Lecture 7: modules over PID's, II

1) Proof of the main Thm.

Ref: [V], Sec 9.3. Dummit & Foote, Chapter 12.

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

1.0) Statement

Let A be PID. Let M be a fin. gen'd A-module. Our goal in this lecture is to prove:

Thm: 1) $\exists\ k \in \mathbb{Z}_{\geq 0}$, 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.

1.1) 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 prove:

Proposition 1: $\exists$ basis $e_1', \dots e_n'$ of $A^{\oplus n}$, integer $r \in \{0, \dots n\}$ and $f_1, \dots f_r \in A \setminus \{0\}$ s.t. $N = \mathrm{Span}_A(f_1 e_1', \dots f_r e_r')$.

After proving this, we will show that:

- $A^{\oplus n}/N \simeq A^{\oplus n-r} \oplus \bigoplus_{i=1}^{r} A/(f_i)$
- and if $f = p_1^{\alpha_1} \dots p_e^{\alpha_e} \in A$, where $p_1, \dots, p_e$ are primes w. $i \neq j \Rightarrow (p_i) \neq (p_j)$, then $A/(f) \simeq \bigoplus_{i=1}^{e} A/(p_i^{\alpha_i})$

These two claims combined with Prop 1 imply I) of Theorem.

We will deduce Proposition 1 from a statement about matrices with coefficients in A.

Definition: Let $n, m \in \mathbb{Z}_{>0}$ & $M_1, M_2 \in Mat_{n,m}(A)$. We say that M_1, M_2 are equivalent ($M_1 \sim M_2$) if $\exists$ invertible $B \in Mat_n(A)$, $C \in Mat_m(A)$ s.t. $M_2 = BM_1C$.

Note that B is invertible $\Leftrightarrow$ $\det B \in A$ is invertible – for the same reason as for fields.

We will give examples of equivalent matrices below. We'll deduce Proposition 1 from

Proposition 2: $\forall M \in Mat_{n,m}$ $\exists r \geq 0$ & $f_1, \dots f_r \in A \setminus \{0\}$ s.t.

$M \sim M' := \begin{pmatrix} f_1 & & & 0 \\ & f_2 & & \\ & & \ddots & \\ 0 & & & f_r \end{pmatrix}$ (w. f_i in entry (i,i) & all other entries equal 0)

1.2) From Proposition 2 to Proposition 1.

First we introduce some notation. We write a tuple of elements of $A^{\oplus n}$ as a vector: $\vec{u} = (u_1, \dots u_m)$. For $M \in Mat_{m \times k}(A)$, we have the k-tuple $\vec{u}M = (\sum_{i=1}^{m} m_{ij} u_i)_{j=1}^{k}$, ($M = (m_{ij})$), note that it consists of linear combinations of $u_1, u_2, \dots u_n$.

Second, observe that $A^{\oplus n}$ is a finitely generated, hence Noetherian, A-module (Corollary in Sec 3 of Lec 5). Therefore, N is finitely generated. Let $\vec{v}=(v_1,\dots v_m)$ be a tuple of generators of N.

Finally, let $\vec{e}=(e_1,\dots e_n)$ denote the standard basis of $A^{\oplus n}$. Form the matrix M with columns v_i so that $\vec{e}M=\vec{v}$. For this M we find non-degenerate matrices $B\in Mat_n(A)$, $C\in Mat_m(A)$ s.t. $M=BM'C$, where M' is as in Prop'n 2.

Set $\vec{e}'=(e_1',\dots,e_n'):=\vec{e}B$, $\vec{v}'=(v_1',\dots,v_m'):=\vec{v}C^{-1}$. Note that

- $\vec{e}BM'C=\vec{v}\Leftrightarrow\vec{e}'M'=\vec{v}'\Leftrightarrow v_i'=f_ie_i'$ for $i\le r$ & $v_i'=0$, else.
- since B is non-degenerate & $\vec{e}$ is a basis of $A^{\oplus n}$, $\vec{e}'$ is also a basis
- since C is non-degerate, $Span_A(\vec{v}')=Span_A(\vec{v})=N$.

Proposition 1 follows.

1.3) Proof of Proposition 2

We start by highlighting two important examples of equivalent matrices.

