Lecture 3.

1) Prime ideals.

2) Modules & homomorphisms.

References: [AM], Chapter 1, Section 4; Chapter 2, Sections 14.

1) \( A \) is commutative unital ring.

Definitions:  
- \( a \in A \) is a zero divisor if \( a \neq 0 \) and \( \exists b \in A, b \neq 0, ab = 0 \).
- \( A \) is domain if \( A \) has no zero divisors.
- Ideal \( \mathfrak{p} \subseteq A \) is prime if \( \mathfrak{p} \neq A \) and \( A/\mathfrak{p} \) is domain.

Exercise: TFAE:

i) \( \mathfrak{p} \) is prime  
\[ \text{remark: } \Leftarrow \text{ is automatic} \]

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 \( I, J \subseteq A \) are ideals, \( IJ \subseteq \mathfrak{p} \Rightarrow I \subseteq \mathfrak{p} \) or \( J \subseteq \mathfrak{p} \).

Examples:  
- maximal \( \Rightarrow \) prime (by field \( \Rightarrow \) domain).
- \( \{0\} \subseteq A \) is prime \( \iff \) \( A \) is domain.
- \( A = \mathbb{Z} \). Every ideal is \( (n) \) for \( n \in \mathbb{Z} \); \( (n) \) is prime \( \iff \) \( n \) is prime or \( n = 0 \). So every prime is maximal 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):
\( \mathbb{F}[x, y]/(x) \cong \mathbb{F}[y] \) (domain but not field).

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

2.1) Definitions (of modules & homomorphisms). \( A \) commutative unital ring.
1) By an \( A \)-module we mean abelian group \( M \) w. map
\[
A \times M \rightarrow M \text{ (multiplication or action map) s.t.}
\]
\[
\begin{align*}
\cdot \text{ Associativity: } & \quad (ab)m = a(bm) \in M \\
\cdot \text{ Distributivity: } & \quad (a+b)m = am + bm, \quad a(m+m') = am + am' \in M \\
\cdot \text{ Unit: } & \quad 1m = m \in M
\end{align*}
\]
\( \forall a,b \in A, \ m,m' \in M. \)

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

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

Observation: Let \( \phi : A \rightarrow B \) be a ring homomorphism.

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

II) If \( \phi : A \rightarrow B \) (surjective), then a \( B \)-module = \( A \)-module, where ker \( \phi \) acts by 0 (\( am = 0 \) if \( m \in \text{ker} \phi \)).
An \( A \)-linear map between \( B \)-modules \( M \& N \) is also \( B \)-linear.

2.2) Examples.

1) \( A = \mathbb{Z} \). Then \( A \times M \rightarrow M \) can be recovered from + in \( M \).
So \( \mathbb{Z} \)-module = abelian group.
2) Modules vs Linear Algebra
   i) $A = \mathbb{F}[x]$ (if $\mathbb{F}$ is field)

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

   $$f(x)m = [f(x): M \rightarrow M] = f(x)m$$

   So $\mathbb{F}[x]$-module = $\mathbb{F}$-vector space w. a linear operator

   An $\mathbb{F}[x]$-module homomorphism $\psi: M \rightarrow N$ is the same thing as a linear map $\psi: M \rightarrow N$ s.t. $X_N \psi = \psi X_M$, where

   $X_M: M \rightarrow M$, $X_N: N \rightarrow N$ are operators coming from $x$.

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

   iii) $A = \mathbb{F}[x_1, \ldots, x_n]/(C_1, \ldots, C_k)$, $C_i \in \mathbb{F}[x_1, \ldots, x_n]$. Use of Observation II w. $\mathbb{F}[x_1, \ldots, x_n] \rightarrow \mathbb{R}$ shows that $A$-module = $\mathbb{F}[x_1, \ldots, x_n]$-module where ker $\psi$ acts by $0$. = $\mathbb{F}$-vector space w. $n$ commuting operators $x_1, \ldots, x_n$ s.t. $C_i(x_1, \ldots, x_n) = 0$ as operators $M \rightarrow M$ $\forall i = 1, \ldots, k$.

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

   For a ring homom. $\phi: A \rightarrow B$, $B$ becomes an $A$-module

   So $A$-algebra is an $A$-module. Conversely, let $M$ be $A$-module. How to describe an (assoc, unital) algebra struc on $M$: this is a map $M \times M \rightarrow M$ s.t.
associative & has unit (M is a unital ring)

- $M \times M \rightarrow M$ 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'ke is a module str'ke + $A$-bilinear product (usual def'n of an algebra).

Once $M$ is an $A$-algebra with this def'n, we get a ring homomorphism $A \rightarrow M$: $a \mapsto a \cdot 1$ (1 unit in $M$).

