Lecture 7.

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

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

Ref: Dummit & Foote, Chapter 12.

1) Motivating question: for a field $\mathbb{F}$, we can completely classify finite dimensional $\mathbb{F}$-vector spaces: $\forall$ such V $\exists\, k\in\mathbb{Z}_{\geq 0}$ s.t. $V\simeq\mathbb{F}^{\oplus k}$; this k is uniquely recovered from V: $k=\dim V$. Can we generalize this to finitely gen'd modules over a ring?

A: Yes, but only in very rare - yet important - cases.

1.1) PID: definition & examples. : A is comm've unital ring.

Definition: · An ideal $I\subset A$ is principal if $I=(a)$ for some $a\in A$.

· Say A is PID if A is a domain & every ideal in A is principal.

Examples: · $\mathbb{Z}$, $\mathbb{F}[x]$ ($\mathbb{F}$ is field) are PID's & every Euclidian domain is a PID.

Non-examples: $\underset{(2,1+\sqrt{-5})}{\mathbb{Z}[\sqrt{-5}]}$, $\underset{(2,x)}{\mathbb{Z}[x]}$, $\underset{(x,y)}{\mathbb{F}[x,y]}$ are not PID: $(2,1+\sqrt{-5})\subset\mathbb{Z}[\sqrt{-5}]$, $(2,x)\subset\mathbb{Z}[x]$, $(x,y)\subset\mathbb{F}[x,y]$ - not principal.

1.2) Unique factorization: $a,b\in A$ (PID) $\rightsquigarrow$ ideal $(a,b)\subset A$

$\exists\, d\in A \mid (a,b)=(d)$

- d divides both a, b.
- every other common divisor of a, b divides d.

So $d = GCD(a,b)$, moreover $d = xa + yb$ for some $x, y \in A$.

Classical application: unique factorization holds for A.

Recall $p \in A$ is prime $\Leftrightarrow (p)$ is a prime ideal.

UF property: $\forall\, a \in A$ decomposes as a product of prime elements in an (essentially) unique way: 2 decompositions are obtained from one another by permuting factors & multiplying them by invertible elements.

Remark: • in a PID every prime ideal is maximal: if (p) is prime, then $(f) \supseteq (p) \Leftrightarrow f$ divides $p \Leftrightarrow (f) = (p)$ or $(f) = A$.

- PID is Noetherian.

2.1) Main theorem: A is PID.

Let M be a finitely generated A-module

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

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

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

Example: $A = \mathbb{Z}$, this 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 closed $\Rightarrow$ primes in $\mathbb{F}[x]$ are $x-\lambda$, $\lambda\in\mathbb{F}$, (up to invert. 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: A module $/\mathbb{F}[x]$ = $\mathbb{F}$-vector space & an operator X.

Choose an $\mathbb{F}$-basis in $\mathbb{F}[x]/\left((x-\lambda_i)^{d_i}\right)$:

$$1, (x-\lambda_i), (x-\lambda_i)^2, \dots, (x-\lambda_i)^{d_i-1}$$

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

So X acts as a Jordan block:

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

Main Thm in this case = 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": $\operatorname{diag}(J_{d_1}(\lambda_1),\dots,J_{d_\ell}(\lambda_\ell))$.

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

3) Proof of Main Thm, part 1) - existence.

Two parts:

Part 1: Prove that $M \simeq A^{\oplus k} \oplus \bigoplus_{i=1}^{m} A/(f_i)$, where $f_1,\dots,f_m \in A$, nonzero.

Part 2: Prove that for $f \in A \setminus \{0\}$, have
$$A/(f) \simeq \bigoplus_{i=1}^{s} A/(p_i^{d_i}),$$ where $p_1 \dots p_s$ are pairwise distinct primes & $f = p_1^{d_1} \cdots p_s^{d_s} \cdot$ (invertible).

Today: Part 1: M is fin. generated $\Rightarrow$ is a quotient of a free module $F \simeq A^{\oplus n}$ (for some n), so have epimorphism $\pi: F \twoheadrightarrow M$, $K := \ker \pi$

Since A is Noetherian $\Rightarrow$ K is finitely generated.