1) If M' is obtained by permuting rows & columns from M, then $M'\sim M$. Indeed, $M'=BMC$ for permutation matrices B,C & they are non-degenerate

2) Suppose $M=\begin{pmatrix}a\\b\end{pmatrix}$, a 2×1-matrix. Let $d:=GCD(a,b)$. We claim that $M\sim\begin{pmatrix}d\\0\end{pmatrix}$. Indeed, $d=xa+yb$ for some $x,y\in A$. We set $B:=\begin{pmatrix}x & y\\ -b/d & a/d\end{pmatrix}$. Since $\det B=x\frac{a}{d}+y\frac{b}{d}=\frac{d}{d}=1$, B is invertible

Similarly, $(a\ b)\sim(d\ 0)$.

Proof of Prop'n 2:

Step1: To $Y \in Mat_{n,m}(A) = (y_{ij})$ we assign the ideal $I_Y := (y_{11}) \subset A$. Consider the set of ideals I_Y for $Y \sim M$, where M is a given matrix. Since A is Noetherian, $\exists\, Y$ s.t. I_Y is maximal w.r.t. $\subseteq$ (Sec 1.2 in Lec 5). Let $d \in A$ be s.t. $I_Y = (d)$.

Step2: We claim that d divides y_{i1} $\forall\, i = 2, \dots n$. Assume the contrary. By permuting rows 2 & i, we can assume $i = 2$. Let $\underline{B} \in Mat_2(A)$ be s.t. $\underline{B}$ is nondegenerate & $\underline{B}\begin{pmatrix} d \\ y_{21} \end{pmatrix} = \begin{pmatrix} d' \\ 0 \end{pmatrix}$, where $d' = GCD(d, y_{21})$. Set B to be block diagonal matrix $diag(\underline{B}, 1, \dots 1)$, nondegenerate. Then $BY (\sim Y)$ has entry $(1,1)$ equal to d' & $(d') \not\supseteq (d)$, leading to a contradiction. Similarly, d divides y_{1j} $\forall\, j = 2, \dots, m$.

Step3: Now we are going to transform Y as follows: we make all entries $(i,1)$, $i > 1$, equal 0: we multiply Y by $\begin{pmatrix} 1 & & \\ -y_{21}/d & 1 & 0 \\ \vdots & & \ddots \\ -y_{n1}/d & 0 & 1 \end{pmatrix}$ from the left leading to an equivalent matrix

Then we multiply by $\begin{pmatrix} 1 & -y_{12}/d & \dots & -y_{1m}/d \\ & 1 & & 0 \\ 0 & & \ddots & \\ & & & 1 \end{pmatrix}$ from the right making entries $(1,j)$ equal 0 (and keeping entries $(i,1)$ equal 0) We arrive at an equivalent matrix of the form $\begin{pmatrix} d & 0 \dots & 0 \\ 0 & & \\ \vdots & M_1 & \\ 0 & & \end{pmatrix}$

w. $M_1 \in Mat_{n-1,m-1}(A)$. This allows us to finish the proof by doing induction on n. □

1.4) Finishing proof of existence

At this point we have a basis $e_1', \dots e_n'$ of $A^{\oplus n}$ & $f_1, \dots f_r \in A \setminus \{0\}$

s.t. $N = \mathrm{Span}(f_1 e_1', \dots, f_r e_r')$

Note that if L_1, L_2 are A-modules & $N_i \subset L_i$ are submodules then there is a natural isomorphism (exercise):

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

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

It remains to prove

Lemma: if $f = p_1^{d_1} \dots p_e^{d_e} \in A$, where $p_1, \dots, p_e$ are primes s.t. $i \neq j \Rightarrow (p_i) \neq (p_j)$, then

$$A/(f) \simeq \bigoplus_{i=1}^{e} A/(p_i^{d_i})$$

The main ingredient is a version of the Chinese remainder theorem:

Proposition 3: Let A be a comm've ring & I_1, I_2 be ideals s.t. $I_1 + I_2 = A$. Then the map $A/I_1 I_2 \xrightarrow{\varphi} A/I_1 \times A/I_2$, $a + I_1 I_2 \mapsto (a + I_1, a + I_2)$ is an A-module isomorphism.

Proof of Proposition: The map is A-linear so it's enough to construct an inverse. Pick $b_i \in I_i$ w. $b_1 + b_2 = 1$ & consider a map

$\varphi'\colon A/I_1 \times A/I_2 \to A/I_1 I_2$, $(a_1 + I_1, a_2 + I_2) \mapsto b_2 a_1 + b_1 a_2 + I_1 I_2$

It's well-defined b/c $b_1 I_2, b_2 I_1 \subset I_1 I_2$. And it's inverse to φ:

$\varphi' \circ \varphi (a + I_1 I_2) = \varphi'(a + I_1, a + I_2) = (b_1 + b_2) a + I_1 I_2 = a + I_1 I_2$.

