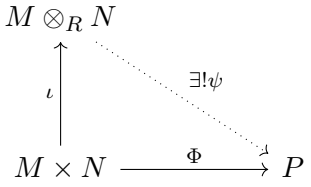
If M is a finitely-generated R-module, it is a quotient of a finitely-generated free R-module, and in particular $0 \longrightarrow K \longrightarrow R^n \longrightarrow M \longrightarrow 0$ is exact. So M is Noetherian, by the previous proposition (middle of a SES Noetherian $\implies$ ends are Noetherian).

■

9.2 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: 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 $\Big\{(m,n) \;\Big|\; m \in M,\ n \in N\Big\}$. 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 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: 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!

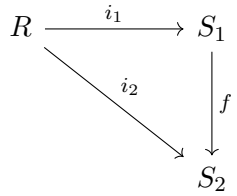
10 Wednesday February 5th

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.

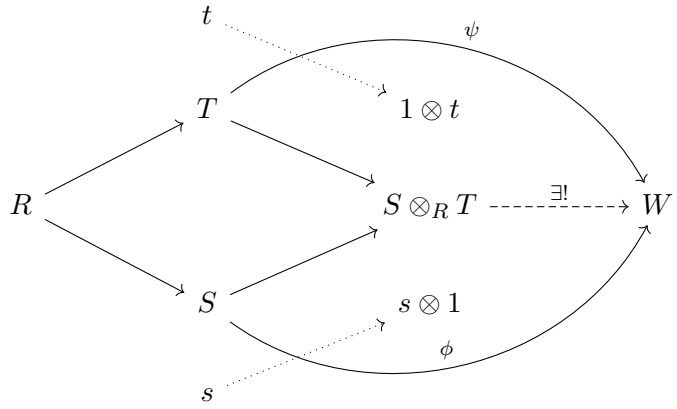
We have a notion of *pullback*, where if $i : R \longrightarrow S$ and N is an S-module then i^*N is an R module with action given by composition $R \xrightarrow{i} S \dot{\to} \mathrm{End}_{\mathbb{Z}}(N)$.

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 $R/I \otimes_R M = M/I$.

> 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: 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: R satisfies the *rank condition* iff whenever there exists a $q : R^m \twoheadrightarrow R^n$, $n \leq m$. 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: 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 $\mathfrak{m} \in \text{maxSpec}\ (R)$. 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: 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.

11 Friday February 7th

11.1 Projective Modules

For X a topological space and $\pi : E \longrightarrow X$ a real vector bundle on X. Then $\Gamma(E, X) = \left\{\sigma : X \longrightarrow E \;\middle|\; \pi \circ \sigma = \text{id}_X\right\}$ 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

