Today, we'll wrap up our "Algebra Boot Camp"
- Structure Theory for Abelian groups
- Modules, associated primes, primary decomps.

Recall that last lecture, we saw that

1. Thm (p.476, thm) TFAE
   - A linear operator on a
     \( \mathbb{R} \)-vector space
   - A \( \mathbb{R}[t] \) module, where \( \mathbb{R} \) is a field.

   Remark: \( \mathbb{R} \) a ring, then an \( \mathbb{R} \)-module \( M \) (reminder) is an Abelian gp under +, with \( \mathbb{R} \) acting linearly on \( M \) as \( \mathbb{R}(m+nr) = rm + rm \)

2. Thm (p.479, thm) Any linear operator \( T \) on a vsfd \( V/\mathbb{R} \) has a matrix where \( T \) consists of diagonal blocks which are invariant.

\[ B_i = \begin{pmatrix} 0 & \cdots & 0 & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & 0 & 0 \\ 0 & \cdots & 0 & 0 \end{pmatrix} \]

\[ T = \begin{pmatrix} B_1 & 0 & \cdots & 0 \\ 0 & B_2 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & B_k \end{pmatrix} \]
Fundamental Thm of Abelian Gps (FTAG)

A) A general Abelian group is isomorphic as a \( \mathbb{Z} \)-module, to

\[
A \cong \mathbb{Z}^k \oplus \bigoplus_{i=1}^{n} \mathbb{Z}/p_i \quad \text{aside, primes}
\]

\[
\bigoplus_{i=1}^{n} \mathbb{Z}/p_i \quad \text{not distinct, } p_i \text{ not distinct}
\]

\[\bigoplus_{i=1}^{n} \mathbb{Z}/p_i \cong \mathbb{Z}/p_1 \times \mathbb{Z}/p_2 \times \cdots \times \mathbb{Z}/p_n\]

Notice: any abelian gp is a \( \mathbb{Z} \)-module, if all \( n \)-times because

\[n \cdot a = a + a + \cdots + a\]

\( \text{in fact, } \mathbb{Z} \)-module

\( \text{Ab. Grp.} \)

B) Same hypotheses, then

\[A \cong \mathbb{Z}^k \oplus \bigoplus_{i=1}^{n} \mathbb{Z}/d_i \text{ with } d_i \mid d_{i+1}\]

\[d_i \neq 0, 1\]

Why are A, B same?

Lemma: If \( p_1, p_2 \) distinct primes, then

\[\mathbb{Z}/p_1 \times \mathbb{Z}/p_2 \cong \mathbb{Z}/p_1 p_2\]

Thm A an \( m \times n \) integer matrix, then \( \exists \ P, Q \)

elementary \( \mathbb{Z} \)-matrices so that

\[A' = QA P^{-1}\] is diagonal, of form

\[
\begin{bmatrix}
d_1 & 0 & 0 \\
d_2 & \ddots & 0 \\
0 & \cdots & d_n
\end{bmatrix}
\]

with \( d_i > 0 \)

\( d_i \mid d_{i+1} \)
Recall elementary matrices

- add integer multiple of row/col to another row
- swap 2 rows or 2 cols
- multiply a row/column by a unit

**Example:** add $2r_1$ to $r_2$

\[
\begin{bmatrix}
1 & 0 \\
2 & 1
\end{bmatrix}
\begin{bmatrix}
a & b \\
c & d
\end{bmatrix} =
\begin{bmatrix}
a & b \\
2a+c & 2b+d
\end{bmatrix}
\]

**Proof:** Do elem. ops to get

\[
A \rightarrow \tilde{A} = \begin{bmatrix}
d_1 & 0 & \cdots & 0 \\
0 & \ddots & \vdots & \vdots \\
0 & \cdots & B & 0 \\
0 & \cdots & 0 & B
\end{bmatrix}
\]

where $d_1$ divides all entries of $B$

*This is tricky!*, key is Euclid's Alg.

To do this:

**STEP 1** Permute rows/cols to get entry of $A$ with smallest absolute value into position $(1,1)$

**STEP 2** Use $(1,1)$ entry to clear out row, col

**Warning:** This is not as easy as when our matrix is over a field!
Lecture 3

Suppose we have \[
\begin{bmatrix}
2 \\
3 \\
\end{bmatrix}
\]

Use 2 to reduce 3 to 1. Now go back to STEP 1, moving 1 to (1,1).

STEP 2 (explicitly) \[ a_{i1} = a_{ii} g + r \]

If \( r = 0 \), \( a_{i1} \) is cleared out.

else \( r < a_{ii} \), go to STEP 1, replacing \( a_{ii} \) w/ r.

