Lecture 7.

1) Further discussion of PID's.
2) Main Thm on modules over PID's.
3) Proof of the main Thm.

Ref: Dummit & Foote, Chapter 12.

BONUS: Finite dimensional modules over $\mathbb{C}[x,y]$.

1) Further discussion of PID's.

Let A be a PID. Take $a_1, \dots a_n \in A \rightsquigarrow$ ideal $(a_1, \dots a_n) \subset A$

$\exists\, d \in A \mid (a_1, \dots a_n) = (d)$, defined uniquely up to invertible factor

- d divides $a_1, \dots, a_n$ b/c $a_1, \dots, a_n \in (d)$.
- d' divides $a_1, \dots, a_n \Rightarrow d'$ divides $d \left(= \sum_{i=1}^{n} x_i a_i \text{ for some } x_1, \dots x_n \in A\right)$.

This d is the GCD of $a_1, \dots a_n$.

Classical application of GCD: PID $\Rightarrow$ UFD.

Remarks: • in a PID every prime ideal $\neq \{0\}$ is maximal:

$(f) \supseteq (p) \Leftrightarrow p \vdots f \Leftrightarrow$ [for (p) prime] $\Leftrightarrow (f) = (p)$ or $(f) = A$.

• PID $\Rightarrow$ Noetherian.

2) Main Thm on modules over PID's.

2.1) Statement.

Let A be PID. Let M be a fin. gen'd A-module.

Thm: 1) $\exists\ k\in\mathbb{Z}_{\geqslant 0}$, primes $p_1,\dots p_\ell \in A$, $d_1,\dots,d_\ell\in\mathbb{Z}_{>0}$ s.t

$$M\simeq A^{\oplus k}\oplus\bigoplus_{i=1}^{\ell} A/(p_i^{d_i}).$$

2) k is uniquely determined by M, $(p_1^{d_1}),\dots,(p_\ell^{d_\ell})$ are uniquely determined up to permutation.

Example: For $A=\mathbb{Z}$, Thm = classif'n of fin. gen'd abelian gr'ps.

2.2) Case of $A=\mathbb{F}[x]$, $\mathbb{F}$ is alg. closed.

Assume $\dim_{\mathbb{F}} M<\infty$ (so $k=0$). $\mathbb{F}$ is alg. closed $\Rightarrow$ primes in $\mathbb{F}[x]$ are $x-\lambda$, $\lambda\in\mathbb{F}$, (up to invertible factor).

Main Thm $\Rightarrow$ $\exists\ \lambda_i\in\mathbb{F}$, $d_i\in\mathbb{Z}_{>0}$ s.t. $M=\bigoplus_{i=1}^{\ell}\mathbb{F}[x]/\left((x-\lambda_i)^{d_i}\right)$.

Reminder (Lec 3, Sec 2.2)

A module over $\mathbb{F}[x]$ = $\mathbb{F}$-vector space & an operator X.
For a fixed $\mathbb{F}$-vector space M, operators $X_M, X_M': M\to M$ give isomorphic $\mathbb{F}[x]$-module structures $\Leftrightarrow$ X_M, X_M' are conjugate:
$\varphi: M\to M$ is a homomorphism between the 2 module structures iff $\varphi\circ X_M = X_{M'}\circ\varphi$ so φ is an isomorphism $\Leftrightarrow$ $\varphi X_M\varphi^{-1}=X_M'$. So the Main Thm allows to classify linear operators up to conjugation.

Choose an $\mathbb{F}$-basis in $\mathbb{F}[x]/((x-\lambda_i)^{d_i})$: $(x-\lambda_i)^j, j=0,\dots d_i-1$.

$$X(x-\lambda_i)^j = [x=(x-\lambda_i)+\lambda_i] = \begin{cases}(x-\lambda_i)^{j+1}+\lambda_i(x-\lambda_i)^j & \text{if } j<d_i-1\\ \lambda_i(x-\lambda_i)^j & \text{if } j=d_i-1.\end{cases}$$

So X acts as a Jordan block:

$$J_{d_i}(\lambda_i)=\begin{pmatrix}\lambda_i & 1 & & 0\\ & \lambda_i & & \\ & & \ddots & 1\\ 0 & & & \lambda_i\end{pmatrix}$$

Main Thm in this case is:

Jordan Normal Form thm:

Let X be a linear operator on a fin. dim. $\mathbb{F}$-vector space, M, let $\mathbb{F}$ be alg. closed. Then in some basis X is represented by a "Jordan matrix": $\mathrm{diag}(J_{d_1}(\lambda_1),\dots, J_{d_\ell}(\lambda_\ell))$.

Can recover the pairs $(d_1,\lambda_1),\dots,(d_\ell,\lambda_\ell)$ from X - will discuss in Lec 8.

3) Proof of the main Thm.

3.1) Strategy of the proof of existence.

Since M is finitely generated, there's a surjective A-linear map $\pi: A^{\oplus n}\twoheadrightarrow M$. Let $N:=\ker\pi$, this is a submodule in M. The main part of the proof is to show that $\exists$ basis $e_1',\dots e_n'$ of $A^{\oplus n}$, $r<n$, and $f_1,\dots f_r\in A\setminus\{0\}$ s.t. $N=\mathrm{Span}_A(f_1e_1',\dots f_re_r')$.

