Lecture 3.

1) Prime ideals.

2) Modules & homomorphisms.

References: [AM], Chapter 1, Section 4; Chapter 2, Sections 1,4.

1) A is comm've unital ring.

Definitions: • $a\in A$ is a zero divisor if $a\neq 0$ & $\exists\, b\in A, b\neq 0, ab=0$.

• A is domain if A has no zero divisors.

• Ideal $\mathfrak{p}\subset A$ is prime if $\mathfrak{p}\neq A$ & $A/\mathfrak{p}$ is domain.

Exercise: TFAE:

i) $\mathfrak{p}$ is prime   remark: $\Leftarrow$ is automatic

ii) If $a,b\in A$ are s.t. $ab\in\mathfrak{p}\Rightarrow a\in\mathfrak{p}$ or $b\in\mathfrak{p}$.

iii) If $I,J\subset A$ are ideals, $IJ\subseteq\mathfrak{p}\Rightarrow I\subseteq\mathfrak{p}$ or $J\subseteq\mathfrak{p}$.

Examples: • maximal $\Rightarrow$ prime (b/c field $\Rightarrow$ domain).

• $\{0\}\subset A$ is prime $\Leftrightarrow$ A is domain.

• $A=\mathbb{Z}$. Every ideal is (n) for $n\in\mathbb{Z}$; (n) is prime $\Leftrightarrow$ n is prime or $n=0$. So every prime is max'l or $\{0\}$.

• Same conclusion for $A=\mathbb{F}[x]$ if $\mathbb{F}$ is field.

• $A=\mathbb{F}[x,y]$, (x) is prime (but not maximal): $\mathbb{F}[x,y]/(x)\xrightarrow{\sim}\mathbb{F}[y]$ (domain but not field).

Remark: Let A is domain, $\mathfrak{p}=(p)$; $\mathfrak{p}$ is prime $\Leftrightarrow$ if $a,b\in A$ w. $ab\,\vdots\, p$, then $a\,\vdots\, p$ or $b\,\vdots\, p$, such p are called prime.

2.1) Definitions (of modules & homomorphisms). A comm've unital ring.

1) By an A-module we mean abelian group M w. map $A \times M \rightsquigarrow M$ (multiplication or action map) s.t.

$\begin{cases} \cdot \text{ Associativity}: (ab)m = a(bm) \in M \\ \cdot \text{ Distibutivity}: (a+b)m = am+bm,\ a(m+m') = am+am' \in M \\ \cdot \text{ Unit}: 1m = m \in M \end{cases}$

$\forall\, a, b \in A,\ m, m' \in M$.

2) Let M, N be A-modules. A homomorphism (a.k.a A-linear map) is abelian group homomorphism $\varphi: M \to N$ s.t. $\varphi(am) = a\varphi(m)$ $\forall\, a \in A,\ m \in M$.

Ex 0: If A is a field, then A-module = vector space over A, homomorphism = linear map.

Observation: Let $\varphi: A \to B$ be a ring homomorphism.

I) If M is a B-module, then we can view M as A-module w. $A \times M \to M$ given by $(a, m) \mapsto \varphi(a)m$. Every B-linear map $M \to N$ is also A-linear.

II) If $\varphi: A \twoheadrightarrow B$ (surjective), then a B-module = A-module, where $\ker\varphi$ acts by 0 ($am = 0\ \forall\, m \in M, a \in \ker\varphi$). An A-linear map between B-modules M & N is also B-linear.

2.2) Examples.

1) $A = \mathbb{Z}$. Then $A \times M \to M$ can be recovered from $+$ in M. So $\mathbb{Z}$-module = abelian group.

2) Modules vs linear algebra

i) $A = \mathbb{F}[x]$ ($\mathbb{F}$ is field)

By Observation I applied to $\mathbb{F} \to \mathbb{F}[x]$, every $\mathbb{F}[x]$-module is $\mathbb{F}$-module = vector space; $xm = Xm$ for an $\mathbb{F}$-linear operator $M \to M$; can recover $\mathbb{F}[x]$-module str're from

$$f(x)m = [f(X): M \to M] = f(X)m.$$

So $\mathbb{F}[x]$-module = $\mathbb{F}$-vector space w. a linear operator. An $\mathbb{F}[x]$-module homomorphism $\varphi: M \to N$ is the same thing as a linear map $\varphi: M \to N$ s.t. $X_N \circ \varphi = \varphi \circ X_M$, where $X_M: M \to M$, $X_N: N \to N$ are operators coming from x.