(\[\text{Can't go on forever.}\]\]

This process gets us to a matrix of the form \( \begin{bmatrix} \ast \end{bmatrix} \), but don't have \( d_1 \) for all entries of B.

STEP 3: If some entry \( b \in B \) is not divisible by \( d_1 \), add that column to \( \text{Col}_1 \);

\( \text{Col}_1 \) now has an entry \( b \).

Repeat step 2:
\[
\begin{bmatrix}
a_{ii} \\
0 \\
\end{bmatrix}
\begin{bmatrix}
0 \\
b \\
\end{bmatrix} = a_{ii} g + r \quad r \neq 0
\]

\( \Rightarrow r < a_{ii} \)

Back to STEP 1

Process terminates because our \( s \) keep getting smaller.
Presentation Matrices

Lemma A f.g. module $M/R \nrightarrow$ Noetherian if

has a presentation matrix

$R^n \xrightarrow{f} R^m \rightarrow M \rightarrow 0$

rels gens (f.g., ok)

(relns is also f.g., because submodule of $R^n$)

Clearly a PID is Noetherian (every ideal has 1 gen!)

Aside Can do without Noetherian, just assume PID

induct on # gens of $M$

if 1 gen, then $R \xrightarrow{1} M \rightarrow 0$, kernel is an ideal, but $R$ a pid so kernel = $<f>$

$R \xrightarrow{1} R \rightarrow M \rightarrow 0$ base case.

Now suppose there if $M$ has $\leq n$ gens, add take $M$ with $n+1$ gens, $x_1, \ldots, x_{n+1}$.

$M/x_i R$ has $n$ gens, finite pres (IH)

$x_i R$ has 1-gen

\[ \begin{array}{cccc}
0 & \rightarrow & R & \rightarrow & M \\
\downarrow & & & & \downarrow \\
0 & \rightarrow & R & \rightarrow & R \\
& & \downarrow & & \\
& & 0 & \rightarrow & 0 \\
\end{array} \]

Exercise - use these to get presentation for $M$. 

\[ \begin{array}{cccc}
0 & \rightarrow & R & \rightarrow & R^m \\
& & \downarrow & & \\
& & M & \rightarrow & R^m \\
& & \downarrow & & \\
& & 0 & \rightarrow & 0 \\
\end{array} \]
Lecture 3

Proof (FTAG)

1. If $A$ is a finitely Abelian group = $\mathbb{Z}$-module, then we have $\mathbb{Z}^m \xrightarrow{\phi} \mathbb{Z}^n \xrightarrow{\pi} A \xrightarrow{\epsilon} 0$ a presentation by previous lemma, $m$

2. By diagonalization then, $\phi = \begin{bmatrix} d_1 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & d_k \end{bmatrix}$

Notice: This says, since $A = \ker \phi$, that $A \cong \mathbb{Z}/d_1 \oplus \mathbb{Z}/d_2 \oplus \cdots \oplus \mathbb{Z}/d_k \oplus \mathbb{Z}^{n-k}$ with $d_i | d_{i+1}$

The same argument works for modules over a PID, see Hungerford, IV 6.12

This concludes our work on structure theory for modules over a Euclidean Domain.

Reminder: This structure theory is the fundamental ingredient in the description of PH as a barcode.
Second Topic of Today: Associated Primes, Primary Decomposition

Recall in Lecture 1, for \( I \subset k[x_1, \ldots, x_n] \), we defined \( V(I) = \{ p \in k^n : f(p) = 0 \text{ for all } f \in I \} \)

Example: \( V(x^2 - x, xy - x) \subset \mathbb{R}^2 \).

Notice: \( \langle x^2 - x, xy - x \rangle = \langle x \rangle \cap \langle x - 1, y - 1 \rangle \)

Aside: we've not yet met operations on ideals.

Exercise: \( I, J \) ideals in \( R \), then \( \sqrt{I + J} \) are ideals in \( R \).

DEF: \( I \) an ideal is irreducible if \( I \neq \bigcup_i I_i \), \( I_i \in \mathfrak{P} \);

A primary ideal if \( x \cdot y \in I \Rightarrow x \in I \text{ or } y^{n} \in I \).

Thm: R. Noether, then any \( I = \bigcap_i I_i \) is irreducible.