Now note that if L_1, L_2 are A-modules & $N_i \subset L_i$, $i=1,2$ are submodules, then there is a natural isomorphism

(*) $(L_1 \oplus L_2)/(N_1 \oplus N_2) \xrightarrow{\sim} L_1/N_1 \oplus L_2/N_2$,

to construct it is an exercise.

So $A^{\oplus n}/N = (\bigoplus_{i=1}^{n} Ae_i')/(\bigoplus_{i=1}^{r} Af_i e_i') \xrightarrow[\sim]{(*)} \bigoplus_{i=1}^{r} Ae_i'/Af_i e_i' \oplus \bigoplus_{i=r+1}^{n} Ae_i' \xrightarrow{\sim} A^{\oplus n-r} \oplus \bigoplus_{i=1}^{r} A/(f_i)$.

Part 1 of the theorem will then follow from

Lemma: for $f = \varepsilon p_1^{d_1} \dots p_s^{d_s}$ (ε is invertible, $p_1, \dots p_s$ are distinct primes, $d_1, \dots d_s > 0$) we have $A/(f) \xrightarrow{\sim} \bigoplus_{i=1}^{s} A/(p_i^{d_i})$.

Proof:

It's enough to show that for $f_1, f_2 \in A$ w. $(f_1, f_2) = A$ ($\Leftrightarrow$ $GCD(f_1, f_2) = 1$), we have $A/(f_1 f_2) \xrightarrow{\sim} A/(f_1) \oplus A/(f_2)$, an A-module isomorphism (then we take $f_1 = \varepsilon p_1^{d_1} \dots p_{s-1}^{d_{s-1}}$, $f_2 = p_s^{d_s}$ and argue by induction on s).

Consider the natural projection $\pi_i : A/(f_1 f_2) \twoheadrightarrow A/(f_i)$, $a + (f_1 f_2) \mapsto a + (f_i)$, it's A-linear. We claim that

$$\pi = (\pi_1, \pi_2) : A/(f_1 f_2) \xrightarrow{\sim} A/(f_1) \oplus A/(f_2).$$

Since $GCD(f_1, f_2) = 1$ $\exists$ $a_1, a_2 \in A$, $a_1 f_1 + a_2 f_2 = 1$.

- π is injective: $\pi(a + (f_1 f_2)) = 0 \Leftrightarrow a \in (f_1) \cap (f_2) \Rightarrow$ $a = (a_1 f_1 + a_2 f_2) a = a_1 f_1 a + a_2 f_2 a \in (f_1 f_2)$ b/c $a \in (f_1) \Rightarrow f_2 a \in (f_1 f_2)$; $f_1 a \in (f_1 f_2)$. So $a + (f_1 f_2) = 0$.

- π is surjective: $\forall$ $x_1, x_2 \in A$ $\exists$ $x \in A$ s.t. $x - x_i \in (f_i)$. Take $x := a_1 f_1 x_2 + a_2 f_2 x_1$. So $x - x_1 = a_1 f_1 x_2 + \cancel{a_2 f_2 x_1} - (a_1 f_1 + \cancel{a_2 f_2}) x_1 = a_1 f_1 (x_2 - x_1) \in (f_1)$. $\square$

Rem: Similarly, one can prove a version of the Chinese remainder Thm: for ideals $I_1, I_2 \subset A$ (general ring) w. $I_1 + I_2 = A$, have $I_1 \cap I_2 = I_1 I_2$ & $A/I_1 I_2 \xrightarrow{\sim} A/I_1 \times A/I_2$ (as rings & as A-modules).

3.2) Basis vectors and their multiples.

We proceed to proving the existence part of Thm. We start w. the following question. Notice that every nonzero vector in a vector space can be included into a basis. Even for free modules over rings, this may fail: take $A = \mathbb{Z}$, $M = \mathbb{Z}$ & $m = 2 \in M$. So, we can ask a more general question: when is an element in $A^{\oplus n}$ a <u>multiple</u> of a basis element (which is obviously the case in our example above). We will see that the answer is YES, as long as A is a PID.

Let $m = (a_1, \dots a_n) \in A^{\oplus n}$, $m \neq 0$. Set $GCD(m) := GCD(a_1, \dots a_n)$

Lemma: The following claims hold:
(i) if $m = \sum_{i=1}^{n} b_i e_i'$ for some basis $e_1', \dots e_n'$ of $A^{\oplus n}$, then $GCD(b_1, \dots, b_n) = \varepsilon\, GCD(m)$ (w. ε invertible)
(i) there's a basis $e_1', \dots e_n'$ w. $m = d e_1'$ for $d \in A \setminus \{0\}$, automatically equal to $GCD(m)$ (by (i)).