$\varphi \circ \varphi' (a_1 + I_1, a_2 + I_2) = \varphi(b_2 a_1 + b_1 a_2 + I_1 I_2) = (b_2 a_1 + b_1 a_2 + I_1, b_2 a_1 + b_1 a_2 + I_2)$

$[= b_2 a_1 + b_1 a_2 - a_1 = \cancel{b_2 a_1} + b_1 a_2 - (b_1 + \cancel{b_2}) a_1 = (a_1 - a_2) b_1 \in I_1$ & similar for 2nd coordinate$] = (a_1 + I_1, a_2 + I_2)$ □

Proof of Lemma: Set $g_1 := p_1^{d_1}$, $g_2 := p_2^{d_2} \dots p_\ell^{d_\ell}$ so that $f = g_1 g_2$. Then set $I_1 = (g_1)$, $I_2 = (g_2)$. Observe that g_1, g_2 are coprime $\Leftrightarrow$ $GCD(g_1, g_2) = 1 \Leftrightarrow$ $I_1 + I_2 = A$. So $A/(f) \xrightarrow{\sim} A/(g_1) \times A/(g_2)$ by Proposition 3. We can then argue by induction on ℓ to decompose $A/(g_2)$ □

This finishes the proof of (1) of Thm.

Exercise: The isomorphism in Proposition 3 is that of rings.

1.5) Proof of uniqueness

We'll prove 2) of Thm by producing invariants of M & read κ & $(p_1^{d_1}), \dots, (p_\ell^{d_\ell})$ from these invariants.

Fix a prime ideal $(p) \subset A$ & $s \in \mathbb{Z}_{>0}$. Consider $p^s M = (p)^s M$, an A-submodule of M (a special case of taking products of ideal and submodule, Sec 2.2 in Lec 4.)

We have $p^{s+1}M \subset p^s M \rightsquigarrow$ quotient $p^s M / p^{s+1} M$. The ideal (p) annihilates the quotient, so it can be viewed as $A/(p)$-module (Sec 2.3 of Lec 4). Note that (p) is maximal ideal (same proof as for $A = \mathbb{Z}$, see Sec 2.2 in Lec 2) so $A/(p)$ is a field. Also $p^s M$ is fin. gen'd over $A \Rightarrow p^s M / p^{s+1} M$ is finitely generated over $A/(p)$, so

$$d_{p,s}(M) := \dim_{A/(p)} p^s M / p^{s+1} M < \infty.$$

Proposition: For $M \simeq A^{\oplus \kappa} \oplus \bigoplus_{i=1}^{\ell} A/(p_i^{d_i})$, we have

$$d_{p,s}(M) = \kappa + \#\{i \mid (p_i) = (p) \ \& \ d_i > s\}.$$

We'll prove this in the next lecture.

Once we know the numbers on the right, 2) of Thm is proved: the number of occurences of $A/(p^s)$ is $d_{p,s-1}(M) - d_{p,s}(M)$ and $\kappa = d_{p,s}(M)$ for all s s.t. $s > d_i$ $\forall i$

Example: $A = \mathbb{F}[x]$ ($\mathbb{F}$ is alg. closed field), M finite dim'l/$\mathbb{F}$ ($\Leftrightarrow \kappa = 0$), $p = x - \lambda$ ($\lambda \in \mathbb{F}$), X is the operator given by x.

$p^s M = \mathrm{Im}(X - \lambda I)^s \Rightarrow d_{p,s}(M) = \mathrm{rk}(X-\lambda I)^s - \mathrm{rk}(X-\lambda I)^{s+1}$.

From Proposition we deduce that matrices $X_1, X_2 \in \mathrm{Mat}_n(\mathbb{F})$ are conjugate $\Leftrightarrow \mathrm{rk}(X_1 - \lambda I)^s = \mathrm{rk}(X_2 - \lambda I)^s$ $\forall \lambda \in \mathbb{F}$, $s \in \mathbb{Z}_{>0}$.

(b/c conjugate matrices $\Leftrightarrow$ isomorphic $\mathbb{F}[x]$-modules).

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 ($\leftrightsquigarrow$ 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 $\mathbb{C}$ is FAR more complicated, yet the resulting geometric object is still important.