Pf: Let \( \Sigma = \) set of all ideals which can't be written as above. Since R. Noether, \( \Sigma \) has a max elt \( I' \). \( I' \) is reducible, so \( I' = I_1 \cap I_2 \), \( I_i \in \mathfrak{P} \), \( I_1 \neq I_2 \), and \( I_i \) are not in \( \Sigma \).

\[ \Rightarrow I' \text{ is a finite } \cap \text{ of } \mathfrak{P} \text{ s} \]

DEF: \( \overline{I} = \{ f \mid f^n \in I \text{ for some } n \in \mathbb{Z}^+ \} \).
(Scheme, ) Fact: In a Noetherian ring, \( I \mid I \Rightarrow \text{primary.} \)

Hence, in a Noetherian ring

\[ I = \bigcap Q_i = \text{primary.} \]

Clearly, \( \overline{\bigcap Q_i} = P_i \)

Example: \( I = \langle x^2 - x, xy - x \rangle = \langle x \rangle \cap \langle x - 1, y - 1 \rangle \)

Notice: \( R[x,y]/_{\langle x \rangle} \cong \mathbb{Z}[y] \) Domain \( \Rightarrow \langle x \rangle \) prime

\( \frac{R[x,y]}{\langle x - 1, y - 1 \rangle} \cong R \) Field \( \Rightarrow \langle x - 1, y - 1 \rangle \) prime

So we've broken \( V(I) \) into \( V(x) \cup V(x - 1, y - 1) \)

Warning: \( \langle x^2, xy \rangle = \langle x^2, y \rangle \cap \langle x \rangle = \langle x^2, xy, y^2 \rangle \cap \langle x \rangle \) both primary decays

* Primary Decomposition is not unique

But the \( NQ_i = P_i \) are unique.

\[ \text{DEF}\text{1} \quad (P_i \text{ is an associated prime of } I) \]

\[ \begin{cases} & \text{if } I = \bigcap Q_i, \overline{\bigcap Q_i} = P_i \end{cases} \]

\[ \text{DEF}\text{2} \quad M \text{ an } R \text{-module, } \text{associated prime of } M \]

\[ \text{if } P = \text{ann}(m), \text{ some } m \in M. \]

Huh? What?
Notice if $P$ is the annihilator of $m \in M$, then consider the submodule (principle)

$$0 \to R : m \to M$$

is

$$R / P$$

In particular, if $M = R \pi$ and $I = \cap \pi_i$ with $\pi_i = P_i$

Clearly $R / P_i \to R / \pi_i \to R / I$

(since $P_i \supseteq \pi_i \supseteq I$) so DEF1 and DEF2 agree.

Who cares

Idea: In topology, a vector bundle on a space $X$ is a collection of vector spaces (all $\cong$) which vary continuously (smoothly, holomorphically, ...) with $p \in X$.

E.g. Line Bundle {1-d vect space} on a curve $C$

"looks like"
Q: How do we visualize a module?
A: Like a Vector Bundle, but the fibers differ

Key idea: Use localization

Visualize the module \( M = \mathbb{R} / \langle x^2 - x, xy - x \rangle \) over \( \mathbb{R}^2 \)

Localize \( M \) at associated primes

\[
M \langle x \rangle 
\quad \text{things outside } x \text{ are units} \Rightarrow x \text{-1, y-1 units}
\Rightarrow M \langle x \rangle \cong \frac{\mathbb{R}}{\langle x \rangle} \cong \mathbb{R}_{y-1} \text{ a line}
\]

\[
M \langle x-1, y-1 \rangle \Rightarrow x \notin \langle x-1, y-1 \rangle \Rightarrow \text{unit} \Rightarrow M \langle x-1, y-1 \rangle \cong \mathbb{R}_{(x-1, y-1)}
\]

\[
M(p) \text{ pa prime } \notin \langle x \rangle, \langle x-1, y-1 \rangle?
\]

then \( x \notin p \), \( x-1, y-1 \notin p \Rightarrow \text{they are units} \)

\[
= x(x-1) \text{ is a unit} \Rightarrow \mathbb{R}_{\text{unit}} = 0
\]

So,

\[
\text{line zero everywhere else.}
\]

\[
\text{over } (x-1, y-1) \text{ we get a point}
\]
1. Prove if \( p_1, p_2 \) distinct primes, then \( \mathbb{Z}/(p_1 p_2) \cong \mathbb{Z}/p_1 \times \mathbb{Z}/p_2 \).

2. Reduce the integer matrix \[
\begin{bmatrix}
3 & 1 & -4 \\
2 & -3 & 1 \\
-4 & 6 & -2
\end{bmatrix}
\]
to diagonal form using (integer) elementary operations.

3. Complete proof on p4 (notes) that a finitely generated module over a PID has a finite presentation.

4. \( I, J \) ideals in \( R \), show \( \{ I+I, I \cap J, I \cdot J \text{ are ideals} \} \).