Lecture 4: rings, ideals & modules, IV.

1) Constructions w. modules.
2) Submodules & quotient modules.
3) Finitely generated & free modules.

References: [AM], Chapter 2, Sections 2,3,5.

1) Construction with modules & homomorphisms: Hom module

Let A be a commutative ring & M,N be A-modules. Define the <u>set</u> $\mathrm{Hom}_A(M,N) := \{A\text{-linear maps } M\to N\}$

Claim: $\mathrm{Hom}_A(M,N)$ is A-module w.r.t. the point-wise operations: for $\varphi,\varphi'\in \mathrm{Hom}_A(M,N)$, $a\in A$

$[\varphi+\varphi'](m) := \varphi(m)+\varphi'(m)\in N$ ($\rightsquigarrow \varphi+\varphi'$ is a map $M\to N$)

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

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

2) The operations $+,\cdot$ turn $\mathrm{Hom}_A(M,N)$ into A-module.

Partial proof: $[a\varphi](bm) = b[a\varphi](m)$ - part of linearity for $a\varphi$.

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

Rest of proof is an exercise. $\square$

Example: 1) Let $M=A$. Then $\mathrm{Hom}_A(A,N)\xrightarrow{\sim} N$ as A-modules.

Namely, we have a map $\mathrm{Hom}_A(A,N) \to N$, $\varphi \mapsto \varphi(1)$. It's A-linear & has inverse: for $n \in N$ define the map $\varphi_n : A \to N$, $a \mapsto an$. The inverse is $n \mapsto \varphi_n$. To check details (that these maps are well-defined & mutually inverse) is an exercise. $\square$

2) $$\begin{array}{ccc} \mathrm{Hom}_A(M_1 \oplus M_2, N) & \xrightarrow{\sim} & \mathrm{Hom}_A(M_1,N) \times \mathrm{Hom}_A(M_2,N) \\ \rotatebox{90}{$\in$} & & \\ \varphi & \mapsto & (\varphi|_{M_1}, \varphi|_{M_2}), \end{array}$$ where $M_1 \hookrightarrow M_1 \oplus M_2$ via $m_1 \mapsto (m_1, 0)$, and similarly for M_2.

Inverse map: $(\varphi_1, \varphi_2) \in \mathrm{Hom}_A(M_1,N) \times \mathrm{Hom}_A(M_2,N)$ goes to $\varphi : M_1 \oplus M_2 \to N$ given by $\varphi(m_1, m_2) := \varphi_1(m_1) + \varphi_2(m_2)$

Exercise: Prove that these two maps are mutually inverse A-module homomorphisms.

3) There is a direct analog of example 2) for $M_1 \oplus \dots \oplus M_k$.

E.g. $$\begin{array}{ccccc} \mathrm{Hom}_A(A^{\oplus k}, N) & \xrightarrow{\sim} & \mathrm{Hom}_A(A,N)^{\times k} & \xrightarrow{\sim} & N^{\times k} \\ \rotatebox{90}{$\in$} & & & & \rotatebox{90}{$\in$} \\ \varphi & \longmapsto & & & (\varphi(e_1), \dots \varphi(e_k)) \end{array}$$

where $e_i = (0, \dots 1, \dots 0)$ (1 in the ith place). The inverse map is given by $\underline{n} = (n_1, \dots n_k) \mapsto \varphi_{\underline{n}} : (a_1, \dots a_k) \mapsto \sum a_i n_i$.

Rem: Example 2 further generalizes to infinite direct sums:

$$\mathrm{Hom}_A\Big(\bigoplus_{i \in I} M_i, N\Big) \xrightarrow{\sim} \prod_{i \in I} \mathrm{Hom}_A(M_i, N)$$

The proof is similar to the above and is left as exercise.

2) Sub & quotient modules.

2.1) Submodules:

Let A be a comm've ring.

Definition: Let M be an A-module; a submodule in M is an abelian subgroup $N \subset M$ s.t. $a \in A, n \in N \Rightarrow an \in N$.

