# Lecture 8.

## Continuation of proof from last lecture

See refs for Lec 7

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

Thm (from Lec 7) 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) $k$ & $(p_1^{d_1}), \dots, (p_\ell^{d_\ell})$ 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 $f \in A \setminus \{0\}$, $f = \varepsilon p_1^{d_1} \cdots p_r^{d_r}$, where $\varepsilon$ 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

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

Proof of Prop'n (modulo Lemma): induction on $r$ w. $r=1$ – nothing to prove. For $r>1$, $I_1 := (p_1^{\alpha_1})$, $I_2 := (p_2^{\alpha_2}\cdots p_r^{\alpha_r})$. Elements $p_1^{\alpha_1}, p_2^{\alpha_2}, \dots, p_r^{\alpha_r}$ are coprime $\Rightarrow$ their GCD $= 1 \Rightarrow$ [$A$ is PID] $I_1 + I_2 = A$. Apply the lemma: $A/(f) = A/I_1 I_2 \xrightarrow{\sim} A/I_1 \oplus A/I_2$. By induction on $r$, have $A/I_2 \xrightarrow{\sim} A/(p_2^{\alpha_2}) \oplus \dots \oplus A/(p_r^{\alpha_r})$, which finishes the proof. □

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

Step 1: We construct a homomorphism $A/I_1 I_2 \longrightarrow A/I_1 \times A/I_2$: $\pi_i : A/I_1 I_2 \longrightarrow A/I_i$ $(i=1,2)$, $a + I_1 I_2 \longmapsto a + I_i$ – makes sense b/c $I_1 I_2 \subset I_i$. Then we define $\pi : A/I \longrightarrow A/I_1 \times A/I_2$, $\pi := (\pi_1, \pi_2)$ – homomorphism of both rings and of $A$-modules.

Step 2: $\pi$ is injective: $\ker \pi = \ker \pi_1 \cap \ker \pi_2$. Have $\ker \pi_i = I_i / I_1 I_2$ $(i=1,2)$. So $\ker \pi_1 \cap \ker \pi_2 = (I_1 \cap I_2)/I_1 I_2$. So what we need to prove is $I_1 I_2 = I_1 \cap I_2$:

$a \in I_1 \cap I_2 \rightsquigarrow a = [a_1 + a_2 = 1] = a(a_1 + a_2) = aa_1 + aa_2$. Since $a \in I_2$, $a_1 \in I_1$, have $aa_1 \in I_1 I_2$. Similarly, $aa_2 \in I_1 I_2$ (use $a \in I_1$). So we have $a \in I_1 I_2$ which proves $I_1 I_2 = I_1 \cap I_2$.

Step 3: prove $\pi$ is surjective: i.e. $\forall\, b_1, b_2 \in A\ \exists\, b \in A$ s.t. $\pi(b + I_1 I_2) = (b_1 + I_1, b_2 + I_2) \Leftrightarrow b - b_i \in I_i$ for $i = 1,2$. We check that $b := a_2 b_1 + a_1 b_2$ works. E.g. for $i=1$ we have $b - b_1 = (a_2 - 1)b_1 + a_1 b_2 = [a_1 + a_2 = 1 \Rightarrow a_2 - 1 = -a_1] = -a_1 b_1 + a_1 b_2 \in I_1$ b/c $a_1 \in I_1$ □

Rem: The lemma is a special $k=2$ case of a more gen'l claim: $I_1, \dots I_k$ w. $I_i + I_j = A$ for $i \neq j \Rightarrow A/I_1 \dots I_k \xrightarrow{\sim} \prod_{i=1}^{k} (A/I_i)$ (Chinese remainder thm).

## 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 $M$. It has a submodule $(p)^{s+1} M$ so can consider the quotient module $p^s M / p^{s+1} M$. Note that $(p)^{s+1} M = (p)(p)^s M$ so $p^s M / p^{s+1} M$ is annihilated by $(p)$ and hence can be viewed as a module over $A/(p)$. As we've remarked in Sec 1.2 of Lec 7, $(p)$ is a maximal ideal in $A$. Hence $A/(p)$ is a field. Since $M$ is finitely generated, so are $p^s M$ & $p^s M / p^{s+1} M$. Therefore the latter is a finite dimensional vector space over $A/(p)$.

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

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

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: 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 $s$ sufficiently large.

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:

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

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

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

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) $A$:

$$\begin{array}{ccc} A & \xrightarrow{p^s} & p^s A \\ \cup & & \cup \\ (p) & \xrightarrow{\sim} & p^{s+1} A \end{array} \rightsquigarrow p^s A / p^{s+1} A \xrightarrow{\sim} A/(p) \text{ as vector spaces}$$

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

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

So $d_{p,s}(M') = 1$

iii) $M'' := A/(q^t)$ but $q, p$ are coprime so $(q^t)+(p^?) = A$
$\Rightarrow p^s M'' = p^{s+1} M'' = M'' \Rightarrow p^s M''/p^{s+1}M'' = 0$

Summing the contributions from the summands together, we arrive at the claim of the theorem □

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

Corollary of part 2): Two matrices $X_1, X_2 \in \mathrm{Mat}_n(\mathbb{F})$ are similar $\Leftrightarrow \mathrm{rk}(X_1-\lambda I)^s = \mathrm{rk}(X_2-\lambda I)^s \ \forall \lambda \in \mathbb{F}, s \in \mathbb{Z}_{>0}$.
(similar matrices $\Leftrightarrow$ isomorphic $\mathbb{F}[x]$-modules).

2) Up next: We've seen a bunch of constr'ns of rings:
- direct products
- rings of polynomials
- quotient rings
- completions (HW 1)

In the next couple of weeks or so we'll cover two more constructions:

· Integral extensions/closures of rings. This generalizes algebraic extensions & closures from field theory and

is motivated by Algebraic Number theory: the rings of algebraic integers are obtained as integral closures (of $\mathbb{Z}$ in finite field extensions of $\mathbb{Q}$).

- Localizations of rings (and modules)

To prepare for our discussion of integral extensions of rings recall that if $K \subset L$ are two fields, then one can talk about:

(1) $L$ being finitely generated (as a field) over $K$.

(2) $L$ being algebraic over $K$.

(3) $L$ being finite over $K$ ($\Leftrightarrow \dim_K L < \infty$)

Now let $A$ be a commutative ring and $B$ be a commutative $A$-algebra (note that we do not require that the corresponding homomorphism $A \to B$ is injective. In Lecture 5 we have defined what it means that $B$ is a finitely generated as an $A$-algebra. This is an analog of (1). An analog of (3) is as follows:

**Definition:** We say that $B$ is *finite* over $A$ if it is a finitely generated $A$-module.

An analog of being algebraic – $B$ is integral over $A$ – will be defined in the next lecture.