So can choose: • a basis $e_1,\dots,e_n$ in F

• a set of generators $y_1,\dots y_r \in K$.

The crucial claim: we can choose $e_1 \dots e_n$ & $y_1 \dots y_r$ in such a way that $\exists\, f_1,\dots f_m \mid r = m \leq n$ & $y_i = f_i e_i$.

Then $$M = F/K = \Big(\bigoplus_{i=1}^{n} Ae_i\Big) \Big/ \Big(\bigoplus_{i=1}^{m} Af_i e_i\Big) \simeq \bigoplus_{i=1}^{m} A/(f_i) \oplus A^{\oplus n-m}.$$
- precisely claim of Part 1.

Now we need to prove the crucial claim: reduce this to a question about matrices w. coeff's in A.
$$y_i = \sum_{j=1}^{n} y_{ij} e_j \rightsquigarrow Y = (y_{ij}) \in Mat_{r \times n}(A).$$

Q: How does changing $y_1 \dots y_r$ & $e_1 \dots e_n$ affect Y?

← by replacing w. non-degenerate linear combin'n replace $(y_1, \dots y_r)$ w. $(y_1, \dots y_r)R$, where $R \in Mat_{r \times r}(A)$ is invertible ($\Longleftrightarrow$ $\det(R) \in A$ is invertible)

Here $Y \rightsquigarrow RY$

Similarly, $(e_1, \dots e_n) \rightsquigarrow (e_1, \dots e_n)N$ ($N \in Mat_{n \times n}(A)$ invertible) gives $Y \rightsquigarrow YN$.

The crucial claim, matrix style:

$\forall\, Y \in Mat_{r \times n}(A)$ $\exists$ non-degenerate ($\Leftrightarrow$ invertible det) $R \in Mat_{r \times r}(A)$, $N \in Mat_{n \times n}(A)$ s.t. $RYN = \begin{pmatrix} f_1 & & & 0 \\ & \ddots & & \\ & & f_m & \\ 0 & & & 0 \end{pmatrix}$

$f_1, \dots f_m \in A$.

Proof of this:

Step 1: Spec. case $r=2$, $n=1$

Lemma: let $y_1, y_2 \in A$, $y := GCD(y_1, y_2)$. Then $\exists$ $R \in Mat_{2 \times 2}(A)$ $\det(R) = 1$ s.t.

$$R \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} y \\ 0 \end{pmatrix}.$$

Proof: Dividing y_1, y_2 by y, can assume $GCD(y_1, y_2) = 1$

$\Rightarrow$ $\exists$ $a, b \in A$ s.t. $\boxed{ay_1 + by_2 = 1}$ (use A is PID)

VIP (very important property)

$R := \begin{pmatrix} a & b \\ -y_2 & y_1 \end{pmatrix}$ $\quad R \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$! $\square$

Step 2: We use the following steps:

(i) Multiply Y w. $\underbrace{\begin{pmatrix} R' & & 0 \\ & 1 & \\ & & \ddots \\ 0 & & & 1 \end{pmatrix}}_{2}\}2$ to kill element in position $(2,1)$

(ii) permute rows #2 & #j $(j>2)$

By iterating these steps: arrive at

$$\begin{pmatrix} * & * \cdots & * \\ 0 & & \\ \vdots & * & \\ 0 & & \end{pmatrix}$$

Now multiply on the right by similar matrices & permute columns.

We arrive at $\begin{pmatrix} f_1 & 0 \cdots & 0 \\ 0 & & \\ \vdots & \underbrace{Y_1}_{n-1} & \\ 0 & & \end{pmatrix} \Big\} r-1$

Continue w. this Y_1 & arrive at $\begin{pmatrix} f_1 & & & 0 \\ & \ddots & & \\ & & f_e & \\ 0 & & & 0 \end{pmatrix}$.

Finishes Part 1. $\square$

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.