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

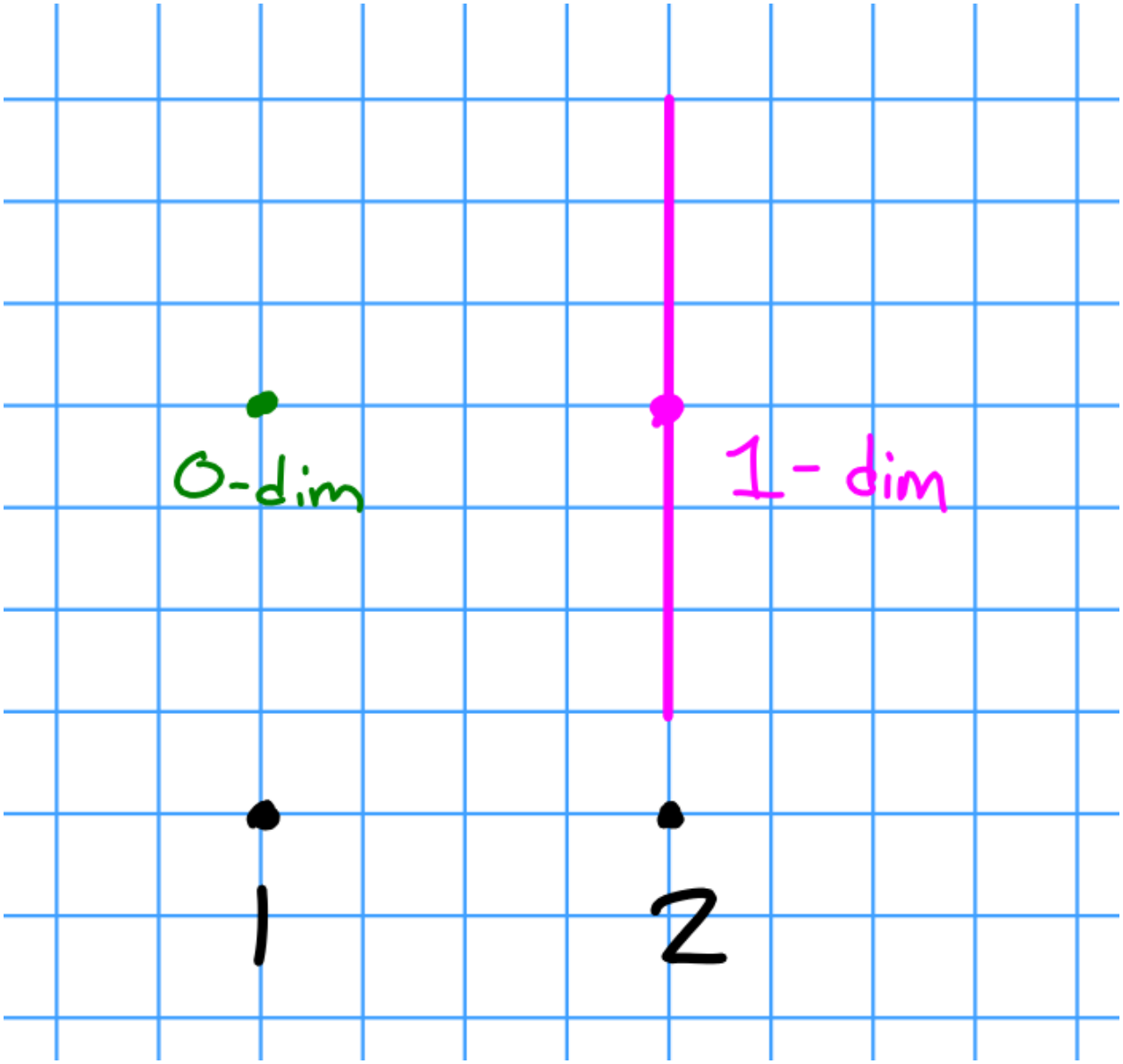
Then $\tilde{\sigma} : X \longrightarrow \mathbb{R}^n$, or equivalently a collection of n continuous functions $\tilde{\sigma}_j \longrightarrow \mathbb{R}$. Thus $\Gamma(X, E) \cong C(X, \mathbb{R})^n$.

Theorem (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: 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: 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: A module P is projective iff $0 \longrightarrow M \longrightarrow N \longrightarrow P \longrightarrow 0$ is split.

Exercise: show that free implies projective. Lift basis and use universal property.

Theorem: If P is projective, then there exists a K such that $P \oplus K$ is free.

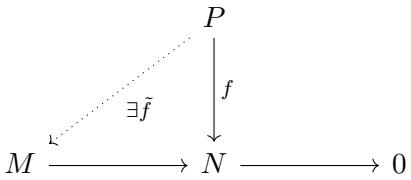
Idea: summands can be *both* a submodule and a quotient module.

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.

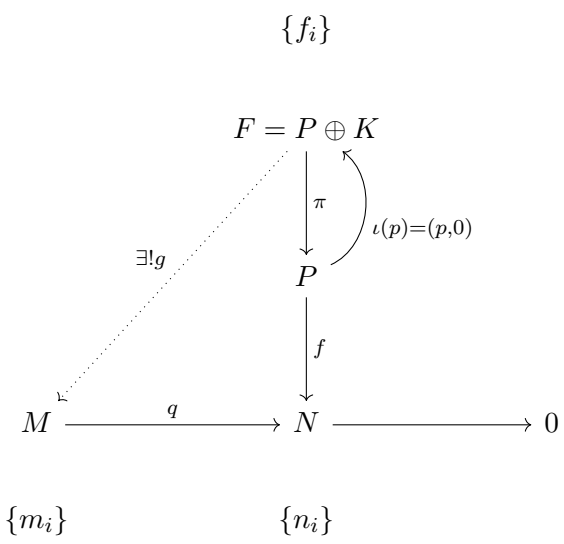
■

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: 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.



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.

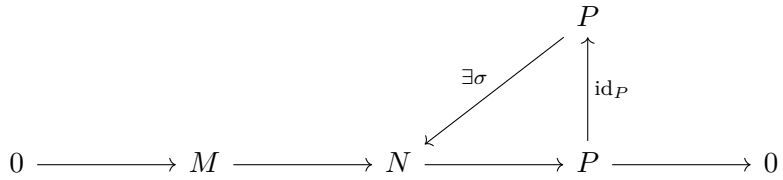
Todo: Revisit!