ii) $A = \mathbb{F}[x_1, \dots x_n]$. An A-module = vector space w. n operators $X_1, \dots X_n$ (coming from $x_1, \dots x_n$) s.t. $X_i X_j = X_j X_i$ $\forall i, j$.

iii) $A = \mathbb{F}[x_1, \dots x_n]/(G_1, \dots, G_k)$, $G_i \in \mathbb{F}[x_1, \dots x_n]$. Use of Observation II w. $\mathbb{F}[x_1, \dots x_n] \overset{\varphi}{\twoheadrightarrow} A$ shows that A-module $= \mathbb{F}[x_1, \dots x_n]$-module where $\ker\varphi$ acts by 0. = $\mathbb{F}$-vector space w. n commuting operators $X_1, \dots X_n$ s.t. $G_i(X_1, \dots X_n) = 0$ as operators $M \to M$ $\forall i = 1, \dots k$.

3) Any ring A is a module over itself (via multiplication $A \times A \to A$).

For a ring homom. $\varphi: A \to B$, B becomes an A-module. So A-algebra is an A-module. Conversely, let M be A-module. How to describe an (assoc've, unital) algebra str're on M: this is a map $M \times M \to M$ s.t.

• associative & has unit (M is a unital ring)
• $M\times M \to M$ is A-bilinear (A-linear in each argument: $m\cdot am' = a(m\cdot m')$, $m\cdot(m_1'+m_2') = m\cdot m_1' + m\cdot m_2'$
$am\cdot m' = a(m\cdot m')$, $(m_1+m_2)\cdot m' = m_1\cdot m' + m_2\cdot m'$.

So algebra str're is a module str're + A-bilinear product (usual definition of an algebra).

Once M is an A-algebra with this definition, we get a ring homomorphism $A\to M: a\mapsto a1$ (1 unit in M).

2.3) Constructions with modules (& homomorphisms).

I) Direct sums & products.

M_1, M_2 A-modules $\rightsquigarrow$

$M_1\oplus M_2$ (direct sum) $= M_1\times M_2$ (direct product) = product $M_1\times M_2$ as abelian groups w. $a(m_1,m_2) := (am_1, am_2)$.

More generally, for a set I (possibly infinite) & M_i, $i\in I$ define: direct product $\prod_{i\in I} M_i = \{(m_i)_{i\in I} \mid m_i\in M_i\}$ w. componentwise operations.

Direct sum: $\bigoplus_{i\in I} M_i = \{(m_i)_{i\in I} \mid \text{only fin. many } m_i\neq 0\}$

Have A-module inclusion:

$$\bigoplus_{i\in I} M_i \hookrightarrow \prod_{i\in I} M_i$$

which is an isomorphism $\Leftrightarrow$ I is finite.

II) Hom module: let M,N be A-modules $\rightsquigarrow \mathrm{Hom}_A(M,N)$:= the set of all A-module homomorphisms. It has a natural A-module str're. Need to define addition & multipl'n by elements of A.

$\psi, \psi' \in Hom_A(M,N)$, $a \in A$

$[\psi+\psi'](m) := \psi(m)+\psi'(m) \in N$

$[a\psi](m) := a\psi(m) \quad \in N$

Lemma: 1) $\psi+\psi'$, $a\psi$ are A-linear maps.

2) The operations $+, \cdot$ turn $Hom_A(M,N)$ into A-module.

Partial proof: $[a\psi](bm) = b[a\psi](m)$.

$[a\psi](bm) = a(\psi(bm)) = ab\,\psi(m) = [ab=ba] = b(a\psi(m)) = b[a\psi](m)$.

Rest of proof is an exercise $\square$

Example: $M = A^{\oplus k}$. Claim: have natural isomorphism

$$Hom_A(A^{\oplus k}, N) \xrightarrow{\sim} N^{\times k}.$$

• Want a map $\iota: Hom_A(A^{\oplus k}, N) \longrightarrow N^{\times k}$: $e_i = (0,..1,..0) \in A^{\oplus k}$ ith coord. vector, $i=1,..k$, so $(a_1,...a_k) = \sum_{i=1}^{k} a_i e_i$.