2.3) Constructions with modules ($\&$ homomorphisms)

I) Direct sums $\&$ products.

$M_1, M_2$ $A$-modules $\Rightarrow$

- $M_1 \oplus M_2$ (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 $\prod M_i = \{ (m_i)_{i \in I} | m_i \in M_i \}$ w.

componentwise operations.

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

Have $A$-module inclusion:

$$\bigoplus M_i \subseteq \prod M_i$$

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

II) Hom module: let $M, N$ be $A$-modules $\Rightarrow \text{Hom}_A(M, N)$

$\text{= the set of all } A$-module homomorphisms. It has a natural $A$-module str'ke. Need to define addition $\&$ multiplication by
Lemma: 1) $\psi + \psi', a\psi$ are $A$-linear maps.
2) The operations $+$, $\cdot$ turn $\text{Hom}_A(M, N)$ into $A$-module.

Partial proof: $[a\psi](bm) = b[a\psi](m)$.
$[a\psi](bm) = a(\psi(bm)) = ab \psi(m) = [ab \cdot \psi](m) = 6(a\psi)(m) = 6[a\psi](m)$.

Rest of proof is an exercise \(\square\)

Example: $M = A^k$. Claim: have natural isomorphism

$$\text{Hom}_A(A^k, N) \xrightarrow{\sim} N^k.$$ 

- Want a map $c : \text{Hom}_A(A^k, N) \to N^k$. $e_i = (0, \ldots, 1, \ldots, 0) \in A^k$
- $i$th coord vector, $i = 1, \ldots, k$, so $(a_1, \ldots, a_k) = \sum_{i=1}^{k} a_i e_i$.
- $c(\psi) = (\psi(e_1), \psi(e_2), \ldots, \psi(e_k)) \in N^k$.

- $N^k \to \text{Hom}_A(A^k, N)$.
- $\psi(a_1, \ldots, a_k) = \sum_{i=1}^{k} a_i e_i$.
- $\mathbf{n} = (n_1, \ldots, n_k) \mapsto \psi_n$.

Exercise: Verify $\psi_n$ is a module homomorphism $A^k \to N$ and that $c$ & $[\mathbf{n} \mapsto \psi_n]$ are indeed mutually inverse $A$-module homomorphisms between $\text{Hom}_A(A^k, N)$ & $N^k$.

**BONUS:** Noncommutative counterparts, part 3.

B1) Prime & completely prime ideals: For a commutative ring $A$
& an ideal \( \mathfrak{p} \subset \mathfrak{a} \) 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 \( I, J \subset \mathfrak{a} \): \( IJ \subset \mathfrak{p} \Rightarrow I \subset \mathfrak{p} \) or \( J \subset \mathfrak{p} \).

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

Definition: Let \( \mathfrak{a} \) be a ring and \( \mathfrak{p} \subset \mathfrak{a} \) 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 \( a, b \in \mathfrak{a} \), have \( ab \in \mathfrak{p} \Rightarrow a \in \mathfrak{p} \) or \( b \in \mathfrak{p} \).

Completely prime \( \Rightarrow \) prime but not vice versa.

Exercise: 1) \( \mathfrak{so}_3 \subset \text{Mat}_n(\mathbf{F}) \) is prime but not completely prime (if \( n \geq 2 \)).
2) \( \mathfrak{so}_3 \subset \text{Weyl}_n(=\mathbf{F}\langle x, y \rangle/(yx-xy-1)) \) is completely prime.

B2) Modules over noncommutative rings. Here we have left & right modules & also bi-modules. Let \( \mathfrak{a} \) be a ring.

Definition: A left \( \mathfrak{a} \)-module \( M \) is an abelian group with multiplication map \( \mathfrak{a} \times M \rightarrow M \) subject to the same axioms as in the commutative case.

A right \( \mathfrak{a} \)-module is a similar thing but with multiplication map \( M \times \mathfrak{a} \rightarrow M \) subject to associativity \( (ma)b = m(ab) \), distributivity & unit axioms.

An \( \mathfrak{a} \)-bi-module is an abelian group \( M \) equipped
There are left and right \( A \)-module structures s.t. we have another associativity axiom: \((am)b = a(mb) \quad \forall a, b \in A\).

When \( A \) is commutative, there's no difference between left and 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 \( A \)-module.
2) \( \mathbb{F}^n \) (the space of columns) is a left \( \text{Mat}_n(\mathbb{F}) \)-module, while its dual \((\mathbb{F}^n)^* \) (the space of rows) is a right \( \text{Mat}_n(\mathbb{F}) \)-module. None of these has a bimodule structure.

Exercise: Construct a left \( \text{Weyl}_2 \)-module structure on \( \mathbb{F}[x] \)
(hint: \( y \) acts as \( \frac{d}{dx} \)).

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