■

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 $\text{Spec}(R_1 \times R_2) = \text{Spec}R_1 \coprod \text{Spec}R_2$

Example (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: Let $R = \mathbb{C} \times \mathbb{C}$, so $\text{Spec}R = \{1, 2\}$, then $M_1 = \mathbb{C} \times 0 \longrightarrow \text{Spec}R$, 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.

12 Wednesday February 12th

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 $\text{Ann}(M \otimes_R N) = \text{Ann}M + \text{Ann}N$. Does this hold for every M, N? The answer is no; we have $\text{Ann}(M \otimes_R N) \supseteq \text{Ann}M + \text{Ann}N$. 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 $\text{Ann}(M/IM) = \text{Ann}(M) + I$? 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: 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 (3.17): Let $I, J, K_1, \cdots, K_n \trianglelefteq R$. Then

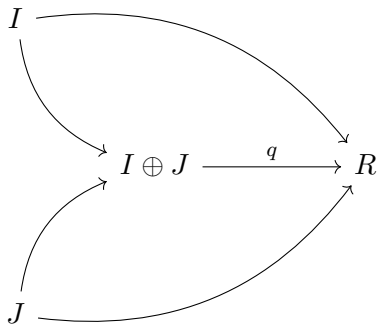
a. $(I + J)(I \bigcap J) \subseteq IJ$

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.

Proposition: 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.

Definition: 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: 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 (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 (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.

13 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: 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: 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.

Big theorem (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: 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: 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: 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:

Fact (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 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 $\{\overline{p}_i\}^a$ of $P/\mathfrak{m}P$ and $\left\{\overline{q}_j\right\}^b$ 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.

13.1 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:

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

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

Example: 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: 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: 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: 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.

Proposition: 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 (NAK, a.k.a. Nakayama-Azumaya-Krull): Let $J \trianglelefteq R$ be an ideal and $M \in \mathrm{R-mod}$ 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: Suppose $J \in \mathcal{J}$ and $M \in \mathrm{R-mod}$ 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: 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: Let $J \in \mathcal{J}$, $M \in \mathrm{R-mod}$ f.g., $x_1, \cdots, x_n$ such that $\{\overline{x}_i\} \in M/JM$ 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.

■

Proposition 3.44 (Generalized NAK): Let $J \trianglelefteq R$, $M \in \mathrm{R-mod}$ 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 $J, \text{Ann}M$ are comaximal, and $J \in \mathcal{Z}$, which forces $\text{Ann}M = R$ and thus $M = 0$.

14 Monday February 17th

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

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

Generalized Nakayama: $M = JM \iff J + \text{Ann}M = R$. The reverse implication is immediate, the forward is by Nakayama.

14.1 Injective Modules

Recall that every R-module is free $\iff$ R is a field. What is the analogous condition for every R-module to be projective?

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

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: 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: M is simple iff $\exists 0 \subsetneq N \subsetneq_R M$.

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

Proof: Omitted, see chapter 8 of notes.

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

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

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

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

In fact, the converse is true:

Theorem: If R is semisimple, then R is a product of fields.:

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

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

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

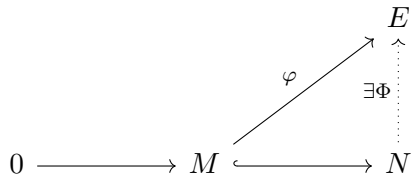
> Note that splitting is slightly stronger than $M_2 \cong M_1 \oplus M_3$.

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: 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: For an R-module E, TFAE

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



4. If $M \hookrightarrow N$, then $\hom(N, E) \twoheadrightarrow \hom(M, E)$.
5. 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: $\mathbb{Z}$ 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.

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: A ring R is *self-injective* iff R is injective as an R-module.

Example: A field or a semisimple ring.

Claim: 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.

[1] 1

Example: Let $R = \mathbb{Z}/p^n\mathbb{Z}$, and let M be a finite p-primary commutative group (i.e. a p-group). Then $\exp M = p^n \iff \mathrm{Ann} M = (p^n)$. 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

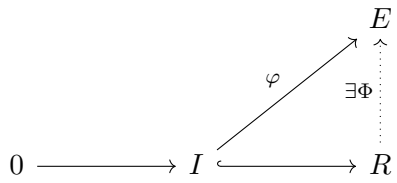
$$0 \longrightarrow \langle x \rangle \longrightarrow M \longrightarrow M/\langle x \rangle \longrightarrow 0.$$

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?

