Lecture 8: modules over PID, II.

1) Continuation of proof from last lecture
2) Localization of rings.

See refs for Lec 7; + [AM], Intro to Sec 3.

1.1) Proof of existence.

Reminder: A is PID, M is a finitely generated A-module.

Thm (Sec 2, Lec 7) 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 & $(p_1^{d_1}),\dots,(p_\ell^{d_\ell})$ are uniquely determined by M.

In Sec 3.1, Lec 7, we have reduced 1) of the theorem to:

Claim: Let $N\subset A^{\oplus n}$ be A-submodule. Then $\exists$ basis $e_1',\dots,e_n'\in A^{\oplus n}$, $r\leqslant n$, $f_1,\dots f_r\in A\setminus\{0\}$ s.t. $N=\operatorname{Span}_A(f_1e_1',\dots f_re_r')$.

Pick $m\in A^{\oplus n}\setminus\{0\}$. We've defined $GCD(m)\in A\setminus\{0\}$ s.t. if $m=\sum_{i=1}^n b_ie_i'$ for a basis $e_1',\dots,e_n'$, then $GCD(m)=GCD(b_1,\dots b_n)$ (i.e $GCD(m)$ is independent of the choice of a basis). We've seen:

$\exists$ basis $e_1',\dots e_n'$ s.t. $m=de_1'$ w. $d=GCD(m)$.

This is Sec 3.2 of Lec 7.

Proof of Claim: We argue by induction on n: suppose we know the claim for submodules of $A^{\oplus n-1}$. Take $m \in N \setminus \{0\}$ s.t. $(GCD(m))$ is maximal among all $(GCD(m'))$, $m' \in N$, - it exists b/c A is Noetherian and hence every nonempty set of ideals contains a max'l element (Sec 1.2 of Lec 5).

Take a basis $e_1'', \ldots e_n'' \in A^{\oplus n}$ s.t. $m = de_1''$, $d = GCD(m)$. We claim that

(*) every element of N is of the form $\sum_{i=1}^n a_i e_i''$ w. $a_1 \vdots d$

Let $m' = \sum_{i=1}^n a_i e_i'' \in N$. Let $d_0 := GCD(d, a_1) \Rightarrow \exists\, x, y \in A$ w. $d_0 = xd + ya_1$. Consider $xm + ym' = d_0 e_1'' + \sum_{i=2}^n y a_i e_i'' \in N$. Then $GCD(xm+ym')$ $=$ [(ii) of Lemma in Sec 2.3] $= GCD(d_0, ya_2, \ldots ya_n)$ divides d_0. By the choice of m, $(d_0) = (d) \Rightarrow d_0 \vdots d$. So $a_1 \vdots d$ proving (*).

Set $N_0 := N \cap Span_A(e_2'', \ldots, e_n'')$. We claim that

(1) $$N = N_0 \oplus A de_1'', \text{ as submodules in } A^{\oplus n}$$

Indeed, $N_0 \cap A de_1'' = \{0\}$, and (*) implies $N = N_0 + A de_1''$.

Now apply inductive assumption to $N_0 \subset Span_A(e_2'', \ldots, e_n'') \simeq A^{\oplus n-1}$. We get a basis $e_2', \ldots, e_n' \in Span_A(e_2'', \ldots, e_n'')$ & $f_2, \ldots f_r$ w. $N_0 = Span_A(f_2 e_2', \ldots, f_r e_r')$. Then take $f_1 := d$, $e_1' := e_1''$. (1) implies the claim $\square$

1.2) Proof of part 2 of Thm: uniqueness.

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 $p^sM/p^{s+1}M$. The ideal (p) annihilates the quotient, so it can be viewed as $A/(p)$-module (Sec 2.3 of Lec 4). By Sec 1 of Lec 7, (p) is maximal ideal, so $A/(p)$ is a field. Also p^sM is fin. gen'd over $A \Rightarrow p^sM/p^{s+1}M$ is finitely generated, so

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

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

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

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 $k = d_{p,s}(M)$ for all s s.t. $s > d_i \ \forall i$

Proof of Prop'n:

Step 1: explain how $d_{p,s}$ behaves on direct sums:

Claim: $d_{p,s}(M_1 \oplus M_2) = d_{p,s}(M_1) + d_{p,s}(M_2)$.

Proof of the claim:

$$\begin{array}{ccc} p^s(M_1 \oplus M_2) & = & p^sM_1 \oplus p^sM_2 \\ \cup & & \cup \\ p^{s+1}(M_1 \oplus M_2) & = & p^{s+1}M_1 \oplus p^{s+1}M_2 \end{array}$$

(as submodules in $M_1 \oplus M_2$ w. $p^{s+1}M_i \subset p^sM_i$).