Rem: N has a natural A-module str're.

Examples: 0) $\{0\}, M \subset M$ are submodules.

1) A is a field (so module = vector space): Submodule = subspace.

2) $A = \mathbb{Z}$ (so module = abelian group): Submodule = subgroup.

3) $A = \mathbb{F}[x]$ ($\mathbb{F}$ is a field). A module M = $\mathbb{F}$-vector space w. operator $X: M \to M$. A submodule $N \subset M$ - subspace s.t. $X(N) \subseteq N$. Conversely, every X-stable subspace is a submodule b/c $f(x)m = f(X)m$ & $X(N) \subseteq N \Rightarrow f(X)(N) \subset N$.

4) A is any ring, $M = A$: submodule = ideal.

2.2) Constructions w. submodules.

1) $\varphi: M \to N$ A-module homom'm: $\ker\varphi \subset M$ & $\operatorname{im}\varphi \subset N$ are submodules, left as exercise.

2) $m_1, \dots, m_k \in M \rightsquigarrow \mathrm{Span}_A(m_1, \dots, m_k) := \{\sum_{i=1}^{k} a_i m_i \mid a_i \in A\}$ - this is special case of image: $\underline{m} = (m_1, \dots, m_k) \rightsquigarrow \varphi_{\underline{m}}: A^{\oplus k} \to M$ (see example 3 in Sec 1.2) Then $\mathrm{Span}_A(m_1, \dots, m_k) = \mathrm{im}\, \varphi_{\underline{m}}$.
Note also that this generalizes the ideal generated by a given collection of elements, Sec 3.1 of Lec 1. More generally, for index set I & $m_i \in M$ $(i \in I) \rightsquigarrow \mathrm{Span}_A(m_i \mid i \in I) = \{$finite A-linear combinations of m_i's$\}$.

3) Sums & intersections: $M_1, M_2 \subset M$ submodules
$M_1 \cap M_2$, $M_1 + M_2 = \{m_1 + m_2 \mid m_i \in M_i\}$ - submodules

4) Product w. ideal: $N \subset M$ submodule, $I \subset A$ ideal
$IN := \{\sum_{i=1}^{\ell} a_i n_i \mid a_i \in I, n_i \in N\}$ - submodule, exercise.
(compare to product of ideals in 1.1 of Lecture 2).

2.3) Quotient modules: M is A-module, $N \subset M$ submodule $\rightsquigarrow$ abelian group $M/N = \{m + N \mid m \in M\}$ & abelian group homom'm $\pi: M \twoheadrightarrow M/N$, $\pi(m) := m + N$. Then M/N has a natural A-module str're. The following is analogous to Proposition in Sec 3.2 of Lecture 1.

Proposition: 1) The map $A \times (M/N) \to M/N$, $(a, m+N) \mapsto am + N$ is well-defined ($am + N$ only depends on $m + N$ & not on m itself) and equips M/N w. A-module structure.

2) This module structure is unique s.t. $\pi: M \to M/N$ is a module homomorphism.

3) (Universal property of M/N & $\pi: M \twoheadrightarrow M/N$) Let $\psi: M \to M'$ be A-module homom'm s.t $N \subset \ker\psi$. Then $\exists!$ module homom'm $\underline{\psi}: M/N \to M'$ s.t. the following diagram is commutative

$$\begin{tikzcd} M \arrow[d, "\pi"'] \arrow[dr, "\psi"] & \\ M/N \arrow[r, dashed, "\underline{\psi}"'] & M' \end{tikzcd}$$

$\underline{\psi}$ is given by: $\underline{\psi}(m+N) := \psi(m)$

Proof: exercise.

Remarks:

1) Let $I \subset A$ be ideal $\rightsquigarrow$ submodule $IM \subset M \rightsquigarrow$ quotient M/IM is A-module where I acts by 0 = A/I-module; explicitly $(a+I)(m+IM) = am + IM$ (see Observation II in Sec 2.2 of Lec 3).