Proof: Observe that two bases in $A^{\oplus n}$ are related via an invertible matrix: in particular, in (ii): $(b_1, \dots b_n)^T = X (a_1, \dots a_n)^T$ for

$X \in Mat_n(A)$ invertible. This is for the same reason as for fields. In particular, $b_i \vdots GCD(a_1, .. a_n)$. Similarly, $(a_1, ... a_n)^T = X^{-1}(b_1, ... b_n)^T$ $\Rightarrow a_i \vdots GCD(b_1, ... b_n) \Rightarrow GCD(a_1, .. a_n) = \varepsilon\, GCD(b_1, ... b_n)$, ε invertible. This shows (ii). The proof of i) is in two steps.

Step 1: (ii) for $n=2$. We need to find invertible $X \in Mat_2(A)$. w. $\begin{pmatrix} a_1 \\ a_2 \end{pmatrix} = X \begin{pmatrix} d \\ 0 \end{pmatrix}$ w. $d = GCD(a_1, a_2)$ (then e_1', e_2' are columns of X)
Let $a_i = x_{1i}\, d$ $(i = 1,2,\ x_{1i} \in A)$. Then $GCD(x_{11}, x_{12})$ is invertible;

$\exists\, x_{21}, x_{22} \in A \mid x_{22}x_{11} - x_{21}x_{12} = GCD(x_{11}, x_{12})$ (can assume $=1$).

Now take $X = \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix}$.

Step 2: (ii) for general n. We want to find invertible $Y \in Mat_n(A)$ w. $Y(a_1, ... a_n)^T = (d, 0, .. 0)^T$, then $d = GCD(a_1, ... a_n)$ by (ii).
We'll present Y as $Y_{n-1} Z_{n-1} Y_{n-2} ... Z_1 Y_1$, where

- $Y_1 = diag(Y_1', 1, ..., 1)$ w. Y_1' invertible in $Mat_2(A)$ w. $Y_1' \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} = \begin{pmatrix} d_1 \\ 0 \end{pmatrix}$ $d_1 = GCD(a_1, a_2)$, this Y_1' exists by Step 1. So $Y_1 \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} d_1 \\ 0 \\ a_3 \\ \vdots \\ a_n \end{pmatrix}$

- $Z_1 = diag\left(1, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, 1, ... 1\right)$: multiplying by Z_1 swaps 2nd & 3rd entries. So $Z_1 Y_1 \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} d_1 \\ a_3 \\ 0 \\ \vdots \\ a_n \end{pmatrix}$.

- $Y_2 = (Y_2', 1, 1, ... 1)$, where $Y_2' \begin{pmatrix} d_1 \\ a_3 \end{pmatrix} = \begin{pmatrix} d_2 \\ 0 \end{pmatrix}$. So $Y_2 Z_1 Y_1 \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} d_2 \\ 0 \\ 0 \\ \vdots \end{pmatrix}$

- Z_2 is permutation matrix permuting the 2nd & 4th entries.

Etc. By the construction, Y has required properties. Then $e_1', ..., e_n'$ is the columns of Y $\square$

6

BONUS: Finite dimensional modules over $\mathbb{C}[x,y]$.

Fix $n \in \mathbb{Z}_{>0}$. Our question: classify $\mathbb{C}[x,y]$-modules that have $\dim_{\mathbb{C}} = n$. In the language of Linear algebra: classify pairs of commuting matrices X, Y (up to simultaneous conjugation).

For n large enough, there's no reasonable solution. However, various geometric objects related to the problem are of great importance, and we'll discuss them below.

Set $C := \{(X,Y) \in Mat_n(\mathbb{C})^{\oplus 2} \mid XY = YX\}$. Consider the subset $C_{cycl} \subset C$ of all pairs for which there is a cyclic vector $v \in \mathbb{C}^n$ meaning that v is a generator of the corresponding $\mathbb{C}[x,y]$-module. The group $GL_n(\mathbb{C})$ acts on C by simultaneous conjugation: $g.(X,Y) = (gXg^{-1}, gYg^{-1})$

Exercise: C_{cycl} is stable under the action & all the stabilizers for the resulting $GL_n(\mathbb{C})$-action are trivial.

Premium exercise: the set of $GL_n(\mathbb{C})$-orbits in C_{cycl} is identified with the set of codim n ideals in $\mathbb{C}[x,y]$.

It turns out that this set of orbits, equivalently, the set of ideals has a structure of an algebraic variety. This variety is called the Hilbert scheme of n points in $\mathbb{C}^2$ and is denoted by $Hilb_n(\mathbb{C}^2)$. It is extremely nice & very important. For example, it is "smooth" meaning it has no singularities.

One can split $Hilb_n(\mathbb{C}^2)$ into the disjoint union of affine spaces (meaning $\mathbb{C}^?$). The affine spaces are labelled by the partitions of n ($\overset{\sim}{\longleftrightarrow}$ ideals in $\mathbb{C}[x,y]$ spanned by monomials) & for each partition we can compute the dimension – thus achieving some kind of classification of points.

One of the reasons why $Hilb_n(\mathbb{C}^2)$ is important is that it appears in various developments throughout Mathematics: Algebraic geometry (not surprising), Representation theory, Math Physics, and even Algebraic Combinatorics & Knot theory (!!)

The structure of the orbit space for the action of $GL_n(\mathbb{C})$ on C is FAR more complicated, yet the resulting geometric object is still important.