$\rightsquigarrow p^s(M_1 \oplus M_2)/p^{s+1}(M_1 \oplus M_2) \simeq p^sM_1/p^{s+1}M_1 \oplus p^sM_2/p^{s+1}M_2$ and the claim follows: the dimension of the direct sum of vector spaces is the sum of dimensions of summands

Step 2: Need to compute $d_{p,s}$ of possible summands of M:
A, $A/(p^t)$, $A/(q^t)$, $(q) \neq (p)$.

i) A:

$$\begin{array}{ccc} A & \xrightarrow{p^s} & p^s A \\ \cup & & \cup \\ (p) & \xrightarrow{\sim} & p^{s+1}A \end{array}$$ is a module isomorphism

$\rightsquigarrow p^sA/p^{s+1}A \xleftarrow[\sim]{p^s\cdot ?} A/(p)$ as vector spaces over the field $A/(p)$ $\Rightarrow d_{p,s}(A) = 1$.

ii) $A/(p^t) =: M'$; if $s \geq t \Rightarrow p^s M' = \{0\} \Rightarrow d_{p,s}(M') = 0$

if $s < t \Leftrightarrow (p^s) \supseteq (p^t)$ so

$p^sM'/p^{s+1}M' \simeq p^sA/p^{s+1}A$ as $A/(p)$-modules.

so $d_{p,s}(M') = 1$ by i)

iii) $M'' = A/(q^t)$ but q, p are coprime so $(q^t) + (p^?) = A$

$\Rightarrow p^sM'' = p^{s+1}M'' = M'' \Rightarrow p^sM''/p^{s+1}M'' = 0$

Summing the contributions from the summands together, we arrive at the claim of the theorem $\square$

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.

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

Corollary of Prop'n : Two matrices $X_1, X_2 \in Mat_n(\mathbb{F})$ are conjugate $\Leftrightarrow$ $rk(X_1-\lambda I)^s = rk(X_2-\lambda I)^s$ $\forall\, \lambda\in\mathbb{F},\ s\in\mathbb{Z}_{>0}$.
(b/c conjugate matrices $\Leftrightarrow$ isomorphic $\mathbb{F}[x]$-modules).

2) Localization

We've seen a bunch of constructions of rings:
- direct products
- rings of polynomials
- quotient rings
- completions (HW 1)

Now we discuss another construction w. rings – localization. It generalizes the construction of $\mathbb{Q}$ from $\mathbb{Z}$. The general construction takes a commutative ring A and a suitable subset of A.

Definition: A subset $S\subset A$ is multiplicative if
- $1\in S$
- $s,t\in S \Rightarrow st\in S$

Now we proceed to defining the localization $A[S^{-1}]$.

Consider $A\times S$ (product of sets), equip it w. equivalence relation $\sim$ defined by
$$(*)\ (a,s)\sim(b,t) \overset{def}{\Longleftrightarrow} \exists\, u\in S \mid uta=usb.$$

Exercise: Check that $\sim$ is indeed an equivalence relation.

Let $A[S^{-1}]$ be the set of equivalence classes. The class of (a, s) will be denoted by $\frac{a}{s}$.

Addition & multiplication in $A[S^{-1}]$ are introduced by:

$$\frac{a_1}{s_1} + \frac{a_2}{s_2} := \frac{s_2 a_1 + s_1 a_2}{s_1 s_2}, \quad \frac{a_1}{s_1} \frac{a_2}{s_2} := \frac{a_1 a_2}{s_1 s_2}$$

Proposition: These operations are well-defined (the result depends only on $\frac{a_1}{s_1}, \frac{a_2}{s_2}$, not on $(a_1, s_1), (a_2, s_2)$) & equip $A[S^{-1}]$ w. structure of a commutative ring (w. unit $\frac{1}{1}$). Moreover, $\iota: A \to A[S^{-1}], a \mapsto \frac{a}{1}$, is a ring homomorphism.

Proof: omitted in order not to make everybody very bored...

Def'n: The ring $A[S^{-1}]$ is called the localization of A (w.r.t. S).

Examples: 1) Let $A = \mathbb{Z}/6\mathbb{Z}$ & $S = \{1, 2, 4\}$. Every equivalence class in $A \times S$ contains a unique element of the form $(a, 2)$ w. $a = 0, 2, 4$. The homomorphism $\iota: A \to A[S^{-1}]$ is surjective (e.g. $1 \to \frac{2}{2}$) and the kernel is (3). So $A[S^{-1}] \simeq \mathbb{Z}/3\mathbb{Z}$. Details are exercise.

2) $S = \{$all invertible elements in $A\}$ is multiplicative. Every

equivalence class in $A \times S$ contains a unique element of the form $(a,1)$ and ι is a ring isomorphism. Details are also an exercise.

Exercise: $A[S^{-1}]$ is the zero ring $\Leftrightarrow 0 \in S$.