2) We have standard "isomorphism theorems":

- for $\varphi: M \to N$, A-module homom'm, have $M/\ker\varphi \xrightarrow{\sim} \operatorname{im}\varphi$ (A-module isomorphism).
- for submodules $K \subset N \subset M$, have $(M/K)/(N/K) \xrightarrow{\sim} M/N$.
- for submodules $N_1, N_2 \subset M$, have $N_1/N_1 \cap N_2 \xrightarrow{\sim} (N_1+N_2)/N_2$

The reason is that the standard abelian group isomorphisms are also module isomorphisms.

3) There are bijections between:

$$\begin{tikzcd}
\{\text{submodules } L\subset M \mid N\subset L\} \arrow[d, bend right, "L\mapsto \pi(L)=L/N"'] \\
\{\text{submodules } \underline{L}\subset M/N\} \arrow[u, bend right, "\underline{L}\mapsto \pi^{-1}(\underline{L})"']
\end{tikzcd}$$

We've seen a similar claim for ideals in Sec. 3.2 of Lec. 1.

3) Finitely generated & free modules.

3.1) Finitely generated modules

Definition: • Elements $m_i\in M$ $(i\in I)$ are **generators** (a.k.a. **spanning set**) of M if $M=\mathrm{Span}_A(m_i \mid i\in I)$, i.e. $\forall m\in M$ is A-linear combination of finite number of m_i's.

• M is **finitely generated** if it has a finite spanning set.

Remarks: 1) $A^{\oplus I}$ is finitely generated $\Leftrightarrow$ I is finite.

2) If M is fin. generated, then so is M/N $\forall N\subset M$:
$M=\mathrm{Span}_A(m_1,\dots m_k) \Rightarrow M/N=\mathrm{Span}_A(\pi(m_1),\dots,\pi(m_k))$.

3) $\underline{m}=(m_1,\dots m_k) \rightsquigarrow \varphi_{\underline{m}}: A^{\oplus k}\to M$, $\varphi_{\underline{m}}(a_1,\dots a_k)=\sum_{i=1}^k a_i m_i$.
$M=\mathrm{Span}_A(m_1,\dots m_k) \Leftrightarrow \varphi_{\underline{m}}$ is surj've $\Rightarrow M \xrightarrow{\sim} A^{\oplus k}/\ker\varphi_{\underline{m}}$
So: fin. gen'd modules = quotients of $A^{\oplus k}$ for some $k\in\mathbb{Z}_{\geq 0}$.

3.2) Free modules

Let M be an A-module.

Definition: • Elements $m_i, i\in I$, form a basis in M if $\forall\, m\in M$ is uniquely written as A-linear combination of $m_i, i\in I$.
• M is free if it has a basis.

Examples: 1) For any set I, $A^{\oplus I}$ is free, for a basis can take coordinate vectors $e_i = (0,\dots \underset{\text{ith place}}{1}, \dots 0..)$, $i\in I$.

2) If A is field, then every module (a.k.a. vector space) is free. If A is not a field, there are non-free modules: let $J\subset A$ be ideal, $J\neq\{0\}, A \Rightarrow A/J$ is not free (over A).
Indeed, for any vector e in a basis we must have $ae\neq 0$ $\forall\, a\in A$. But for any $e\in A/J$ we have $ae=0$ $\forall\, a\in J$.

Remarks 1) Every free module is isomorphic to $A^{\oplus I}$ for some set I: choose basis $m_i\in M$ $(i\in I)$: $\varphi_{\underline{m}}: A^{\oplus I} \xrightarrow{\sim} M$. Moreover, Problem 5 in HW1 shows that I is uniquely determined by M (up to bijection of sets)

2) As for vector spaces, any homomorphism $\varphi: A^{\oplus k} \longrightarrow A^{\oplus \ell}$ is given by multiplication by an $\ell\times k$-matrix (where elements of $A^{\oplus k}, A^{\oplus \ell}$ are viewed as column vectors) & the matrix is uniquely determined by φ.