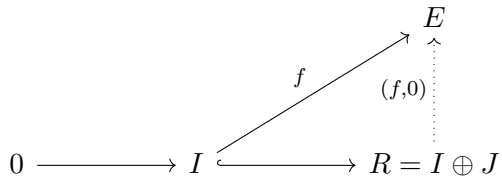
Baer's Criterion: If suffices to check the lifting condition for $N = R$ and $M = I \trianglelefteq R$. I.e. if there is a lift of the following form:



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.

15 Monday February 24th

15.1 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 $M \cong R/\text{Ann}M$, and there are two cases:

- $\text{Ann}M = 0$, 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 $x \in \text{Ann}(M) \setminus \{0\}$. 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.

15.2 Toward Localization

Proposition 15.1 ***(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 15.2.
Let $\mathfrak{p} \in \operatorname{Spec}(R)$ 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 $x \coloneqq \prod x_i \in \prod I_i \subset \mathfrak{p}$; 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.

15.3 Radicals

Definition 15.1.
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 15.3.
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 15.4.
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) $I^{\sum e_i} = (0)$.

■

An ideal is nil iff all generators are nilpotent.

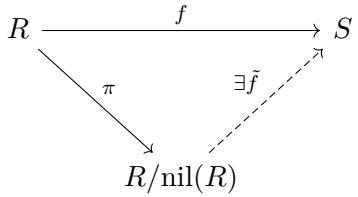
Corollary: If R is Noetherian, I is nilpotent iff I is nil.

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 15.2.
The *nilradical* of R, $\operatorname{nil}(R)$, is the set of all nilpotent elements.

Proposition 15.5. a. $\operatorname{nil}(R) \trianglelefteq R$, since $a^n = b^n = 0 \implies (xa + yb)^{2n} = 0$.

b. $R/\mathrm{nil}(R)$ 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. $\mathrm{nil}(R) = \bigcap_{\text{prime ideal}} \mathfrak{p}$.

Proof (of c).
$\subseteq$: If $x \in \mathrm{nil}(R)$, 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 $\mathfrak{p} \in \mathrm{Spec}(R)$ such that $S \bigcap \mathfrak{p} = \emptyset$.
■

Definition 15.3.
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 15.6.
Prime ideals are radical.

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

16 Wednesday February 26th

16.1 Radicals

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

Definition 16.1.
For $I \trianglelefteq R$, we define $\mathrm{rad}(I) = \left\{x \in R \;\middle|\; \exists n,\ x^n \in I\right\} \supseteq I$.

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

Definition 16.2.
I is a *radical ideal* iff $I = \mathrm{rad}(I)$.

Example 16.1.
Prime ideals are radical.

Definition 16.3.
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 16.1.
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 $x^{2n} = x^n x^N \in IJ \implies x \in \text{rad}(IJ)$.

■

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

■

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

■

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

Example 16.2.
Take $R = \mathbb{C}[x]$, a PID. Suppose $I \trianglelefteq R$ and $\text{rad}(I) = x^n$, 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 $J = \text{rad}(I)$, 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 $\text{rad}(I) = \langle x, y \rangle$ 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 16.4.
The *Jacobson radical* is defined by $\mathcal{J}(R) = \bigcap_{\mathfrak{m} \in \text{maxSpec } (R)} \mathfrak{m}$.

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

Example 16.3.
If $(R, \mathfrak{m})$ is a local domain, then $\text{nil}(R) = 0$ and $\mathcal{J}(R) = \mathfrak{m}$.

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

Proposition 16.2.
$x \in \mathcal{J}(R) \iff 1 \pm xR \subset R^\times$.

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

17 Friday February 28th

17.1 Radicals: The Jacobson Radical

Definition 17.1.
$\mathcal{J}(R) = \bigcap \mathfrak{m} \in \text{maxSpec } (R)\mathfrak{m}$. 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).

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 17.2.
A ring is *semiprimitive (or $\mathcal{J}$-semisimple or Jacobson-semisimple)* iff $\mathcal{J}(R) = 0$.

Proposition 17.1.
$x \in \mathcal{J}(R) \iff 1 - xR \subset R^\times$.

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.

17.2 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 17.2 ***(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 17.3 ***(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 $(r', \overline{s}) \in R' \times R/I_n$. 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 $s + I_n = \overline{s} + I_n$.
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 $R/I \otimes R/J$.

17.3 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 17.1.
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 $\left(\sum_{m\in M} r_m[m]\right)\left(\sum_{m\in M} s_m[m]\right) =?$.