Lecture 3. Rings, ideals & modules III.

1) Prime ideals, continued

2) Modules & homomorphisms.

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

BONUS: Non-commutative counterparts, 3.

1) Prime ideals, continued

Here's a motivation to care about prime ideals from Number theory. Let A be a domain.

Def: • an element $a\in A$ is called *irreducible* if it's not invertible and $a=a_1a_2 \Rightarrow$ one of a_i is invertible.

• $p\in A$ is called *prime* if (p) is prime, i.e. $ab \vdots p \Rightarrow a \vdots p$ or $b\vdots p$.

Exercise: $(a)=(b) \Leftrightarrow \exists$ invertible $\varepsilon\in A$ s.t. $b=\varepsilon a$.

• prime $\Rightarrow$ irreducible

• TFAE: (i) $\forall$ irreducible element is prime

(ii) A is a UFD (unique factorization domain), i.e $\forall a\in A$ $\exists$ irreducible elements $a_1,\dots a_k$ w. $a=a_1\dots a_k$ <u>unique</u> up to permutation & multiplication by invertible el'ts.

Examples (of UFD): $\mathbb{Z}[x_1,\dots x_n]$, $\mathbb{F}[x_1,\dots x_n]$ ($\mathbb{F}$ is field), $\mathbb{Z}[\sqrt{-1}]$.
Non-example: $\mathbb{Z}[\sqrt{-5}]$: $2, 3, 1\pm\sqrt{-5}$ are irreducible with

$$2\cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5}).$$

An especially important case for Number theory is when A is a "ring of algebraic integers" (to be defined later in the course). Examples of such include $\mathbb{Z}[\sqrt{d}]$ ($d \equiv 2$ or $3 \bmod 4$) where d is square free (case $d\equiv 1 \bmod 4$ requires a modification to be explained later)

A very important observation, due to Dedekind, is that while the unique factorization in a ring of algebraic integers (and somewhat more general rings now called Dedekind domains) may fail on the level of elements, it always holds on the level of ideals: every nonzero ideal uniquely decomposes as the product of nonzero prime ($\Leftrightarrow$, for these rings, maximal) ideals. So the failure of being UFD is the failure of ideals to be principal.

2) Modules & homomorphisms.

2.1) Definitions (of modules & homomorphisms)

A is a commutative ring.

Definitions:

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

following axioms hold:

$$\left.\begin{array}{lll} \cdot\ \text{Associativity} & : & (ab)m = a(bm) \in M \\ \cdot\ \text{Distibutivity} & : & (a+b)m = am+bm, \\ & & a(m+m') = am+am' \in M \\ \cdot\ \text{Unit} & : & 1m = m \in M \end{array}\right\} \forall\, a,b \in A,\ m,m' \in M.$$

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.

$$\forall\, a \in A,\ m \in M \Rightarrow \varphi(am) = a\varphi(m).$$

2.2) Examples.

0) $A = \mathbb{Z}$. Then $A \times M \to M$ can be recovered from $+$ in M, thx to unit & distributivity. So $\mathbb{Z}$-module = abelian group. And a $\mathbb{Z}$-module homomorphism is the same thing as group homomorphism.

1) If A is a field, then A-module = vector space over A, and homomorphism = linear map.

For the next examples & also below, we will need:

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 $B=A/I$ & φ is proj'n $\pi: A\twoheadrightarrow A/I$ then a B-module $=$ A-module, where I acts by 0 ($am=0\ \forall m\in M, a\in I$).
Let M,N be B-modules; $\psi: M\to N$ is A-linear ($\Leftrightarrow \psi(\pi(a)m)=$
$=\pi(a)\psi(m)\ \forall a\in A, m\in M \Leftrightarrow \psi(bm)=b\psi(m)\ \forall b\in B, m\in M) \Leftrightarrow$ B-linear.

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 $X: M\to M$; from X we can recover $\mathbb{F}[x]$-module str're

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

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. $X_iX_j=X_jX_i\ \forall i,j$.

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. $\mathbb{F}[x_1,\dots x_n]\overset{\pi}{\twoheadrightarrow} A$ shows that A-module

$= \mathbb{F}[x_1, .. x_n]$-module s.t. $(G_1, .. G_k)$ acts by 0 = $\mathbb{F}$-vector space w. n commuting operators $X_1, .. X_n$ s.t. $G_i(X_1, .. X_n) = 0$ as operators $M \to M$ $\forall i = 1..k$.

3) Any ring B is a module over itself (via multiplication $B \times B \to B$). This is often called the regular module.

2.3) A-algebras.

Definition: • Let L, M, N be A-modules. A map $\beta: L \times M \to N$ is called A-bilinear if it's A-linear in both arguments:
$\beta(l + l', m) = \beta(l, m) + \beta(l', m)$, $\beta(al, m) = a\beta(l, m)$ $\forall l, l' \in L, a \in A, m \in M$.
& similarly in the m-argument

• Let A be a commutative ring. By an A-algebra we mean an A-module B w. A-bilinear map $B \times B \to B$ that is a ring multiplication (in particular, B is a ring).

Note that we have $1_B \in B$ & $\varphi: A \to B$, $\varphi(a) := a 1_B$ is ring homomorphism. Conversely, if B is commutative & $\varphi: A \to B$ is a ring homomorphism, then (by Ex 3 & Observation I), B is A-module & mult'n $B \times B \to B$ is A-bilinear. So B is an A-algebra. Details are an exercise.

Usually, when B is obtained from A using some construction, it becomes an A-algebra. E.g A/I & $A[x_1, \dots x_n]$ are A-algebras.

2.4) Constructions with modules: 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) & modules $M_i, i \in I$, 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 $\Leftrightarrow$ $M_i \neq \{0\}$ only for finitely many i.

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 **prime** 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 **completely prime** if for $a, b \in A$, have $ab \in \mathfrak{p} \Rightarrow a \in \mathfrak{p}, b \in \mathfrak{p}$.

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

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

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

B2) Modules over noncommutative rings.

Here we have left & right modules & also bimodules. Let A be a ring.

Definition:
- A **left A-module** M is an abelian group w. multiplication map $A \times M \to M$ subject to the same axioms as in the commutative case.
- A **right A-module** 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 $Mat_n(\mathbb{F})$-module, while its dual $(\mathbb{F}^n)^*$ (the space of rows) is a right $Mat_n(\mathbb{F})$-module. None of these has a bimodule structure.

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