Lecture 8.

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

See refs for Lec 7 for 1); [AM], intro to Chapter 3 for 2)

1) Reminder: A is PID, M is fin. gen'd A-module

Thm (from 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 Lec 7, we've proved $M\simeq A^{\oplus k}\oplus\bigoplus_{i=1}^{m}A/(f_i)$ for $f_1,\dots f_m\in A\setminus\{0\}$.

1.1) Finishing part 1) of Thm.

Proposition: Let $f\in A\setminus\{0\}$, $f=\varepsilon p_1^{d_1}\dots p_r^{d_r}$, where ε is invertible, $(p_1),\dots(p_r)$ are pairwise distinct prime ($\Leftrightarrow$ maximal) ideals. Then $A/(f)\simeq\bigoplus_{i=1}^{r}A/(p_i^{d_i})$ (as A-modules).

Lemma: Let A be any (comm've & unital) ring, $I_1,I_2\subset A$ be ideals. If $I_1+I_2=A$, then have an isom'm

$$A/I_1I_2\xrightarrow{\sim}A/I_1\times A/I_2 \text{ (of rings - and of } A\text{-modules).}$$

Proof of Prop'n (modulo Lemma): induction on r w. $r=1$ - nothing to prove. For $r>1$, $I_1:=(p_1^{d_1})$, $I_2:=(p_2^{d_2}\dots p_r^{d_r})$. Elements

1] $p_1^{d_1}, p_2^{d_2}\dots p_r^{d_r}$ are coprime $\Rightarrow$ their GCD $=1\Rightarrow$ [A is PID]

$I_1+I_2=A$. Apply the lemma: $A/(f)=A/I_1I_2 \xrightarrow{\sim} A/I_1 \oplus A/I_2$.
Done by induction $\square$

Proof of lemma: $I_1+I_2=A \Rightarrow \exists\, a_i \in I \mid a_1+a_2=1$

Step 1: To construct a homom'm: $A/I_1I_2 \longrightarrow A/I_1 \times A/I_2$

$\pi_i: A/I_1I_2 \longrightarrow A/I_i$ $(i=1,2)$, $a+I_1I_2 \longmapsto a+I_i$ - makes sense b/c $I_1I_2 \subset I_i$

$\pi: A/I \longrightarrow A/I_1 \times A/I_2$, $\pi=(\pi_1,\pi_2)$ - homomorphism of unital rings (& of A-modules).

Step 2: π is injective: $\ker\pi = \ker\pi_1 \cap \ker\pi_2$

$\ker\pi_i = I_i/I_1I_2$ $(i=1,2)$. So what we have to prove: $I_1I_2 = I_1 \cap I_2$.

$a \in I_1 \cap I_2 \rightsquigarrow a=[a_1+a_2=1]=a(a_1+a_2)=aa_1+aa_2 \in I_1I_2$

$\in I_1\cap I_2 \subset I_2$ $\quad \in I_1$ $\quad \in I_1I_2$

which proves $I_1I_2=I_1\cap I_2$.

Step 3: prove π is surjective: i.e. $\forall\, b_1,b_2\in A\ \exists\, b\in A$ s.t. $\pi(b+I_1I_2)=(b_1+I_1,\ b_2+I_2) \Longleftrightarrow b-b_i\in I_i$ for $i=1,2$

$b:=a_2b_1+a_1b_2$

$b-b_1=(a_2-1)b_1+a_1b_2=[a_1+a_2=1\Rightarrow a_2-1=-a_1]=-a_1b_1+a_1b_2\in I_1$

b/c $a_1 \in I_1$ $\square$

Rem: a special $k=2$ case of a more gen'l claim:

$I_1,\dots I_k$ w. $I_i+I_j=A$ for $i\neq j \Rightarrow A/I_1\cdots I_k \xrightarrow{\sim} \prod_{i=1}^{k}(A/I_i)$

(Chinese remainder thm)

1.2) Proof of part 2 of Thm.

Fix a prime $p \in A$ (rather fix (p)), $s \geqslant 0$

Consider $\underset{\cup}{p^s M} = (p)^s M$ is an A-submodule of M.

$p^{s+1}M \rightsquigarrow p^sM/p^{s+1}M$ is an A-module killed

by (p). Therefore $p^sM/p^{s+1}M$ is an $\underbrace{A/(p)}_{\text{field}}$-module b/c (p) is max'l

M is fin. gen'd $\Rightarrow p^sM$ is fin. gen'd hence

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

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

Once we know the numbers on the right, 2) is proved: e.g. the number of occurences of $A/(p^s)$ is $d_{p,s-1}(M) - d_{p,s}(M)$.

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:

$\underset{\cup}{p^s(M_1 \oplus M_2)} = p^sM_1 \oplus \underset{\cup}{p^sM_2}$ (as submodules in $M_1 \oplus M_2$)

$p^{s+1}(M_1 \oplus M_2) = p^{s+1}M_1 \oplus p^{s+1}M_2$

$\rightsquigarrow p^s(M_1 \oplus M_2)/p^{s+1}(M_1 \oplus M_2) \simeq p^sM_1/p^{s+1}M_1 \oplus p^sM_2/p^{s+1}M_2$

and the claim follows.

Step 2: Need to compute $d_{p,s}$ of:

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 $\rightsquigarrow$ $p^sA/p^{s+1}A \xrightarrow{\sim} A/(p)$ 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 $d_{p,s}(M') = 1$

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/$\mathbb{F}$ ($\Leftrightarrow k=0$), $p = x - \lambda$ ($\lambda \in \mathbb{F}$), 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 part 2): Two matrices $X_1, X_2 \in \operatorname{Mat}_n(\mathbb{F})$ are similar $\Leftrightarrow \operatorname{rk}(X_1 - \lambda I)^s = \operatorname{rk}(X_2 - \lambda I)^s \ \forall \lambda \in \mathbb{F}, s \in \mathbb{Z}_{>0}$.

(similar matrices $\Leftrightarrow$ isomorphic $\mathbb{F}[x]$-modules).

2) Localization of rings.

So far we've learned three constructions with rings:

- rings of polynomials } Lec 1
- quotient rings }
- completions - HW 1.

Localization is another such construction: starts w. (comm've & unital) A & a subset $S\subset A$ satisfying certain conditions.

Definition: $S\subset A$ is <u>localizable</u> if the term we'll use, it's not standard.

- $1\in S$
- $0\notin S$
- $s,t\in S \Rightarrow st\in S$

We'll give examples in the next lecture.

The localization, A_S, will consist of fractions $\frac{a}{s}$ w. $a\in A$, $s\in S$. Here's a formal def'n of A_S as a <u>set</u>.

Definition: • Consider $A\times S$ (product of sets), equip it w. equivalence relation $\sim$ defined by

$$(*)\ (a,s)\sim(b,t) \overset{def}{\Longleftrightarrow} \exists\, u\in S \mid uta=usb.$$

- A_S is the set of equivalence classes.
- the class of (a,s) will be denoted by $\frac{a}{s}$.

Rem: if S contains no zero divisors, then $(*)$ simplifies:

$ta = sb$. But, in general, the latter equality fails to give an equivalence relation.

Addition & multiplication in A_S 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 w. structure of comm've unital ring (w. unit $\frac{1}{1}$).

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