$\iota(\psi) := (\psi(e_1), \psi(e_2), ..., \psi(e_k)) \in N^{\times k}$.

• $N^{\times k} \longrightarrow Hom_A(A^{\oplus k}, N)$ $\quad \psi_{\underline{n}}(a_1,...a_k) := \sum_{i=1}^{k} a_i n_i$

$\underline{n} = (n_1, ... n_k) \longmapsto \psi_{\underline{n}}$

Exercise: Verify $\psi_{\underline{n}}$ is a module homomorphism $A^{\oplus k} \to N$ & that ι & $[\underline{n} \mapsto \psi_{\underline{n}}]$ are indeed mutually inverse A-module homomorphisms between $Hom_A(A^{\oplus k}, N)$ & $N^{\times k}$.

BONUS: Noncommutative counterparts, part 3.

B1) Prime & completely prime ideals: For a comm've ring A

& an ideal $\mathfrak{p} \subset A$ we have two equivalent conditions:

- For $a, b \in \mathfrak{p}$: $ab \in \mathfrak{p} \Rightarrow a \in \mathfrak{p}$ or $b \in \mathfrak{p}$
- For ideals $I, J \subset A$: $IJ \subset \mathfrak{p} \Rightarrow I \subset \mathfrak{p}$ or $J \subset \mathfrak{p}$.

For noncommutative A and a two-sided ideal $\mathfrak{p}$, these conditions are no longer equivalent.

Definition: Let A be a ring and $\mathfrak{p} \subset A$ be a two-sided ideal.

- We say $\mathfrak{p}$ is <u>prime</u> if for two-sided ideals $I, J \subset \mathfrak{p}$, have $IJ \subset \mathfrak{p} \Rightarrow I \subset \mathfrak{p}$ or $J \subset \mathfrak{p}$.
- We say $\mathfrak{p}$ is <u>completely prime</u> if for $a, b \in A$, have $ab \in \mathfrak{p} \Rightarrow a \in \mathfrak{p}, b \in \mathfrak{p}$.

completely prime $\Rightarrow$ prime but not vice versa.

Exercise: 1) $\{0\} \subset \mathrm{Mat}_n(\mathbb{F})$ is prime but not completely prime (if $n > 1$).

2) $\{0\} \subset \mathrm{Weyl}_1 \, (= \mathbb{F}\langle x, y\rangle / (yx - xy - 1))$ is completely prime.

B2) Modules over noncommutative rings. Here we have left & right modules & also bimodules. Let A be a ring.

Definition: • A <u>left A-module</u> M is an abelian group w. multiplication map $A \times M \to M$ subject to the same axioms as in the commutative case.

• A <u>right A-module</u> is a similar thing but with multiplication map $M \times A \to M$ subject to associativity ($(ma)b = m(ab)$), distributivity & unit axioms.

• An A-bimodule is an abelian group M equipped

w. left & right A-module structures s.t. we have another associativity axiom: $(am)b = a(mb)$ $\forall\, a, b \in A$.

When A is commutative, there's no difference between left & right modules and any such module is also a bimodule. Note also that for two a priori different rings A, B we can talk about A-B-bimodules

Example: 1) A is an A-bimodule.

2) $\mathbb{F}^n$ (the space of columns) is a left $\mathrm{Mat}_n(\mathbb{F})$-module, while its dual $(\mathbb{F}^n)^*$ (the space of rows) is a right $\mathrm{Mat}_n(\mathbb{F})$-module. None of these has a bimodule structure.

Exercise: Construct a left Weyl_1-module structure on $\mathbb{F}[x]$ (hint: y acts as $\frac{d}{dx}$).

Remark: let M, N be left A-modules. In general, $\mathrm{Hom}_A(M,N)$ is not an A-module, it's just an abelian group. If M is an A-B-bimodule, then $\mathrm{Hom}_A(M,N)$ gets a natural left B-module structure (exercise: how?). Similarly, if N is an A-C-bimodule, then $\mathrm{Hom}_A(M,N)$ is a right C-module. And if M is an A-B-bimodule, and N is an A-C-bimodule, then $\mathrm{Hom}_A(M,N)$ is a B-C-bimodule.